**А.М. ГОЛИКОВ**

# ЗАЩИТА ИНФОРМАЦИИ В ИНФОКОММУНИКАЦИОННЫХ СИСТЕМАХ И СЕТЯХ

**Учебное пособие**

для специалитета: 11.05.01 - Радиоэлектронные системы и комплексы (Радиоэлектронные системы передачи информации)

Курс лекций, компьютерные лабораторные работы, компьютерный практикум, задание на самостоятельную работу

**Второе издание дополненное и переработанное**

**Томск 2017**

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное
учреждение высшего образования
Томский государственный университет систем управления и
радиоэлектроники

**А.М. ГОЛИКОВ**

# ЗАЩИТА ИНФОРМАЦИИ В ИНФОКОММУНИКАЦИОННЫХ СИСТЕМАХ И СЕТЯХ

Учебное пособие
для специалитета: 11.05.01 - Радиоэлектронные системы и комплексы
(Радиоэлектронные системы передачи информации)
Курс лекций, компьютерные лабораторные работы, компьютерный
практикум, задание на самостоятельную работу
**Второе издание дополненное и переработанное**

**Томск 2017**

УДК 621.39(075.8)

ББК 32.973(я73)
Г 60
Голиков А.М.
Защита информации в инфокоммуникационных системах и сетях. Учебное пособие для специалитета: 11.05.01 - Радиоэлектронные системы и комплексы (Радиоэлектронные системы передачи информации). Курс лекций, компьютерные лабораторные работы, компьютерный практикум, задание на самостоятельную работу. Второе издание дополненное и переработанное. / А.М.Голиков. – Томск: Томск. гос. ун-т систем упр. и радиоэлектроники, 2017. – 655 с.: ил. — (Учебная литература для вузов)

Учебное пособие предназначено для направления подготовки специалистов по направлению 11.05.01 - Радиоэлектронные системы и комплексы (Радиоэлектронные системы передачи информации). В учебном пособии рассмотрены основные понятия теории информационной безопасности, методология построения систем защиты автоматизированных информационных систем (АС), понятие формальных политик безопасности, дана классификация математических моделей информационной безопасности, рассмотрены основные дискреционные и мандатные модели, основные критерии защищенности АС, классы защищенности, включая международные стандарты: ISO 15408 «Критерии оценки безопасности информационных технологий» Common Criteria и ISO 17799 «Практические правила управления информационной безопасностью», а также основные средства защиты информации, включая неформальные (законодательные, административные, процедурные) и формальные (программно-технические), рассмотрена типовая модель безопасности информационной сети предприятия, методы и средства аудита безопасности информационных систем.

Рассмотрены технические методы и средства защиты информации, даны понятия об объектах защиты информации, о характеристиках угроз, технических каналах утечки информации, методах и средствах поиска электронных устройств перехвата информации, освещаются вопросы организации инженерно-технической защиты информации и ее методическое обеспечение. В приложении к учебному пособию приведены современные технические средства защиты информации.

Учебное пособие предназначено для изучения вопросов, предлагаемых Государственными образовательными стандартами высшего профессионального образования для специалитета: 11.05.01 – Радиоэлектронные системы и комплексы (Радиоэлектронные системы передачи информации).

**СОДЕРЖАНИЕ**

**Введение**

Проблема защиты информации не нова. Она появилась вместе с компьютерами. Естественно, что стремительное совершенствование компьютерных технологий отразилось и на принципах построения защиты информации. Задачи изменились, а мнения остались прежние - так рождаются мифы. Вот несколько мифов компьютерной безопасности.

Миф первый. «Защита информации и криптография - близнецы-братья». Этот миф, видимо, связан с тем, что с самого начала своего развития системы информационной безопасности разрабатывались для военных ведомств. Разглашение такой информации могла привести к огромным жертвам, в том числе и человеческим. Поэтому конфиденциальности (т.е. неразглашению информации) в первых системах безопасности уделялось особое внимание. Очевидно, что надежно защитить сообщения и данные от подглядывания и перехвата может только полное их шифрование. Видимо, из-за этого начальный этап развития компьютерной безопасности прочно связан с криптошифрами.

Однако сегодня информация имеет уже не столь «убойную» силу, и задача сохранения ее в секрете потеряла былую актуальность. Сейчас главные условия безопасности информации - ее доступность и целостность. Любой файл или ресурс системы должен быть доступен в любое время (при соблюдении прав доступа). Если какой-то ресурс недоступен, то он бесполезен. Другая задача защиты - обеспечить неизменность информации во время ее хранения или передачи. Это так называемое условие целостности.

Таким образом, конфиденциальность информации, обеспечиваемая криптографией, не является главным требованием при проектировании защитных систем. Выполнение процедур криптокодирования и декодирования может замедлить передачу данных и уменьшить их доступность, так как пользователь будет слишком долго ждать свои "надежно защищенные" данные, а это недопустимо в некоторых современных компьютерных системах. Поэтому система безопасности должна в первую очередь гарантировать доступность и целостность информации, а затем уже (если необходимо) ее конфиденциальность. Принцип современной защиты информации можно выразить так - поиск оптимального соотношения между доступностью и безопасностью.

Миф второй. «Во всем виноваты хакеры». Этот миф поддерживают средства массовой информации, которые со всеми ужасающими подробностями описывают «взломы банковских сеток». Однако редко упоминается о том, что хакеры чаще всего используют некомпетентность и халатность обслуживающего персонала. Хакер - диагност. Именно некомпетентность пользователей можно считать главной угрозой безопасности. Также серьезную угрозу представляют служащие, которые чем-либо недовольны, например, заработной платой.

Одна из проблем подобного рода - так называемые слабые пароли. Пользователи для лучшего запоминания выбирают легко угадываемые пароли. Причем проконтролировать сложность пароля невозможно. Другая проблема - пренебрежение требованиями безопасности. Например, опасно использовать непроверенное программное обеспечение. Обычно пользователь сам «приглашает» в систему вирусы и «троянских коней». Кроме того, много неприятностей может принести неправильно набранная команда. Так, при

программировании аппарата ФОБОС-1 ему с Земли была передана неправильная команда. В результате связь с ним была потеряна.

Таким образом, лучшая защита от нападения - не допускать его. Обучение пользователей правилам безопасности может предотвратить нападения. Другими словами, защита информации включает в себя кроме технических мер еще и обучение или правильный подбор обслуживающего персонала.

Миф третий. «Абсолютная защита». Абсолютной защиты быть не может. Распространено такое мнение – «установил защиту и можно ни о чем не беспокоиться». Полностью защищенный компьютер - это тот, который стоит под замком в бронированной комнате в сейфе, не подключен ни к какой сети (даже электрической) и выключен. Такой компьютер имеет абсолютную защиту, однако, использовать его нельзя. В этом примере не выполняется требование доступности информации. «Абсолютности» защиты мешает не только необходимость пользоваться защищаемыми данными, но и усложнение защищаемых систем. Использование постоянных, не развивающихся механизмов защиты опасно, и для этого есть несколько причин.

Кроме того, нельзя забывать о развитии и совершенствовании средств нападения. Техника так быстро меняется, что трудно определить, какое новое устройство или программное обеспечение, используемое для нападения, может обмануть вашу защиту. Например, криптосистема DES, являющаяся стандартом шифрования в США с 1977 г., сегодня может быть раскрыта методом «грубой силы» - прямым перебором.

Компьютерная защита - это постоянная борьба с глупостью пользователей и интеллектом хакеров.

В заключение хочется сказать о том, что защита информации не ограничивается техническими методами. Проблема значительно шире. Основной недостаток защиты - люди, и поэтому надежность системы безопасности зависит в основном от отношения к ней служащих компании. Помимо этого, защита должна постоянно совершенствоваться вместе с развитием компьютерной сети. Не стоит забывать, что мешает работе не система безопасности, а ее отсутствие.

## 1. Структура теории информационной безопасности

### 1.1. Основные понятия теории информационной безопасности

Для того, чтобы определить эти понятия воспользуемся математической логикой. Пусть А конечный алфавит, $A$ - множество слов конечной длины в алфавите А.

Из А при помощи некоторых правил выделено подмножество $Я$ правильных слов, которое называется языком. Если $Я_1$ - язык описания одной информации, $Я_2$ - другой, то

можно говорить о языке Я, объединяющем $Я_1$ и $Я_2$ описывающем ту и другую информацию. Тогда $Я_1$ и $Я_2$ подъязыки *Я*.

Будем считать, что любая информация представлена в виде слова в некотором языке *Я*. Кроме того, можно полагать, что состояние любого устройства в вычислительной системе достаточно полно описано словом в некотором языке. Тогда можно отождествлять слова и состояния устройств и механизмов вычислительной системы или произвольной электронной системы обработки данных (ЭСОД). Эти предположения позволяют весь анализ вести в терминах некоторого языка.

*Определение:* Объектом относительно языка Я называется произвольное конечное множество языка *Я*.

*Пример 1*: Пусть текст в файле разбит на параграфы так, что любой параграф также является словом языка *Я* и, следовательно, тоже является объектом. Таким образом, один объект может являться частью другого.

*Пример 2:* Принтер компьютера - объект. Существует некоторый (достаточно сложный) язык, описывающий принтер и его состояния в произвольный момент времени. Множество допустимых описаний состояний принтера является конечным подмножеством слов в этом языке. Именно это конечное множество и определяет принтер как объект.

Другими словами объект – это пассивная сущность (любая именованная составляющая компьютерной системы), используемая для хранения или получения информации. В качестве объекта могут выступать записи, блоки, байты, слова, страницы, сегменты, файлы, биты, директории, терминалы, узлы, сети и т.д.

В информации выделим описания преобразований данных. Преобразование информации отображает слово, описывающее исходные данные, в другое слово. Описание преобразования данных также является словом. Примерами объектов, описывающих преобразования данных, являются программы для ЭВМ.

Каждое преобразование информации может:

а) храниться;

б) действовать.

В случае а) речь идет о хранении описания преобразования в некотором объекте (файле). В этом случае преобразование ничем не отличается от других данных. В случае б) описание программы взаимодействует с другими ресурсами вычислительной системы - памятью, процессором, коммуникациями и др.

*Определение:* Ресурсы системы, выделяемые для действия преобразования, называются доменом.

Однако для осуществления преобразования одних данных в другие кроме домена необходимо передать этому преобразованию особый статус в системе, при котором ресурсы системы осуществляют преобразование. Этот статус будем называть «управление».

*Определение:* Преобразование, которому передано управление, называется процессом.

При этом подразумевается, что преобразование осуществляется в некоторой системе, в которой ясно, что значит передать управление.

*Определение:* Объект, описывающий преобразование, которому выделен домен и передано управление, называется субъектом.

То есть субъект можно определить как активную сущность (любая именованная составляющая компьютерной системы), которая может инициировать запросы ресурсов и использовать их для выполнения каких – либо вычислительных заданий. Под субъектами обычно понимаю пользователя, процесс или устройство.

С одной стороны основную концепцию идентификации субъектов и объектов в системе описать просто, а вот с другой стороны, при практической реализации оказывается не тривиальной задачей определить: что есть субъект, а что – объект. Например, в ОС процессы, безусловно, являются субъектами, в то время как файлы и связанные с ними директории – объектами. Но, когда субъекты получают сигналы на выполнение каких – либо заданий от других субъектов, то возникает вопрос рассматривать их как субъекты или же, как объекты.

В процессе исполнения субъекты выполняют некоторые операции. В результате происходит взаимодействие субъектов и объектов.

*Определение:* Доступ – это взаимодействие между субъектами и объектами, результатом которого является перенос информации между ними.

Существует две базовые операции, переносящие информации между ними субъектами и объектами: чтение, запись. Под операцией чтения понимается операция, результатом которой является перенос информации от объекта к субъекту. Под операцией записи понимается операция, результатом которой является перенос информации от объекта к субъекту [1 – 7].

В заключение можно добавить аксиому: все вопросы безопасности информации описываются доступами субъектов к объектам.

**1.2. Ценность информации**

Чтобы защитить информацию, надо затратить силы и средства, а для этого надо знать какие потери мы могли бы понести. Ясно, что в денежном выражении затраты на защиту не должны превышать возможные потери. Для решения этих задач в информацию вводятся вспомогательные структуры - ценность информации. Рассмотрим примеры.

*1. Аддитивная модель.* Пусть информация представлена в виде конечного множества элементов и необходимо оценить суммарную стоимость в денежных единицах из оценок компонент. Оценка строится на основе экспертных оценок компонент, и, если денежные оценки объективны, то сумма дает искомую величину. Однако, количественная оценка компонент не всегда объективна даже при квалифицированной экспертизе. Это связано с неоднородностью компонентов в целом. Поэтому делают единую иерархическую относительную шкалу (линейный порядок, который позволяет сравнивать отдельные компоненты по ценности относительно друг друга). Единая шкала означает равенство цены всех компонент, имеющих одну и туже порядковую оценку.

*Пример:* $0_1,...,0_n$ - объекты, шкала 1<...<5. Эксперты оценили (2, 1, 3,...., 4) - вектор относительных ценностей объектов. Если есть цена хотя бы одного объекта, например, $C_1$=100 руб., то вычисляется оценка одного балла $C_1/\lambda$. = 50 руб.,

где $\lambda$ - число баллов оценки первого объекта, и вычисляется цена каждого следующего объекта: $C_2$=50руб., $C_3$=150 руб. и т.д. Сумма дает стоимость всей информации. Если априорно известна цена информации, то относительные оценки в порядковой шкале позволяют вычислить цены компонент.

*2. Порядковая шкала ценностей.* Далеко не всегда возможно и нужно давать денежную оценку информации. Например, оценка личной информации, политической информации или военной информации не всегда разумна в денежном исчислении. Однако подход, связанный со сравнением ценности отдельных информационных элементов между собой, по-прежнему имеет смысл.

*Пример:* При оценке информации в государственных структурах используется порядковая шкала ценностей. Все объекты (документы) государственного учреждения разбиваются по грифам секретности. Сами грифы секретности образуют порядковую шкалу: несекретно < для служебного пользования <секретно < совершенно секретно (НС<ДСП<С<СС) или у американцев : unclassified<confidential<secret<top secret (U<Conf<S<TS). Более высокий класс имеет более высокую ценность и поэтому требования по его защите от несанкционированного доступа более высокие.

**1.3. Анализ угроз информационной безопасности**

Информация с точки зрения информационной безопасности обладает следующими категориями:

- *конфиденциальность* – гарантия того, что конкретная информация доступна только тому кругу лиц, для кого она предназначена; нарушение этой категории называется хищением либо раскрытием информации

- *целостность* – гарантия того, что информация сейчас существует в ее исходном виде, то есть при ее хранении или передаче не было произведено несанкционированных изменений; нарушение этой категории называется фальсификацией сообщения
- *аутентичность* – гарантия того, что источником информации является именно то лицо, которое заявлено как ее автор; нарушение этой категории также называется фальсификацией, но уже автора сообщения
- *апеллируемость* – довольно сложная категория, но часто применяемая в электронной коммерции – гарантия того, что при необходимости можно будет доказать, что автором сообщения является именно заявленный человек, и не может являться никто другой; отличие этой категории от предыдущей в том, что при подмене автора, кто-то другой пытается заявить, что он автор сообщения, а при нарушении апеллируемости – сам автор пытается «откреститься» от своих слов, подписанных им однажды.

В отношении информационных систем применяются иные категории:

- *надежность* – гарантия того, что система ведет себя в нормальном и внештатном режимах так, как запланировано
- *точность* – гарантия точного и полного выполнения всех команд
- *контрол*ь доступа – гарантия того, что различные группы лиц имеют различный доступ к информационным объектам, и эти ограничения доступа постоянно выполняются
- *контролируемость* – гарантия того, что в любой момент может быть произведена полноценная проверка любого компонента программного комплекса
- *контроль идентификации* – гарантия того, что клиент, подключенный в данный момент к системе, является именно тем, за кого себя выдает
- *устойчивость к умышленным сбоям* – гарантия того, что при умышленном внесении ошибок в пределах заранее оговоренных норм система будет вести себя так, как оговорено заранее.

Под угрозой обычно понимают потенциально возможное событие, действие, процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам.

Исследователи предложили выделить три различных типа угроз. А именно, было отмечено, что наиболее общие угрозы вычислительным системам могут быть рассмотрены как относящиеся к раскрытию, целостности или отказу служб вычислительной системы.

*Угроза конфиденциальности*. Заключается в том, что информация становится известной тому, кому не следовало бы ее знать. В терминах компьютерной безопасности данная угроза имеет место всякий раз, когда получен доступ к некоторой секретной информации, хранящейся в вычислительной системе или передаваемой от одной системы к другой. Иногда в связи с угрозой раскрытия используется термин «утечка».

В руководстве по использованию стандарта защиты информации американцы говорят, что существует только два пути нарушения конфиденциальности:

утрата контроля над системой защиты;

каналы утечки информации.

Если система обеспечения защиты перестает адекватно функционировать, то, естественно, траектории вычислительного процесса могут пройти через состояние, когда осуществляется запрещенный доступ. Каналы утечки характеризуют ту ситуацию, когда-либо проектировщики не смогли предупредить, либо система не в состоянии рассматривать такой доступ как запрещенный. Утрата управления системой защиты может быть реализована оперативными мерами и здесь играют существенную роль административные и кадровые методы защиты. Утрата контроля над защитой может возникнуть в критической ситуации, которая может быть создана стихийно или искусственно. Поэтому одной из главных опасностей для системы защиты является отсутствие устойчивости к ошибкам.

Утрата контроля может возникнуть за счет взламывания защиты самой системы защиты. Противопоставить этому можно только созданием защищенного домена для системы защиты.

Большой спектр возможностей дают каналы утечки. Основной класс каналов утечки в - каналы по памяти (т.е. каналы, которые образуются за счет использования доступа к общим объектам системы).

*Угроза целостности*. Нарушения целостности информации - это незаконные уничтожение или модификация информации.

Традиционно защита целостности относится к категории организационных мер. Основным источником угроз целостности являются пожары и стихийные бедствия. К уничтожению и модификации могут привести также случайные и преднамеренные критические ситуации в системе, вирусы, «троянские кони» , случайная ошибка и т.д.

Но не исключены санкционированные изменения, т.е. такие, которые сделаны определенными лицами с обоснованной целью (таким изменением является периодическая запланированная коррекция некоторой базы данных).

Некоторое время условно считалось, что правительства сосредотачивались на раскрытии, а деловые круги касались целостности. Но, обе эти стороны могли бы быть более или менее связаны каждой из двух угроз в зависимости от приложения.

*Угроза отказа служб.* Возникает всякий раз, когда в результате преднамеренных действий, предпринятых другим пользователем, умышленно блокируется доступ к некоторому ресурсу вычислительной системы. То есть, если один пользователь запрашивает доступ к службе, а другой предпринимает что-либо для недопущения этого доступа, мы говорим, что имеет место отказ службы. Реально блокирование может быть постоянным, так

чтобы запрашиваемый ресурс никогда не был получен, или оно может вызывать только задержку запрашиваемого ресурса, достаточно долгую для того, что бы он стал бесполезным. В таких случаях говорят, что ресурс исчерпан.

Кроме перечисленных основных видов угроз существуют и другие, которые принято классифицировать по ряду признаков.

1. *По природе возникновения.*

1.1. Естественные угрозы (независящих от человека: стихийные бедствия, магнитные бури. радиоактивное излучение и т.п.).

1.2. Искусственные угрозы (вызванные деятельностью человека: внедрение агентов в число персонала системы; подкуп, шантаж и т.п. персонала или отдельных пользователей; несанкционированного копирования секретных данных; разглашение, передача или утрата паролей, ключей шифрования, идентификационных карточек, пропусков и т.п. ).

2. *По степени преднамеренности проявления*. .

2.1. Угрозы случайного действия и/или угрозы, вызванные ошибками или халатностью персонала (проявление ошибок программно-аппаратных средств АС; некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности; неумышленная порча оборудования, удаление, искажение файлов с важной информацией или программ, в том числе системных и т.п.);

2.2. Угрозы преднамеренного действия (угрозы действий злоумышленника для хищения информации).

3. *По положению источника угроз*.

3.1. Угрозы, источник которых расположен вне контролируемой зоны территории (помещения), на которой находится АС. (перехват побочных электромагнитных, акустических и других излучений устройств и линий связи, дистанционная фото- и видеосъемка).

3.2. Угрозы, источник которых расположен в пределах контролируемой зоны территории (помещения), на которой находится АС. ( хищение производственных отходов (распечаток, записей, списанных носителей информации и т.п; отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т.д.); применение подслушивающих устройств).

3.3. Угрозы, источник которых имеет доступ к периферийным устройствам АС (терминалам).

3.4. Угрозы, источник которых расположен в АС. (проектирование архитектуры системы и технологии обработки данных, разработка прикладных программ, которые представляют опасность для работоспособности системы и безопасности информации; некорректное использование ресурсов АС).

**4. По степени зависимости от активности АС.**

4.1. Угрозы, которые могут проявляться независимо от активности АС.(вскрытие шифров криптозащиты информации; хищение магнитных дисков, лент, микросхем памяти, запоминающих устройств и компьютерных систем).

4.2. Угрозы, которые могут проявляться только в процессе автоматизированной обработки данных (например, угрозы выполнения и распространения программных вирусов).

5. *По степени воздействия на АС.*

5.1. Пассивные угрозы, которые при реализации ничего не меняют в структуре и содержании АС (например, угроза копирования секретных данных).

5.2. Активные угрозы, которые при воздействии вносят изменения в структуру и содержание АС. (Например, внедрение "закладок" и "вирусов"; изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных радиопомех на частотах работы устройств системы и т.п.)

6. *По этапам доступа пользователей или программ к ресурсам АС.*

6.1. Угрозы, которые могут проявляться на этапе доступа к ресурсам АС (например, угрозы несанкционированного доступа в АС).

6.2. Угрозы, которые могут проявляться после разрешения доступа к ресурсам АС (например, угрозы несанкционированного или некорректного использования ресурсов АС).

7. *По способу доступа к ресурсам АС.*

7.1. Угрозы, направленные на использование прямого стандартного пути

доступа к ресурсам АС. (незаконное получение паролей и других реквизитов разграничения доступа; несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики)

7.2. Угрозы, направленные на использование скрытого нестандартного пути доступа к ресурсам АС (вход в систему в обход средств защиты (загрузка посторонней операционной системы со сменных магнитных носителей и т.п.); доступ к ресурсам АС путем использования недокументированных возможностей ОС).

8. *По текущему месту расположения информации, хранимой и обрабатываемой в АС.*

8.1. Угрозы доступа к информации на внешних запоминающих устройствах (например, угроза несанкционированного копирования секретной информации с жесткого диска). 8.2. Угрозы доступа к информации в оперативной памяти. ( чтение остаточной информации из оперативной памяти; угроза доступа к системной области оперативной памяти со стороны прикладных программ.)

8.3. Угрозы доступа к информации, циркулирующей в линиях связи. (незаконное подключение к линиям связи с целью подмены законного пользователя путем его физического отключения после входа в систему и успешной аутентификации с

последующим вводом дезинформации и навязыванием ложных сообщений; перехват всего потока данных с целью дальнейшего анализа не в реальном масштабе времени).

8.4. Угрозы доступа к информации, отображаемой на терминале или печатаемой на принтере (например, угроза записи отображаемой информации на скрытую видеокамеру).

Вне зависимости от конкретных видов угроз или их проблемно-ориентированной классификации АС удовлетворяет потребности эксплуатирующих ее лиц, если обеспечиваются ликвидированы три основные угрозы (конфиденциальности, целостности и доступности).

### 1.4. Структура теории информационной безопасности

#### Основные уровни защиты информации

При рассмотрении вопросов защиты АС обычно используют четырехуровневую градацию доступа к хранимой, обрабатываемой и защищаемой АС информации. Это позволяет систематизировать и обобщить весь спектр методов обеспечения защиты, относящихся к информационной безопасности. Перечислим основные уровни защиты информации:

- уровень носителей информации;
- уровень средств взаимодействия с носителем;
- уровень представления информации;
- уровень содержания информации.

Данные уровни были введены по следующим соображениям: во-первых, информация для удобства манипулирования чаще всего фиксируется на некотором материальном носителе, которым может быть бумага, дискета или что-нибудь в этом роде. Во-вторых, если способ представления информации таков, что она не может быть непосредственно воспринята человеком, возникает необходимость в преобразователях информации в доступный для человека способ представления.

#### Защита магнитных носителей информации (МНИ)

Проблема защиты машинных носителей информации (МНИ) в АС, решается в основном за счет организационно-режимных мер, делающих невозможным или существенно ограничивающим доступ злоумышленников к МНИ и документальным материалам АС. Одним из наиболее надежных подходов к защите НИИ является их физическая защита. В то же время защита МНИ имеет специфику, определяемую их реализацией и организацией.

Независимо от типа носителя, данные на носителях хранятся блоками (секторами, кластерами и т.п.). Как известно, для доступа к данным МНИ существуют два основных способа:

- последовательный доступ, когда блоки записываются друг за другом и

для чтения следующего нужно пройти все предыдущие;

- прямой (произвольный) доступ, отличающийся тем, что блоки записываются и читаются в произвольном порядке.

Например, дисковые накопители являются устройствами произвольного доступа, накопители на магнитной ленте - последовательного доступа. Кроме этого, МНИ характеризуются:

- различными физическими принципами реализации;
- широким спектром объемов хранимой информации - от единиц до десятков тысяч мегабайт;
- многообразием конкретных реализаций носителей различными производителями.

Злоумышленник не может получить доступ к информации на машинном носителе в двух случаях:

1. когда злоумышленнику недоступен сам носитель;

2. когда злоумышленнику доступен носитель, но отсутствуют соответствующие средства взаимодействия с носителем.

Основными задачами обеспечения информационной безопасности АС от угрозы раскрытия конфиденциальности на уровне МНИ являются:

1. исключение прохождения носителей по технологическим участкам, не обусловленным производственной необходимостью;

2. предупреждение непосредственного доступа к носителям персонала, не отвечающего за операции с носителями (минимизация доступа), предупреждение утраты или хищения носителей информации.

Первая задача решается за счет рациональной организации производственного процесса движения носителей информации, обеспечивающего целенаправленное распределение носителей по технологическим участкам, вторая - за счет четкой и обоснованной регламентации порядка обращения с носителями.

При обеспечении сохранности информационных ресурсов персональных компьютеров многое зависит от выбора методов защиты информации на гибких, магнитных дисках (дискетах) от несанкционированного копирования.

Помимо классического изменения структуры дискеты (привязки к временным параметрам чтения и записи, нестандартной разметки дорожек и изменения межсекторной дистанции) можно предложить использовать методы кодирования информации, хранящейся на гибком диске, в соответствии с алгоритмом криптографического преобразования по ГОСТу 28147-89.

Алгоритм криптографического преобразования предназначен для аппаратной или программной реализации, удовлетворяет криптографическим требованиям, а его возможности не накладывают ограничений на применение. Устанавливая единый алгоритм криптографического преобразования для систем обработки информации, он определяет правила шифрования данных и выработки имитоприставки и рекомендован для организаций, предприятий и учреждений, применяющих криптографическую защиту информации, хранимой и передаваемой в сетях ЭВМ, в отдельных вычислительных комплексах или отдельных компьютерах.

Режим гаммирования[1] с обратной связью был выбран как обеспечивающий наибольшую криптостойкость системы: в результате сцепления блоков информации

изменение одного бита во входном информационном потоке приводит к изменению всего выходного потока, так как кодирование каждого блока информации зависит от кодирования предыдущего блока.

Для более ясного понимания сути метода защиты информации на гибких магнитных дисках от копирования рассмотрим отличия стандартной структуры дискеты и структуры, реализованной в данном методе.

На стандартной дискете после форматирования можно выделить четыре основные области, а именно: загрузочный сектор (boot area), область таблицы размещения файлов (FAT area), корневой каталог (directory area) и область данных (data area). Загрузочный сектор всегда является первым сектором на дискете, именно сюда записывается информация

---

[1] Во второй половине XIX в. появился весьма устойчивый способ усложнения числовых кодов - *гаммирование.* Он заключался в перешифровании закодированного сообщения с помощью некоторого ключевого числа, которое и называлось *гаммой.* Шифрование с помощью гаммы состояло в сложении всех кодированных групп сообщения с одним и тем же ключевым числом. Эту операцию стали называть *"наложениемгаммы".* Например, результатом наложения гаммы 6413 на кодированный текст 3425 71028139 являлась числовая последовательность 9838 3515 4552:

3425 7102 8139
\+ 6413 6413 6413
9838 3515 4552

Единицы переноса, появляющиеся при сложении между кодовыми группами, опускались. *"Снятие гаммы"* являлось обратной операцией:

9838 3515 4552
\- 6413 6413 6413
3425 7102 8139

в 1888 г. француз маркиз де Виари в одной из своих научных статей, посвященных криптографии, обозначил греческой буквой Х любую букву шифрованного текста, греческой буквой Г любую букву гаммы и строчной буквой *с* любую букву открытого текста. Он, по сути, *доказал,* что алгебраическая формула

x = (c+r)mod26

воспроизводит зашифрование по Виженеру при замене букв алфавита числами согласно следующей таблице: (в таблице каждой букве латинского алфавита соответствовала цифра совподающая с порядковым номером буквы в алф.).

Тем самым была заложена алгебраическая основа для исследования шифров замены типа шифра Виженера. Используя уравнение шифрования, можно было отказаться от громоздкой таблицы Виженера.

Позже лозунговая гамма стала произвольной последовательностью, а шифр с уравнением шифрования (1) стал называться *шифром гаммирования.*

о том, как организована дискета. За счет этого операционная система позволяет работать с большим набором по-разному организованных гибких дисков.

Назначение некоторых байтов загрузочного сектора, которые описывают организацию дискеты, приведены ниже:

11-12 байты — число байтов в секторе;

13 байт — число секторов в кластере;

14-15 байты — число резервных секторов;

16 байт — число копий FAT;

17-18 байты — число позиций в корневом каталоге;

19-20 байты — число секторов на диске;

21 байт — код типа диска.

Следующая важная область — FAT, в которой операционная система назначает секторы для размещения различных файлов. Здесь для каждого сектора имеется своя запись, содержащая информацию о том, занят сектор файлом или нет, если да, то каким именно, а также указывается информация о поврежденных секторах.

Размер таблицы размещения файлов зависит от размера диска: чем выше его емкость, тем больший размер должен быть у таблицы для хранения информации обо всех секторах диска. Для большей надежности подобных таблиц может быть несколько (обычно для стандартной дискеты 3,5" емкостью 1,44 Мб их две).

В корневом каталоге хранится информация о файлах, каталогах, времени и дате их создания, размерах и другие необходимые сведения. Каждой позиции каталога отводится 32 байта, назначение которых приведено ниже:

1-8 — имя файла;

9—11 байты — расширение имени;

12 байт — атрибуты файла;

13-22 байты — в резерве операционной системы;

23-24 байты — время создания;

25-26 байты — дата создания;

27-28 байты — начальный кластер;

29-32 байты — размер файла.

Все остальное дисковое пространство является областью данных, в которой хранится информация.

Использование метода защиты информации на гибких магнитных дисках от копирования подразумевает создание структуры дискеты, отличной от стандартной.

При форматировании дискеты создаются следующие разделы: системная область и область данных. В системной области указывается размер файла в байтах, его имя и расширение, пароль, с которым данный файл был зашифрован, информация о порядке расположения секторов и поврежденных секторах. Системная область и область с данными хранятся в зашифрованном виде.

На стандартных дискетах DOS при записи файлов формирует таблицу их размещения, в которой указывается последовательность расположения секторов для каждого файла. Применение классического метода изменения параметров дисковода пресекает возможность просмотра дискеты обычными средствами, которые работают со стандартными форматами дискет, в результате чего такую дискету нельзя скопировать без специальных программ.

Применяя программу DISK EXPLORER, можно проанализировать логическую структуру дискеты и, прочитав каждый сектор, сделать отдельные копии секторов, находящихся на дискете после изменения параметров дисковода. Но получение полного объема информации в этом случае не представляется возможным, поскольку последовательность расположения секторов с данными пользователю не известна, а определение нужной последовательности потребует перебора множества комбинаций. К тому же каждый сектор кодирован в режиме гаммирования с обратной связью, и его декодирование будет зависеть от декодирования предыдущего сектора.

Для того чтобы изменить режим работы дисковода, необходимо модифицировать содержимое определенных ячеек оперативной памяти. По адресу 0000h:0078h находится указание на таблицу данных, которые используются контроллером дисковода при работе с дискетой, и изменение этих параметров позволит работать с нестандартными форматами дискет.

В данном методе используется форматирование с параметрами, отличающимися для каждого сектора. Два сектора используются для хранения системной информации (размер, полное имя файла, данные о порядке следования секторов и поврежденных секторах, пароль, с которым был зашифрован файл).

Во время форматирования проверяется качество записи и считывания сектора, так как из-за потенциального наличия на дискете поврежденных секторов на ней может измениться допустимый объем. После этого вычисляется свободный объем на диске и сверяется с размером записываемого файла.

При восстановлении файла у пользователя запрашивается пароль, посредством которого декодируется системная область и проверяется пароль, полученный в процессе декодирования. При несовпадении работа завершается. В случае положительного результата выставляются новые параметры для дисковода, и происходит декодирование файла, записанного на диск.

Основным преимуществом разработанного метода является высокая криптографическая стойкость информации, записываемой на гибкий магнитный диск, которая достигается благодаря применению алгоритма криптографического преобразования, основанного на ГОСТе 28147-89. Применение согласно этому ГОСТу дополнительного режима выработки имитоприставки обеспечивает защиту находящейся на диске информации от изменений и имитации.

По сравнению с существующими стандартными программами для персональных компьютеров время чтения и записи сокращено в них на 10 %.

Особое внимание следует уделять любым носителям информации, покидающим пределы фирмы. Наиболее частыми причинами этого бывают ремонт аппаратуры и списание технологически устаревшей техники. Необходимо помнить, что на рабочих поверхностях носителей даже в удаленных областях находится информация, которая может представлять либо непосредственный интерес, либо косвенно послужить причиной вторжения в систему. Так, например, при использовании виртуальной памяти часть содержимого ОЗУ записывается на жесткий диск, что теоретически может привезти даже к сохранению пароля на постоянном носителе (хотя это и маловероятно). Ремонт, производимый сторонними фирмами на месте, должен производится под контролем инженера из службы информационной безопасности. Необходимо помнить, что при нынешнем быстродействии ЭВМ копирование файлов производится со скоростью, превышающей мегабайт в секунду, а установить второй жесткий диск для копирования в момент ремонта без надзора специалиста можно практически незаметно. Все носители информации, покидающие фирму должны надежно чиститься либо уничтожаться механически (в зависимости от дальнейших целей их использования).

И еще немного слов о защищенности самих носителей информации. На сегодняшний день не существует разумных по критерию «цена/надежность» носителей информации, не доступных к взлому. Строение файлов, их заголовки и расположение в любой операционной системе может быть прочитано при использовании соответствующего программного обеспечения. Практически невскрываемым может быть только энергонезависимый носитель, автоматически разрушающий информацию при попытке несанкционированного подключения к любым точкам, кроме разрешенных разъемов, желательно саморазрушающийся при разгерметизации, имеющий внутри микропроцессор, анализирующий пароль по схеме без открытой передачи. Однако, все это из области «сумасшедших» цен и военных технологий.

Для бизнес класса и частной переписки данная проблема решается гораздо проще и дешевле – с помощью криптографии. Любой объем информации от байта до гигабайта, будучи зашифрован с помощью более или менее стойкой криптосистемы, недоступен для

прочтения без знания ключа. И уже совершенно не важно, хранится он на жестком диске, на дискете или компакт-диске, не важно под управлением какой операционной системы. Против самых новейших технологий и миллионных расходов здесь стоит математика, и этот барьер до сих пор невозможно преодолеть. Вот почему силовые ведомства практически всех стран, будучи не в состоянии противостоять законам математики, применяют административные меры против так называемой стойкой криптографии. Вот почему ее использование частными и юридическими лицами без лицензии Федерального агентства по связи и информации (ФАПСИ), входящего в структуру одного из силовых ведомств государства, запрещено и у нас в России.

### 1.5. Основные виды атак на АС

Атака на компьютерную систему – это действие, предпринятое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости.

Основные виды атак:

1. *Вмешательство человека в работу АС*. К этому виду относятся организационные средства нарушения безопасности АС (кража носителей информации, несанкционированный доступ (НСД) к устройствам хранения и обработки информации, порча оборудования и т.д.) и осуществление нарушителем НСД к программным компонентам АС ( все способы НСД в АС, а также способы получения нарушителем незаконных прав доступа к компонентам АС). Меры, противостоящие таким атакам, носят организационный характер (охрана, режим доступа к АС), а также включает в себя совершенствование систем обнаружения попыток атак (попыток подбора паролей).

2. *Аппаратно–техническое вмешательство в работу АС*. Т.е. нарушение безопасности и целостности информации в АС с помощью технических средств, например, получение информации по электромагнитному излучению устройств АС. Защита от таких угроз, кроме организационных мер, предусматривает соответствующие аппаратные (экранирование излучений аппаратуры) и программные меры (шифрация).

3. *Разрушающее воздействие на программные компоненты АС с помощью программных средств* (разрушающих программных средств (РПС)). К ним относятся компьютерные вирусы, троянские кони, закладки, «логическая бомба», «часовая мина». Средства борьбы с подобными атаками программно реализованных средств защиты.

Последний вид атак развивается более динамично, используя все последние достижения в области информационных достижений. Остановимся на нем более детально и дадим краткое описания некоторых РПС.

*«Логические бомбы»* и *«часовые мины»* - Это РПС, которые не выполняют никаких функций до наступления определенного события в системе, после чего «срабатывают», что,

как правило, заключается в серьезных нарушениях работы системы, уничтожении информации.

*«Троянский конь»* - программа, содержащая в себе некоторую разрушающую функцию, которая активизируется при наступлении некоторого условного срабатывания. Обычно такие программы маскируются под какие – нибудь полезные утилиты, игровые программы, картинки или музыку.

Закладки также содержат некоторую функцию, наносящую ущерб АС, но эта функция, наоборот, старается быть как можно незаметнее, т.к. чем дольше программа не будет вызывать подозрений, тем дольше закладка сможет работать.

В качестве примера приведем некоторые функции, реализуемые троянскими конями и закладками:

1. Уничтожение информации. Конкретный выбор объектов и способов уничтожения зависит от фантазии автора такой программы и возможностей ОС
2. Перехват и передача информации.
3. Целенаправленная модификация кода программы, интересующая нарушителя. Обычно это программы, реализующие функции безопасности и защиты.

*Компьютерный вирус* – программа, которая может заражать другие программы, модифицируя их посредством добавления своей, возможно измененной, копии. Способен к саморазмножению, при этом «копии» вируса могут структурно и функционально различаться между собой.

В настоящее время в мире насчитывается более 40 тысяч только зарегистрированных компьютерных вирусов. Все компьютерные вирусы могут быть классифицированы по следующим признакам:

1. по среде обитания;
2. по способу заражения;
3. по степени опасности деструктивных (вредительских) воздействий;
4. по алгоритму функционирования.

По среде обитания вирусы делятся так же на:

1. сетевые;
2. файловые;
3. загрузочные;
4. комбинированные;

Средой обитания сетевых вирусов являются элементы компьютерных сетей. Файловые вирусы размещаются в исполняемых файлах. Загрузочные вирусы находятся в загрузочных секторах (областях) внешних запоминающих устройств (boot - секторах). Комбинированные вирусы размещаются в нескольких средах обитания. Примером таких вирусов служат

загрузочные файловые вирусы. Эти вирусы могут размещаться как в загрузочных секторах накопителей на магнитных дисках, так и в теле загрузочных файлов.

По способу заражения среды обитания компьютерные вирусы делятся на:

1. резидентные;
2. нерезидентные.

*Резидентные вирусы* после их активации полностью или частично перемещаются из среды обитания (сеть, загрузочный сектор, файл) в оперативную память ЭВМ. Эти вирусы, используя привилегированные режимы работы, разрешенные только операционной системе, заражают среду обитания и при выполнении определенных условий реализуют деструктивную функцию. *Нерезидентные вирусы* попадают в оперативную память ЭВМ только на время их активности, в течение которого выполняют вредительскую функцию и функцию заражения. Затем вирусы полностью покидают оперативную память, оставаясь в среде обитания. Если вирус помещает в оперативную память программу, которая не заражает среду обитания, то такой вирус считается нерезидентным.

Арсенал вредительских возможностей вирусов весьма обширен. Деструктивные возможности вирусов зависят от целей и квалификации их создателя, а так же от особенностей компьютерных систем.

По степени опасности для информационных ресурсов пользователя компьютерные вирусы делятся на:

1. безвредные вирусы;
2. опасные вирусы;
3. очень опасные вирусы.

*Безвредные вирусы* создаются авторами, которые не ставят себе цели нанести какой – либо ущерб ресурсам компьютерной системы (АС). Деструктивное воздействие таких вирусов сводиться к выводу на экран монитора невинных картинок, исполнению музыкальных фрагментов. Но при всей своей безобидности они расходуют ресурсы системы, в какой – то степени снижая эффективность функционирования, могут содержать ошибки, приводящие к нарушению алгоритма работы системы.

К *опасным* относятся вирусы, которые вызывают существенное снижение эффективности АС, но не приводящие к нарушению целостности и конфиденциальности информации, хранящейся в запоминающих устройствах. В пример можно привести вирусы, вызывающие необходимость повторного выполнения программ, перезагрузки операционной системы.

*Очень опасными* следует считать вирусы, вызывающие нарушение конфиденциальности, уничтожение, необратимую модификацию информации, а так же вирусы, блокирующие доступ к информации, приводящие к отказу аппаратных средств.

Одним из основных условий безопасной работы АС является соблюдение ряда правил.

Правило 1: периодически обновляйте вашу антивирусную программу

Антивирусные сканеры способны защищать только от тех компьютерных вирусов, данные о которых содержатся в антивирусной базе. Конечно, существуют механизмы поиска и неизвестных вирусов (т.е. тех, описаний которых нет в антивирусной базе).. Однако это все равно слишком мало для того, чтобы считаться абсолютной защитой.

В связи с этим первоочередную важность приобретает необходимость регулярно обновлять антивирусные базы. Чем чаще будете это делаться, тем более защищенным будет рабочее место. Наиболее оптимальным решением является ежедневная загрузка обновлений, хотя бывают случаи, когда за день появляется сразу несколько обновлений. В связи с этим, рекомендуют настроить внутренний планировщик, присутствующий в большинстве современных антивирусных программ, на автоматическую загрузку обновлений 2 или 3 раза в день: утром, днем и вечером.

*Правило 2: будьте осторожны с файлами в письмах электронной почты*

Вряд ли стоит акцентировать внимание на том, что ни в коем случае нельзя запускать программы, присланные неизвестным лицом. Это правило является общеизвестным и не нуждается в пояснениях.

Другое дело файлы, полученные от знакомых, коллег, друзей. Во-первых, посланные ими программы могут быть инфицированы. Во-вторых, знакомые могут даже и не знать, что с их компьютера несанкционированно отправляются письма: вирус может это делать от чужого имени незаметно для владельца компьютера! Именно таким способом, к примеру, распространялись такие известные вирусы, как LoveLetter, Melissa и многие другие. Они незаметно получали доступ к адресной книге почтовой программы Outlook и рассылали свои копии по найденным адресам электронной почты, сопровождая послания завлекательными комментариями, призывающими запустить вложенный файл.

Не менее важным моментом является кажущаяся безопасность вложенных файлов определенного формата. Думаете, файлы с расширением PIF, GIF, TXT не могут содержать вредоносных программ? Даже в таких «безобидных» программах могут быть замаскированы вирусы.

*Правило 3: ограничьте круг пользующихся компьютером*

Идеальным вариантом является ситуация, когда никто, кроме самого владельца, не имеет доступа к компьютеру. Однако если это невозможно, то необходимо четко разграничить права доступа и определить круг разрешенных действий для других лиц. В первую очередь это касается работы с мобильными носителями, Интернет и электронной почтой. В данном случае важно контролировать все источники вирусной опасности и отрезать от них других пользователей.

*Правило 4: своевременно устанавливайте «заплатки» установленному ПО*

Многие вирусы используют “дыры” в системах защиты операционных систем и приложений. Антивирусные программы способны защищать от такого типа вредоносных программ, даже если на компьютере не установлена соответствующая “заплатка”, закрывающая “дыру”. Несмотря на это, рекомендуется регулярно проверять Web-сайты производителей установленного программного обеспечения и следить за выпуском новых “заплаток”. В первую очередь, это правило относится к операционной системе Windows и другим программам корпорации Microsoft. Нет, совсем не потому, что у этой компании самые худшие продукты, а потому, что они наиболее распространены и, соответственно, получают больше всего внимания со стороны создателей вирусов.

*Правило 5: обязательно проверяйте мобильные носители информации*

Несмотря на то, что около 85% всех зарегистрированных случаев заражения компьютерными вирусами приходятся на электронную почту и Интернет, не стоит забывать о таком традиционном способе транспортировки вредоносных кодов, как мобильные носители (дискеты, компакт-диски и т.п.). Перед тем, как начать их использовать на своем компьютере, необходимо тщательно проверить их антивирусной программой. Исключением могут быть разве что диски, предназначенные для форматирования.

Большую опасность представляют собой и столь широко распространенные в России пиратские компакт-диски. К примеру, проверка, проведенная «Лабораторией Касперского» в 1999 году, выявила факт присутствия вирусов на 23% закупленных носителей. Вывод прост: тщательно проверять даже приобретенные компакт-диски.

*Правило 6: будьте осторожны с источниками, заслуживающими доверия*

Как любви подвластны все возрасты, так же никто не застрахован от компьютерных вирусов. Это в равной мере относится к крупным компаниям-производителям программного и аппаратного обеспечения. Нередко случается, что посетителям их сайтов предлагаются зараженные программы. Показательный случай, когда в течение нескольких недель на сайте Microsoft находился документ Word, зараженный макро-вирусом Concept.

Не менее редки случаи присутствия вирусов на дискетах с драйверами к аппаратному обеспечению, с лицензионным программным обеспечением. Часто случается, что компьютер, переданный на техническое обслуживание в ремонтную мастерскую, возвращается не совсем чистым. Не то чтобы на мониторе был толстый слой пыли, а на клавиатуре паутина (хотя такое тоже случается), а просто на диске заводятся вирусы. Как правило, это происходит из-за того, что ремонтники пользуются одними и теми же дискетами для загрузки программ для тестирования различных узлов компьютера. Таким образом, они очень быстро переносят компьютерную «заразу» с одних компьютеров на

другие. Вывод состоит в том, что, получив компьютер из ремонта, не забудьте тщательно проверить его на наличие вирусов.

Все это делает необходимым проверять даже те данные, которые получены из источников, заслуживающих доверия. Вряд ли в данном случае стоит обвинять самих производителей, что они якобы нарочно стараются заразить компьютер: в каждой работе бывают осечки. Просто иногда они касаются и антивирусной безопасности.

*Правило 7: сочетайте разные антивирусные технологии*

Не стоит ограничиваться классическим антивирусным сканером, запускаемым по требованию пользователя или при помощи встроенного планировщика событий. Существует ряд других, нередко более эффективных технологий, комбинированное использование которых способно практически гарантировать безопасную работу. К числу таких технологий относятся: во-первых, антивирусный монитор, постоянно присутствующий в памяти компьютера и проверяющий все используемые файлы в масштабе реального времени, в момент доступа к ним; во-вторых, ревизор изменений, который отслеживает все изменения на диске и немедленно сообщает, если в каком-либо из файлов поселился вирус; в-третьих, поведенческий блокиратор, обнаруживающий вирусы не по их уникальному коду, а по последовательности их действий. Сочетание описанных способов борьбы с вирусами является залогом успешной защиты от вредоносных программ.

*Правило 8: всегда имейте при себе чистый загрузочный диск*

Часто происходит так, что вирусы лишают компьютеры возможности производить первоначальную загрузку. Иными словами, информация на диске остается в целости и сохранности, но операционная система теряет способность загружаться. Для успешного разрешения подобных проблем необходимо иметь специальную чистую дискету с установленной антивирусной программой. С ее помощью Вы сможете произвести загрузку и восстановить систему.

*Правило 9: регулярное резервное копирование*

Это правило поможет  сохранить данные не только в случае поражения компьютера каким-либо вирусом, но и в случае, если у  компьютера произошла серьезная поломка в аппаратной части. Вряд ли кому-то хочется потерять результаты многолетних наработок вследствие произошедшего сбоя в системе вне зависимости от того, вызвано это вирусами или нет. Именно поэтому рекомендуют регулярно проводить копирование наиболее ценной информации на независимые носители: дискеты, магнитооптические диски, магнитные ленты, компакт-диски.

*Правило 10: не паникуйте!*

Вирусы являются такими же программами, как, допустим, калькулятор или записная книжка Windows. Их отличительная черта в том, что вирусы способны размножаться (т.е.

создавать свои копии), интегрироваться в другие файлы или загрузочные секторы и производить другие несанкционированные действия. Вирусы создаются самыми обычными людьми, и ничего потустороннего в них нет. Гораздо больший вред сможете принести, если испугаетесь и совершите необдуманные действия, направленные на нейтрализацию вируса. Если работаете в корпоративной сети, немедленно позовите системного администратора. Если же просто домашний пользователь, то свяжитесь с компанией, у которой приобрели антивирусную программу. Дайте возможность профессионалам позаботиться о вашей безопасности. В конце концов, они за это получают деньги.

Существует еще один вид атаки, встречающийся в литературе под названием *«атака по социальной психологии».* Сделаем краткий обзор нескольких довольно часто встречающихся методов.

Звонок администратору – злоумышленник выбирает из списка сотрудников того, кто не использовал пароль для входа в течение нескольких дней (отпуск, отгулы, командировка) и кого администратор не знает по голосу. Затем следует звонок с объяснением ситуации о забытом пароле, искренние извинения, просьба зачитать пароль, либо сменить его на новый. Больше чем в половине случаев просьба будет удовлетворена, а факт подмены будет замечен либо с первой неудачной попыткой зарегистрироваться истинного сотрудника, либо по произведенному злоумышленником ущербу.

Почти такая же схема, но в обратную сторону может быть разыграна злоумышленником в адрес сотрудника фирмы – звонок от администратора. В этом случае он представляется уже сотрудником службы информационной безопасности и просит назвать пароль либо из-за произошедшего сбоя в базе данных, либо якобы для подтверждения личности самого сотрудника по какой-либо причине (рассылка особо важных новостей), либо по поводу последнего подключения сотрудника к какому-либо информационному серверу внутри фирмы. Фантазия в этом случае может придумывать самые правдоподобные причины, по которым сотруднику «просто необходимо» вслух назвать пароль. Самое неприятное в этой схеме то, что если причина запроса пароля придумана, что называется "с умом", то сотрудник повторно позвонит в службу информационной безопасности только через неделю, месяц, если вообще это произойдет. Кроме того, данная схема может быть проведена и без телефонного звонка – по электронной почте, что неоднократно и исполнялось якобы от имени почтовых и Web-серверов в сети Интернет.

В качестве программных профилактических мер используются экранные заставки с паролем, появляющиеся через 5-10 минут отсутствия рабочей активности, автоматическое отключение клиента через такой же промежуток времени.

## 2. Методология построения систем защиты АС

### 2.1. Построение системы защиты от угрозы нарушения конфиденциальности информации

Функционирование комплексной системы защиты информации (АСЗИ) зависит не только от характеристик созданной системы, но и от эффективности ее использования на этапе эксплуатации АС. Основными этапами эксплуатации является максимальное использование возможностей АСЗИ, заложенных в систему при построении, и совершенствование ее защитных функций в соответствии с изменяющимися условиями.

Процесс эксплуатации АСЗИ можно разделить на применение системы по прямому назначению, непосредственно связанных с защитой информации в АС, и техническую эксплуатацию. Применение по назначению предусматривает организацию доступа к ресурсам АС и обеспечение их целостности.

Под организацией доступа к ресурсам понимается весь комплекс мер, который выполняется в процессе эксплуатации системы для предотвращения несанкционированного воздействия на технические и программные средства, а так же информацию.

Организация доступа к ресурсам предполагает:

1. разграничение прав пользователей и обслуживающего персонала по доступу к ресурсам АС в соответствии с функциональными обязанностями должностных лиц;
2. организацию работы с конфиденциальными информационными ресурсами на объекте;
3. защиту от технических средств разведки;
4. охрану объекта;
5. эксплуатацию системы разграничения доступа.

Система разграничения доступа (СРД) является одной из основных составляющих АСЗИ. В этой системе можно выделить следующие компоненты:

1. средства аутентификации субъекта доступа;
2. средства разграничения доступа к техническим устройствам АС;
3. средства разграничения доступа к программам и данным;
4. средства блокировки неправомочных действий;
5. средства регистрации событий;
6. дежурный оператор системы разграничения доступа.

Согласно руководящим документам Гостехкомиссии под несанкционированным доступом к информации (НСД) будем понимать доступ к информации, нарушающий установленные правила разграничения доступа и осуществляемый с использованием штатных средств АС. НСД может носить случайный или преднамеренный характер.

Можно выделить несколько обобщенных категорий методов защиты от НСД, в частности:

- организационные;
- технологические;
- правовые.

К первой категории относятся меры и мероприятия, регламентируемые внутренними инструкциями организации, эксплуатирующей информационную систему. Пример такой защиты - присвоение грифов секретности документам и материалам, хранящимся в отдельном помещении, и контроль доступа к ним сотрудников. Вторую категорию составляют механизмы защиты, реализуемые на базе программно-аппаратных средств, например систем идентификации и аутентификации или охранной сигнализации. Последняя категория включает меры контроля за исполнением нормативных актов общегосударственного значения, механизмы разработки и совершенствования нормативной базы, регулирующей вопросы защиты информации.

Рассмотрим подробнее такие взаимосвязанные методы защиты от НСД, как идентификация, аутентификация и используемое при их реализации криптографическое преобразование информации.

*Идентификация* - это присвоение пользователям идентификаторов (понятие идентификатора будет определено ниже) и проверка предъявляемых идентификаторов по списку присвоенных.

*Аутентификация* - это проверка принадлежности пользователю предъявленного им идентификатора. Часто аутентификацию также называют подтверждением или проверкой подлинности.

Под безопасностью (стойкостью) системы идентификации и аутентификации будем понимать степень обеспечиваемых ею гарантий того, что злоумышленник не способен пройти аутентификацию от имени другого пользователя.

Различают три группы методов аутентификации, основанных на наличии у каждого пользователя:

1. индивидуального объекта заданного типа;
2. знаний некоторой известной только ему и проверяющей стороне ин формации;
3. индивидуальных биометрических характеристик.

К первой группе относятся методы аутентификации, использующие удостоверения, пропуска, магнитные карты и другие носимые устройства, которые широко применяются для контроля доступа в помещения, а также входят в состав программно-аппаратных комплексов защиты от НСД к средствам вычислительной техники.

Во вторую группу входят методы аутентификации, использующие пароли. По экономическим причинам они включаются в качестве базовых средств защиты во многие

программно-аппаратные комплексы защиты информации. Все современные операционные системы и многие приложения имеют встроенные механизмы парольной защиты.

Последнюю группу составляют методы аутентификации, основанные на применении оборудования для измерения и сравнения с эталоном заданных индивидуальных характеристик пользователя: тембра голоса, отпечатков пальцев, структуры радужной оболочки глаза и др.

Если в процедуре аутентификации участвуют только две стороны, устанавливающие подлинность друг друга, такая процедура называется непосредственной аутентификацией (direct password authentication). Если же в процессе аутентификации участвуют не только эти стороны, но и другие, вспомогательные, говорят об аутентификации с участием доверенной стороны (trusted third party authentication). При этом третью сторону называют сервером аутентификации (authentication server) или арбитром (arbitrator).

Наиболее распространенные методы аутентификации основаны на применении многоразовых или одноразовых паролей. Из-за своего широкого распространения и простоты реализации парольные схемы часто в первую очередь становятся мишенью атак злоумышленников. Эти методы включают следующие разновидности способов аутентификации:

1. по хранимой копии пароля или его свёртке (plaintext-equivalent);
2. по некоторому проверочному значению (verifier-based);
3. без непосредственной передачи информации о пароле проверяющей стороне (zero-knowledge);
4. с использованием пароля для получения криптографического ключа (cryptographic).

В первую разновидность способов входят системы аутентификации, предполагающие наличие у обеих сторон копии пароля или его свертки. Для организации таких систем требуется создать и поддерживать базу данных, содержащую пароли или сверки паролей всех пользователей. Их слабой стороной является то, что получение злоумышленником этой базы данных позволяет ему проходить аутентификацию от имени любого пользователя.

Способы, составляющие вторую разновидность, обеспечивают более высокую степень безопасности парольной системы, так как проверочные значения, хотя они и зависят от паролей, не могут быть непосредственно использованы злоумышленником для аутентификации.

Наконец, аутентификация без предоставления проверяющей стороне какой бы то ни было информации о пароле обеспечивает наибольшую степень защиты. Этот способ гарантирует безопасность даже в том случае, если нарушена работа проверяющей стороны (например, в программу регистрации в системе внедрен «троянский конь»).

Особым подходом в технологии проверки подлинности являются криптографические

протоколы аутентификации. Такие протоколы описывают последовательность действий, которую должны совершить стороны для взаимной аутентификации, кроме того, эти действия, как правило, сочетаются с генерацией и распределением криптографических ключей для шифрования последующего информационного обмена. Корректность протоколов аутентификации вытекает из свойств задействованных в них математических и криптографических преобразований и может быть строго доказана.

Обычные парольные системы проще и дешевле для реализации, но менее безопасны, чем системы с криптографическими протоколами. Последние обеспечивают более надежную защиту и дополнительно решают задачу распределения ключей. Однако используемые в них технологии могут быть объектом законодательных ограничений.

Для более детального рассмотрения принципов построения парольных систем сформулируем несколько основных определений.

Идентификатор пользователя - некоторое уникальное количество информации, позволяющее различать индивидуальных пользователей парольной системы (проводить их идентификацию). Часто идентификатор также называют именем пользователя или именем учетной записи пользователя.

Пароль пользователя - некоторое секретное количество информации, известное только пользователю и парольной системе, которое может быть запомнено пользователем и предъявлено для прохождения процедуры аутентификации. Одноразовый пароль дает возможность пользователю однократно пройти аутентификацию. Многоразовый пароль может быть использован для проверки подлинности повторно.

Учетная запись пользователя-совокупность его идентификатора и его пароля.

База данных пользователей парольной системы содержит учетные записи всех пользователей данной парольной системы.

Под парольной системой будем понимать программно-аппаратный комплекс, реализующий системы идентификации и аутентификации пользователей АС на основе одноразовых или многоразовых паролей. Как правило, такой комплекс функционирует совместно с подсистемами разграничения доступа и регистрации событий. В отдельных случай пароль-система может выполнять ряд дополнительных функций, в частности генерацию и распределение кратковременных (сеансовых) криптографических ключей.

Основными компонентами парольной системы являются:

1. интерфейс пользователя;

2. интерфейс администратора;

3.модуль сопряжения с другими подсистемами безопасности;

4. база данных учетных записей.

Ниже перечислены типы угроз безопасности парольных систем.

1. Разглашение параметров учетной записи через:

- подбор в интерактивном режиме;
- подсматривание;
- преднамеренную передачу пароля его владельцем другому лицу;
- захват базы данных парольной системы (если пароли не хранятся в базе в открытом виде, для их восстановления может потрясаться подбор или дешифрование);
- перехват переданной по сети информации о пароле;
- хранение пароля в доступном месте.

2. Вмешательство в функционирование компонентов парольной системы через:

- внедрение программных закладок;
- обнаружение и использование ошибок, допущенных на стадии разработки;
- выведение из строя парольной системы.

Некоторые из перечисленных типов угроз связаны с наличием так называемого человеческого фактора, проявляющегося в том, что пользователь может:

- выбрать пароль, который легко запомнить и также легко подобрать;
- записать пароль, который сложно запомнить, и положить запись в доступном месте;
- ввести пароль так, что его смогут увидеть посторонние;
- передать пароль другому лицу намеренно или под влиянием заблуждения.

Далее рассмотрим криптографические методы защиты, которые в настоящее время являются базовыми для обеспечения надежной аутентификации сторон информационного обмена, защиты информации в транспортной подсистеме АС, подтверждения целостности объектов АС и т.д.

К средствам криптографической защиты информации (СКЗИ) относятся аппаратные, программно-аппаратные и программные средства, реализующие криптографические алгоритмы преобразования информации с целью:

- защиты информации при ее обработке, хранении и передаче по транспортной среде АС;
- обеспечения достоверности и целостности информации (в том числе с использованием алгоритмов цифровой подписи) при ее обработке, хранении и передаче по транспортной среде АС;
- выработки информации, используемой для идентификации и аутентификации субъектов, пользователей и устройств:
- выработки информации, используемой для защиты аутентифицирующих элементов защищенной АС при их выработке, хранении, обработке и передаче.

Отметим несколько существенных особенностей криптографического преобразования:

- в СКЗИ реализован некоторый алгоритм преобразования информации (шифрование, электронная цифровая подпись, контроль целостности и др.);
- входные и выходные аргументы криптографического преобразования присутствуют в АС в некоторой материальной форме (объекты АС);
- СКЗИ для работы использует некоторую конфиденциальную информацию (ключи);
- алгоритм криптографического преобразования реализован в виде некоторого материального объекта, взаимодействующего с окружающей средой (в том числе с субъектами и объектами защищенной АС).

В результате роль СКЗИ в защищенной АС - преобразование объектов.

Существенно важными являются следующие моменты:

1. СКЗИ обменивается информацией с внешней средой, а именно: в него вводятся ключи, открытый текст при шифровании;
2. СКЗИ в случае аппаратной реализации использует элементную базу ограниченной надежности (т.е. в деталях, составляющих СКЗИ, возможны неисправности или отказы);
3. СКЗИ в случае программной реализации выполняется на процессоре ограниченной надежности и в программной среде, содержащей посторонние программы, которые могут повлиять на различные этапы его работы;
4. СКЗИ хранится на материальном носителе (в случае программной реализации) и может быть при хранении преднамеренно или случайно искажено;
5. СКЗИ взаимодействует с внешней средой косвенным образом (питается от электросети, излучает электромагнитные поля и т.д.);
6. СКЗИ изготавливает или/и использует человек, могущий допустить ошибки (преднамеренные или случайные) при разработке и эксплуатации.

Разработчик преднамеренно или непреднамеренно может внести в программу некоторые свойства (например, возможность переключения в отладочный режим с выводом части информации на экран или внешне носители). Эксплуатирующий программу защиты человек может решить, что программа для него "неудобна" и использовать ее неправильно (вводить короткие ключи либо повторять один и тот же ключ для шифрования разных сообщений). То же замечание относится и к аппаратным средствам защиты.

В связи с этим помимо встроенного контроля над пользователем необходимо отслеживать правильность разработки и использования средств защиты с применением организационных мер.

Правильность функционирования технических средств АС, в рамках которых реализовано СКЗИ, определяется как соответствие выполнения элементарных инструкций

(команд) описанному в документации. Ремонт и сервисное обслуживание СКЗИ также не должно приводить к ухудшению свойств СКЗИ в части параметров надежности.

Рассмотрим требования к средам разработки, изготовления и функционирования СКЗИ. Аппаратные средства, на которых реализуются программные или программно-аппаратные СКЗИ, и программно-аппаратная среда (программно-аппаратное окружение), в которой разрабатываются, изготавливаются и эксплуатируются СКЗИ, не должны иметь явных и скрытых функциональных возможностей, позволяющих:

- модифицировать или изменять алгоритм работы СКЗИ в процессе их разработки, изготовления и эксплуатации;
- модифицировать или изменять информационные или управляющие потоки и процессы, связанные с функционированием СКЗИ:
- осуществлять доступ (чтение и модификацию) посторонних лиц (либо управляемых ими процессов) к ключам и идентификационной, и аутентификационной информации;
- получать доступ к конфиденциальной информации СКЗИ.

Состав и назначение программно-аппаратных средств должны быть фиксированы и неизменны в течение всего времени, определенного в заключении о возможности использования.

Возможны два подхода к процессу криптографической защиты (в основном к шифрованию) объектов АС: предварительное и динамическое («прозрачное»).

Предварительное шифрование состоит в зашифровании файла некой программой (субъектом), а затем расшифровании тем же или иным субъектом (для расшифрования может быть применена та же или другая (специально для расшифрования) программа). Далее расшифрованный массив непосредственно используется прикладной программой пользователя. Данный подход имеет ряд недостатков, хотя и применяется достаточно широко.

Принципиальные недостатки метода предварительного шифрования:

- необходимость дополнительного ресурса для работы с зашифрованным объектом (дискового пространства - в случае расшифрования в файл с другим именем, или времени);
- потенциальная возможность доступа со стороны активных субъектов АС к расшифрованному файлу (во время его существования);
- необходимость задачи гарантированного уничтожения расшифрованного файла после его использования.

Сущность динамического шифрования объектов АС состоит в следующем. Происходит зашифрование всего файла (аналогично предварительному шифрованию).

Затем с использованием специальных механизмов обеспечивающих модификацию

функций ПО АС, выполняющего обращения к объектам, ведется работа с зашифрованным объектом. При этом расшифрованию подвергается только та часть объекта, которая в текущий момент времени используется прикладной программой. При записи со стороны прикладной программы происходит зашифрование записываемой части объекта.

Данный подход позволяет максимально экономично использовать вычислительные ресурсы АС, поскольку расшифровывается только та часть объекта, которая непосредственно нужна прикладной программе. Кроме того, на внешних носителях информация всегда хранится в зашифрованном виде, что исключительно ценно с точки зрения невозможность доступа к ней. Динамическое шифрование целесообразно, таким образом, применять для защиты разделяемых удаленных или распределенных объектов АС.

### *2.2. Построение системы защиты от угрозы нарушения целостности*

На этапе эксплуатации АС целостность информации в системе обеспечивается путем:

1. дублирования информации;
2. контроля целостности информации в АС;
3. особой регламентации процессов технического обслуживания;
4. выполнения комплекса антивирусных мероприятий.

Одним из важных условий обеспечения целостности информации в АС является ее дублирование. Стратегия дублирования выбирается с учетом важности информации, трудоемкости восстановления данных.

Простейшим методом контроля целостности является метод контрольных сумм. Для исключения возможности внесения изменений в контролируемый файл с последующей коррекцией контрольной суммы необходимо хранить контрольную сумму в зашифрованном виде или использовать секретный алгоритм вычисления контрольной суммы. Однако более приемлемым методом контроля целостности информации является использование хэш-функции, значение которой невозможно подделать без знания ключа, т.е. использование криптографических приемов.

Для защиты от компьютерных вирусов следует руководствоваться правилами, изложенными в первом разделе.

В силу того, что средства контроля целостности программ и файлов данных, хранимых в АС, должны обеспечивать защиту от несанкционированного изменения, то цифровая (электронная) подпись является одним из часто используемых для решения данной задачи механизмов.

В конце обычного письма или документа исполнитель или ответственное лицо обычно ставит свою подпись. Подобное действие преследует следующие цели. Во-первых,

получатель имеет возможность убедиться в истинности письма, сличив подпись с имеющимся у него образцом. Во-вторых, личная подпись является юридическим гарантом авторства документа. Последний аспект особенно важен при заключении разного рода торговых сделок, составлении доверенностей, обязательств и т.д.

Если подделать подпись человека на бумаге весьма непросто, а установить авторство подписи современными криминалистическими методами - техническая деталь, то с цифровой подписью дело обстоит иначе. Подделать цепочку битов, просто ее скопировав, или незаметно внести нелегальные исправление в документ сможет любой пользователь.

В самой общей модели аутентификации сообщений представлено пять участников. Это отправитель А, получатель В, злоумышленник С, доверенная сторона Д и независимый арбитр Е. Задача отправителя А заключается в формировании и отправке сообщения Т получателю В. Задача получателя В заключается в получении сообщения Т и в установлении его подлинности. Задача доверенной стороны Д является документированная рассылка необходимой служебной информации абонентам вычислительной сети, чтобы в случае возникновения спора между А и В относительно подлинности сообщения представить необходимые документы в арбитраж. Задача независимого арбитра Е заключается в разрешении спора между абонентами А и В относительно подлинности сообщения Т.

Перечислим возможные способы обмана (нарушения подлинности сообщения) при условии, что между участниками модели А, В, С отсутствует кооперация.

*Способ А:* отправитель А заявляет, что он не посылал сообщение Т получателю В, хотя в действительности его посылал (подмена отправленного сообщения или отказ от авторства).

*Способ В1*: получатель В изменяет полученное от отправителя А сообщение Т и заявляет, что данное измененное сообщение он получил от отправителя А (подмена принятого сообщения).

*Способ В2*: получатель в сам формирует сообщение и заявляет, что получил его от отправителя А (имитация принятого сообщения).

*Способ С1:* злоумышленник С искажает сообщение, которое отправитель А передает получателю В (подмена передаваемого сообщения).

*Способ С2:* злоумышленник С формирует и посылает получателю В сообщение Т от имени отправителя А (имитация передаваемого сообщения).

*Способ С3:* злоумышленник С повторяет ранее переданное сообщение, которое отправитель Д посылал получателю В (повтор ранее переданного сообщения).

Термин "цифровая подпись" используется для методов, позволяющих устанавливать подлинность автора сообщения при возникновении за относительно авторства этого сообщения. Как было уже сказано цифровая подпись применяется в информационных системах, в которых отсутствует взаимное доверие сторон (финансовые системы, системы

контроля за соблюдением международных договоров и др.).

Защита от угрозы нарушения целостности информации на уровне содержания в обычной практике рассматривается как защита от дезинформации. Пусть у злоумышленника нет возможности воздействовать на отдельные компоненты АС, находящиеся в пределах контролируемой зоны, но если источники поступающей в нее информации находятся вовне системы, всегда остается возможность взять их под контроль противоборствующей стороной.

Для успешности борьбы с вероятной дезинформацией следует:

• различать факты и мнения;

• применять дублирующие каналы информации;

• исключать все лишние промежуточные звенья и т. п.

### 2.3. Построение системы защиты от угрозы отказа доступа к информации

Поскольку одной из основных задач АС является своевременное обеспечение пользователей системы необходимой информацией (сведениями, данными, управляющими воздействиями и т.п.), то угроза отказа доступа к информации применительно к АС может еще рассматриваться как угроза отказа в обслуживании или угроза отказа функционирования.

На этапе эксплуатации АС доступность информации в системе обеспечивается путем:

1. повышения отказоустойчивости АС;
2. противодействия перегрузкам и «зависания » системы;
3. использование строго определенного множества программ;
4. особой регламентации процессов технического обслуживания и проведения доработок.

Доступность информации поддерживается путем резервирования аппаратных средств, блокировок ошибочных действий людей, использование надежных элементов АС и отказоустойчивых систем. Устраняются так же преднамеренные угрозы перезагрузки элементов системы. Для этого используются механизмы измерения интенсивности поступления заявок на выполнение и механизмы ограничения таких заявок. Должна быть предусмотрена возможность определения причин резкого потока заявок на выполнение программ или передачу информации.

В сложных системах практически не возможно избежать ситуаций, приводящих к «зависаниям» систем или их фрагментов. В результате сбоев аппаратных или программных средств, алгоритмических ошибок, допущенных на этапе разработки, ошибок операторов в системе происходят зацикливания программ, непредусмотренные остановки и другие ситуации, выход из которых возможен лишь путем прерывания вычислительного процесса и последующего его восстановления. На этапе эксплуатации ведется статистика и

осуществляется анализ таких ситуаций. «Зависания» своевременно обнаруживаются, вычислительный процесс восстанавливается.

В защищенной АС должно использоваться только разрешенное программное обеспечение. Контроль состава программного обеспечения осуществляется при плановых проверках комиссиями и должностными лицами, дежурным оператором по определенному плану, неизвестному пользователям.

При прибытии специалистов из других организаций, например, для проведения доработок, кроме обычной проверки лиц, допускаемых на объект, должны проверяться на отсутствие закладок приборы, устройства, которые доставлены для выполнения работ.

Таким образом, надежность функционирования АС может быть сведена к надежности функционирования входящего в ее состав программного обеспечения. И существуют два основных подхода к обеспечению защиты ПО АС от угрозы отказа функционирования - предотвращение неисправностей (fault avoidance) и отказоустойчивость (fault tolerance). Отказоустойчивость предусматривает, что оставшиеся ошибки ПО обнаруживаются во время выполнения программы. Предотвращение неисправностей связано с анализом природы ошибок, возникающих на разных фазах создания ПО, и причин их возникновения.

Рассматривая защиту АС определим еще два уровня: уровень представления и уровень содержания информации.

На уровне представления информации защиту от угрозы отказа доступа к информации (защиту семантического анализа) можно рассматривать как противодействие сопоставлению используемым синтаксическим конструкциям (словам некоторого алфавита, символам и т. п.) определенного смыслового содержания. Применительно к АС задача защиты от угрозы доступности информации может рассматриваться как использование для обработки файла данных программ, обеспечивающих воспроизведение данных в том виде, как они были записаны.

На уровне содержания защита информации от угрозы доступности обеспечивается защитой актуальности информации или легализацией полученных сведений или данных. Применительно к АС защита содержания информации от угрозы блокировки доступа (отказа функционирования) означает юридическую обоснованность обработки и использования информации, хранящейся в АС.

### 2.4. Построение систем защиты от угрозы раскрытия параметров информационной системы

Методы защиты от угрозы раскрытия параметров информационной системы, в принципе, не отличаются от рассмотренных выше методов защиты конфиденциальности информации. Цель данного раздела - дать представление о тех параметрах АС, раскрытие которых позволит злоумышленнику в дальнейшем реализовать основные виды угроз: нарушения

конфиденциальности информации, нарушения целостности информации и блокирования доступа к информации.

Для осуществления НСД злоумышленник не применяет никаких аппаратных или программных средств, не входящих в состав АС. Он осуществляет НСД, используя:

- знания о АС и умения работать с ней;
- сведения о системе защиты информации;
- сбои, отказы технических и программных средств;
- ошибки, небрежность обслуживающего персонала и пользователей.

Существует пять нестандартных методов исследований, которыми может воспользоваться злоумышленник для получения нужной ему информации:

1. диалоговые руководства и модели программ;
2. анализ найденных МНИ;
3. копание в мусоре;
4. изучение «фотографий»;
5. «вынюхивание».

Более детально рассмотрим первые два.

Диалоговые обучающие руководства и модели программ. Руководства и модели программ часто используются для обучения работе с компьютерной системой. Эти программы имитируют компьютерные экраны, какими видел бы их пользователь в процессе реальной работы в сети. Руководства и модели отличаются от реальной работы тем, что сообщают пользователю о стандартных методах общения с системой и иногда даже показывают ему необходимые в работе специальные детали. Если пользователь не прошел курс обучения, ему обычно выдается сборник упражнений для работы с облегченной версией настоящей системы, причем, как правило, выдается вместе с богатым набором всевозможных шпаргалок.

Руководства и модели дают новым пользователям практический опыт общения с программным обеспечением, с которым им придется иметь дело, знакомят с его функциями и задачами. Такие программы весьма часто используются в учебных целях вместо реальной системы, или же как дополнение к ней. На то имеется несколько причин. Что, если система еще внедряется, или проходит стадию обновления? А может быть, новичка слишком накладно обучать на «живой» системе - мало ли что. Модели решают подобные проблемы, так как их можно инсталлировать на любой компьютер.

Программы-модели можно получить в общественных, специализированных и даже научных библиотеках. Можно также заказать такую у производителя, написав ему, что собираетесь хорошо заплатить за его продукцию. Лесть, лож, давление на чувство

сверхполноценства производителя, а потом, будто бы невзначай, вопрос: а нет ли, случаем, у господ хороших какой-нибудь «демонстрашки»? Не исключено, что удастся добыть такую программу у дружески настроенного сотрудника компьютерного отдела компании.

Анализ найденных МНИ. Пусть злоумышленник получил доступ к МНИ с конфиденциальной информацией. Для того чтобы получить доступ к содержанию информации, в общем случае он должен обеспечить

- считывание с МНИ хранящейся на нем информации
- получение доступа к содержимому логической единицы хранения информации (файла);
- воспроизведение содержимого файла в штатном режиме;
- экспертную оценку считанной и воспроизведенной информации.

При проведении злоумышленником мероприятий, направленных на учение информации с МНИ (как правило, это гибкий или жесткий магнитный диск), у него возникает необходимость решения следующих задач.

1. Диагностика состояния носителя, включающая получение
- необходимых для конкретной ОС элементов формата носителя;
- признаков инструментальных средств подготовки носителя к использованию;
- характеристики распределения информации по рабочей поверхности носителя;
- признаков удаленной, остаточной и скрытой информации;
- данных о сбойных секторах и недоступных для чтения областей;
- признаков нестандартного форматирования носителя.

2. Профилактика состояния носителя (выявление причин, приведших к тому или иному состоянию носителя).

3. Восстановление рабочего состояния носителя.

4. Восстановление, копирование и преобразование информации на носителе.

Как уже было отмечено, необходимым условием для считывания информации с МНИ является наличие аппаратной, программной и организационной составляющих физического доступа.

Чтобы осуществить подбор привода, настройку программного обеспечения и обращение к содержимому МНИ, необходимо провести идентификацию его типа. Для этого используются первичные признаки носителя:

- внешний вид данного носителя;
- информация о типе носителя;
- характеристика данного носителя.

Исходя из описанных возможных действий злоумышленника, необходимо создавать

соответствующие защитные меры от разведки параметров системы, а именно не допускать при эксплуатации АС получения потенциальным противником указанных выше сведений.

Если имевшийся в наличии машинный носитель был правильно идентифицирован злоумышленником, для него подобран привод, то с большой вероятностью ему будет известен формат оригинального носителя, или же этот формат будет автоматически идентифицирован операционной системой, допускающей работу с приводом для данного носителя. Например, обычные 3,5" дискеты, как правило, отформатированы в стандарте IBM (MS DOS) на 1,44 Мбайта или 720 Кбайт либо в стандарте Apple Macintosh на 1,44 Мбайта или 720 Кбайт.

Однако возможно введение произвольных нестандартных способов разметки носителя, которые могут применяться не только для удобства их эксплуатации, но и с целью защиты хранящейся информации. Тогда потенциальный злоумышленник будет иметь дело с последовательностью из нулей и единиц. В этом случае потребуется классификация служебной, содержательной, остаточной и скрытой информации. По своему смыслу эта работа близка к довольно глубокому криптоанализу. Нельзя также исключать и применение более изощренных криптографических алгоритмов при зашифровании всего содержимого носителя, включая служебные области.

Процедура определения формата носителя на логическом уровне предполагает:

- определение числа и размера кластеров;
- выделение таблицы размещения файлов;
- выделение корневой директории.

Основным критерием того, осуществлен или нет логический доступ, служит способность злоумышленника выделить каждый файл на доступом ему машинном носителе. В настоящее время, из-за использования ограниченного числа типов операционных систем и еще меньшего числа способов размещения файлов на носителях, данная задача для злоумышленника может считаться решенной. В то же время для отдельных особо критичных АС (при наличии достаточного количества средств) можно рассмотреть вопрос о разработке уникальной подсистемы взаимодействия с носителем.

Если злоумышленник имеет файл, то ему известно его название с расширением, дата создания, объем, статус (только для чтения и др.). С учетом того, что существуют различные виды информации (текст, графимое изображение, звуковой и видеосигнал, программные модули и т.д.), а также различные способы ее представления, разработаны и активно используются стандарты оформления (форматы) файлов. Перечень таких форматов очень широк. Их многообразие объясняется в первую очередь большим количеством соответствующих программных продуктов. Заранее знать, в каком формате подготовлен

файл, не всегда возможно. Однако для каждого вида информации, представленной в файле, для каждого формата существуют характерные признаки. Таким образом, задача выявления смысла содержимого файла предполагает определение программного средства, с помощью которого этот файл был подготовлен, включая использованные для зашифрования средства криптографической защиты информации.

В случае применения криптографических средств защиты злоумышленник может применять криптографический анализ.

Отдельным направлением защиты АС является сокрытие логики ее работы и ее защитных функций, реализованных программно или программно - аппаратно. Это связано с тем, что большинство атак злоумышленников на системы защиты и защищаемую ими информацию включают в себя как обязательный этап изучение логики защитных и функциональных механизмов. В свою очередь, изучение логики программ АС разбивается на три стадии:

- выделение чистого кода программы;
- дизассемблирование;
- семантический анализ.

Выделение чистого кода программ может потребоваться злоумышленнику по следующим причинам.

- предприняты специальные меры для противодействия исследованию этого кода;
- предприняты меры, направленные на преобразование кода в другую форму, которые не преследуют реализацию противодействия; чаще всего это архивация или кодирование исходного

Дизассемблированием называется процесс перевода программы из исполняемых или объектных кодов на язык ассемблера. Задача дизассемблирования практически решена. В настоящее время практически для всех операционных систем существует много хороших дизассемблеров, почти стопроцентно справляющихся со стандартным кодом. Дизассемблированный текст может считаться полностью правильным, если при повторном ассемблировании получается исходный код. Аналогично, код считается не содержащим специальных приемов защиты от исследования, если дизассемблер получает полностью правильный текст. С помощью этапа дизассемблирования можно проверить качество выполнения этапа получения чистого кода: если дизассемблер не генерирует полностью правильный код, то тот этап не был закончен.

Семантический анализ программы - исследование программы изучением смысла составляющих ее функций (процедур) в аспекте операционной среды компьютера. Этот этап является заключительным и позволяет восстановить логику работы программы без исходных

текстов. При этом используется вся полученная на предыдущих этапах информация, которая, как уже отмечалось, может считаться правильной только с некоторой вероятностью, причем не исключены вообще ложные факты или умозаключения.

Семантический анализ применяется к полученным ассемблерным текстам программы и состоит в нахождении и выделении управляющих конструкций, таких как циклы, подпрограммы и т.п., и основных структур данных. При этом определяются входные и выходные данные, а также реконструируется логика проводимых с ними преобразований.

Простейшим методом защиты исполняемого кода программы является его модификация. Самым примитивным способом модификации кода (по сложности реализации и надёжности) является его упаковка при помощи одной из стандартных программ-упаковщиков: PkUte, Diet и т.д. Подобная защита ненадёжна, но тем не менее позволяет скрыть истинный исполняемый код, содержащиеся в нём текстовые строки и другую информацию, особенно если после перекодировки предприняты дополнительные меры защиты, такие как затирание идентификатора упаковщика и прочей информации, характеризующей метод упаковки.

Более надёжным методом является использование нестандартных упаковщиков. Если в предыдущем случае при удачном определении метода упаковки исполняемый код можно «развернуть», используя готовое средство, то при неизвестном упаковщике эта операция потребует предварительного анализа исполняемого кода подпрограммы, осуществляющей распаковку программы при её запуске.

Значительно более эффективным методом является шифрование тела программы и данных. Поскольку целью данного механизма защиты является обеспечение работы программы в нормальном режиме и предотвращение доступа к истинному исполняемому коду во всех остальных случаях, в качестве ключа к шифру целесообразно выбирать параметры системы и временные характеристики её работы, соответствующие именно этому режиму (картину расположения в памяти, значения системных переменных, режим работы видеоадаптера, взаимодействие с таймером).

Кроме того, модификация может не затрагивать всего кода, а касаться лишь отдельных команд (наиболее предпочтительны команды передачи управления, вызовы прерываний или их параметры), а также небольших фрагментов кода, играющих ключевую роль.

Более специализированными являются методы противодействия отладчикам. Это могут быть различные способы модификации кода при работе программы (совмещение сегмента стека с сегментом кода, шифрование кода и т.п.), активное противодействие путём периодической проверки и изменения векторов прерываний, в том числе и некорректными способами, блокировка клавиатуры и вывода на экран, контроль времени выполнения отдельных блоков программы, использование специфических особенностей микропроцессоров и т.п.

### 2.5. Методология построения защищенных АС

Рассмотрим методы построения защищенных АС. Эти методы условно можно разделить на две группы:

1) относящиеся к произвольному ПО АС:

- иерархический метод разработки;
- исследование корректности и верификация.

2) специфичные только для систем защиты (теория безопасных систем).

*Иерархический метод разработки ПО АС.* В соответствии с принципом абстракции при проектировании АС разработчики могут идти по меньшей мере двумя путями: от аппаратуры «вверх» - к виртуальной машине, представляющей АС, или от виртуальной машины «вниз»- к реальному оборудованию. Это и есть два основных метода проектирования - метод снизу вверх и метод сверху вниз. Остальные методы по своей сути сводятся к этим двум или являются их сочетанием.

Первый метод достаточно прост, требует намного меньших капитальных вложений, но и обладает меньшими возможностями. Он основан на известной схеме : «Вы – злоумышленник. Ваши действия?». То есть служба информационной безопасности, основываясь на данных о всех известных видах атак, пытается применить их на практике с целью проверки, а возможно ли такая атака со стороны реального злоумышленника.

Метод снизу вверх предполагает начало проектирования с основного аппаратного оборудования системы. При проектировании модули разбиваются на ряд слоев, причём нулевой слой виртуальной системы образует аппаратура. Слои, реализующие одно или несколько необходимых свойств, добавляются последовательно пока не будет получена желаемая виртуальная машина. К недостаткам метода проектирования снизу вверх относят:

- необходимость с самого начала принимать решение о выборе способа реализации компонентов АС-с помощью аппаратуры, микропрограмм или программ, что сделать очень трудно;
- возможность проектирования АС только после разработки аппаратуры;
- расхождение между реальной АС и определённой в ТЗ.

Метод «сверху вниз» представляет собой, наоборот, детальный анализ всей существующей схемы хранения и обработки информации. Первым этапом этого метода является, как и всегда, определение, какие информационные объекты и потоки необходимо защищать. Далее следует изучение текущего состояния системы информационной безопасности с целью определения, что из классических методик защиты информации уже реализовано, в каком объеме и на каком уровне. На третьем этап производится

классификация всех информационных объектов на классы в соответствии с ее конфиденциальностью, требованиями к доступности и целостности (неизменности).

Далее следует выяснение насколько серьезный ущерб может принести фирме раскрытие или иная атака на каждый конкретный информационный объект. Этот этап носит название «вычисление рисков». В первом приближении риском называется произведение «возможного ущерба от атаки» на «вероятность такой атаки». Существует множество схем вычисления рисков, остановимся на одной из самых простых.

Ущерб от атаки может быть представлен неотрицательным числом в приблизительном соответствии со следующей таблицей 2.1.

Таблица 2.1.

| Величина ущерба | Описание |
|---|---|
| 0 | Раскрытие информации принесет ничтожный моральный и финансовый ущерб фирме |
| 1 | Ущерб от атаки есть, но он незначителен, основные финансовые операции и положение фирмы на рынке не затронуты |
| 2 | Финансовые операции не ведутся в течение некоторого времени, за это время фирма терпит убытки, но ее положение на рынке и количество клиентов изменяются минимально |
| 3 | Значительные потери на рынке и в прибыли. От фирмы уходит ощутимая часть клиентов |
| 4 | Потери очень значительны, фирма на период до года теряет положение на рынке. Для восстановления положения требуются крупные финансовые займы. |
| 5 | Фирма прекращает существование |

Вероятность атаки представляется неотрицательным числом в приблизительном соответствии со следующей таблицей 2.2.

Таблица 2.2.

| Вероятность | Средняя частота появления |
|---|---|
| 0 | Данный вид атаки отсутствует |
| 1 | реже, чем раз в год |
| 2 | около 1 раза в год |

| | |
|---|---|
| 3 | около 1 раза в месяц |
| 4 | около 1 раза в неделю |
| 5 | практически ежедневно |

Необходимо отметить, что классификацию ущерба, наносимого атакой, должен оценивать владелец информации, или работающий с нею персонал. А вот оценку вероятности появления атаки лучше доверять техническим сотрудникам фирмы.

Следующим этапом составляется табл. 2.3. - таблица рисков предприятия. Она имеет следующий вид.

Таблица 2.3. Таблица рисков

| Описание атаки | Ущерб | Вероятность | Риск (=Ущерб*Вероятность) |
|---|---|---|---|
| Спам (переполнение почтового ящика) | 1 | 4 | 4 |
| Копирование жесткого диска из центрального офиса | 3 | 1 | 3 |
| ... | ... | ... | 2 |
| Итого: | | | 9 |

На этапе анализа таблицы рисков задаются некоторым максимально допустимым риском, например значением 7. Сначала проверяется каждая строка таблицы на не превышение риска этого значения. Если такое превышение имеет место, значит, данная строка – это одна из первоочередных целей разработки политики безопасности. Затем производится сравнение удвоенного значения (в нашем случае 7*2=14) с интегральным риском (ячейка «Итого»). Если интегральный риск превышает допустимое значение, значит, в системе набирается множество мелких погрешностей в системе безопасности, которые в сумме не дадут предприятию эффективно работать. В этом случае из строк выбираются те, которые дает самый значительный вклад в значение интегрального риска и производится попытка их уменьшить или устранить полностью.

На самом ответственном этапе производится собственно разработка политики безопасности предприятия, которая обеспечит надлежащие уровни как отдельных рисков, так и интегрального риска. При ее разработке необходимо, однако, учитывать объективные проблемы, которые могут встать на пути реализации политики безопасности. Такими

проблемами могут стать законы страны и международного сообщества, внутренние требования корпорации, этические нормы общества.

После описания всех технических и административных мер, планируемых к реализации, производится расчет экономической стоимости данной программы. В том случае, когда финансовые вложения в программу безопасности являются неприемлимыми или просто экономически невыгодными по сравнению с потенциальным ущербом от атак, производится возврат на уровень, где мы задавались максимально допустимым риском 7 и увеличение его на один или два пункта.

Завершается разработка политики безопасности ее утверждением у руководства фирмы и детальным документированием. За этим должна следовать активная реализация всех указанных в плане компонентов. Перерасчет таблицы рисков и, как следствие, модификация политики безопасности фирмы чаще всего производится раз в два года.

Структурный принцип имеет фундаментальное значение и составляет основу большинства реализаций. Согласно этому принципу, для построения ПО требуются только три основные конструкции:

- функциональный блок;
- конструкция обобщенного цикла;
- конструкция принятия двоичного решения.

Функциональный блок можно представить как отдельный вычислительный оператор или как любую другую реальную последовательность вычислений с единственным входом и единственным выходом, как в подпрограмме. Организация цикла в литературе часто упоминается как элемент DO-WHILE. Конструкция принятия двоичного решения называется IF-THEN-ELSE.

Эти конструкции могут сами рассматриваться как функциональные блоки, поскольку они обладают только одним входом и одним выходом. Таким образом, можно ввести преобразование операции цикла в функциональный блок и в последующем рассматривать всякий такой оператор цикла эквивалентом (несколько более сложного) функционального блока. Аналогично можно ввести преобразование конструкции принятия решения к функциональному блоку. Наконец, можно привести любую последовательность функциональных элементов к одному функциональному элементу. В то же время обратная последовательность преобразований может быть использована в процессе проектирования программы по нисходящей схеме, т.е. исходя из единственного функционального блока, который постепенно раскладывается в сложную структуру основных элементов.

Принцип модульного проектирования заключается в разделении программ на функционально самостоятельные части (модули), обеспечивающие заменяемость,

кодификацию, удаление и дополнение составных частей.

Преимущества использования модульного принципа состоят в следующем:

- Упрощается отладка программ, так как ограниченный доступ к модулю и однозначность его внешнего проявления исключают влияние ошибок в других, связанных с ним, модулях на его функционирование.
- Обеспечивается возможность организации совместной работы больших коллективов разработчиков, так как каждый программист имеет дело с независимой от других частью программы.
- Повышается качество программы, так как относительно малый размер модулей и, как следствие, небольшая сложность их позволяют провести более полную проверку программы.

*Исследование корректности реализации и верификация АС.* Понятие корректности или правильности подразумевает соответствие проверяемого объекта некоторому эталонному объекту или совокупности формализованных эталонных характеристик и правил. Корректность ПО при разработке наиболее полно определяется степенью соответствия предъявляемым к ней формализованным требованиям программной спецификации. В спецификациях отражается совокупность эталонных характеристик, свойств и условий, которым должна соответствовать программа. 1 Основную часть спецификации составляют функциональные критерии и Ц характеристики. Исходной программной спецификацией, которой должна соответствовать программа, является ТЗ

При отсутствии полностью формализованной спецификации требований в качестве ТЗ, которому должна соответствовать АС и результаты ее функционирования, иногда используются неформализованные предоставления разработчика, пользователя или заказчика программ. Однако понятие корректности программ по отношению к запросам пользователя или заказчика сопряжено с неопределённостью самого эталона, которому должна соответствовать АС. Для сложных программ всегда существует риск обнаружить их некорректность (по мнению пользователя или заказчика) при формальной корректности относительно спецификаций вследствие неточности самих спецификаций. Традиционный взгляд на спецификацию требований заключается в том, что она представляет собой документ на естественном языке, который является интерфейсом между заказчиком и изготовителем. Хотя подготовке документа может предшествовать некоторое взаимодействие, именно этот документ в значительной степени выступает как «отправная точка» для изготовителя программ.

Таким образом, можно сделать вывод о том, что создание совокупности взаимоувязанных непротиворечивых спецификаций является необходимой базой для обеспечения корректности проектируемой программы. При этом спецификации должны:

- быть формальными;
- позволять проверять непротиворечивость и полноту требований заказчика;
- служить основой для дальнейшего формализованного проектирования ОС.

Существует несколько подходов к определению спецификаций требований.

*Спецификация как описание*. Заказчик выдает спецификацию, чтобы изготовители могли снабдить его тем изделием, которое он желает, поэтому заказчик видит этот документ главным образом как описание системы, которую он желал бы иметь. В принципе, в описании должно быть указано, что должна и что не должна делать система. На практике обычно по умолчанию предполагается, что система должна делать то, что уточняется в спецификации, и не должна делать ничего более. В этом состоит главная проблема с описательной стороной спецификации. Предполагается, что заказчик всегда точно знает всё, что система должна и не должна делать. Более того. в дальнейшем предполагается, что заказчик полностью перенёс это знание в специфицированный документ.

*Спецификация как предписание.* Изготовитель смотрит на специфицированный документ как на набор составных частей, подлежащих сборке, чтобы разрешить проблему заказчика. Такой предписывающий взгляд обуславливается не только трудностями создания описательного документа (как указывалось выше), но и сведениями, которые умышленно или неумышленно расширяют или ограничивают свободу изготовителя.

*Договорная методология.* В рамках «описание заказчика-предписание изготовителю» спецификация рассматривается как формальное разделение между сторонами. Что касается заказчика, то он оговаривает минимально приемлемое, тогда как изготовитель - максимально требуемое. Договор предлагается и принимается при зарождении системы и заканчивается после завершения системы, когда заказчик принимает систему как отвечающую его минимальным требованиям. Во время изготовления системы в принципе не предполагается никаких взаимодействий, даже если изготовитель подозревает, что предписываемое не совсем соответствует тому, что заказчик желает видеть в действительности.

*Спецификация как модель*. Современные более строгие представления о спецификации трактуют ее как модель системы. При условии, что лежащая в основе модели семантика в достаточной мере обоснована, такая спецификация обеспечивает чёткую формулировку требований.

Соответствующие модели подходят также для автоматизированного контроля целостности и другого прогнозного анализа, который, в частности, обеспечит прекращение разработки системы, в принципе не способной удовлетворить требованиям.

Модели как описание системы имеют следующие отличительные черты по сравнению с другими способами формального описания:

- хорошее сочетание нисходящего и восходящего подходов к их разработке с возможностью выбора абстрактного описания;
- возможность описания параллельной, распределенной и циклической работы;
- возможность выбора различных формализованных аппаратов для описания систем.

Основное преимущество использования формальной модели заключается в возможности исследования с ее помощью особенностей моделируемой системы. Основывая формальный метод разработки на математической модели и затем, исследуя модель, можно выявить такие грани поведения системы, которые в противном случае не были бы очевидны до более поздних стадий.

Так как целевым объектом проектирования является АС, то модель может описывать либо саму АС, либо ее поведение, т.е. внешние проявления функционирования АС. Модель, описывающая поведение АС по сравнению с моделью АС, обладает одним важным преимуществом - она может быть проверена и оценена как исполнителями, так и заказчиками, поскольку заказчики не знают, как должна работать АС, но зато они представляют, что она должна делать. В результате такого моделирования может быть проверена корректность спецификаций относительно исходной постановки задачи, т.е. ТЗ. Кроме того, критерии правильности считаются достаточными при условии, что спецификация представляет собой. исчерпывающее описание «внешнего» поведения объекта при всех возможных (или запланированных) ситуациях его использования.

Как было отмечено выше, при разработке АС, особенно ее компонентов, представляющих систему защиты информации, для обеспечения высоких гарантий отсутствия неисправностей и последующего доказательства того, что система функционирует согласно требованиям ТЗ, используются формальные подходы к ее проектированию.

Формальное проектирование алгоритмов базируется, в основном, на языках алгоритмических логик, которые включают высказывание вида Q{S}R, читающееся следующим образом: если до исполнения оператора S было выполнено условие Q, то после него будет R'. Здесь Q называется предусловием, а R-постусловием. Эти языки были изобретены практически одновременно Р.У. Флойдом (1967 г.), С.А.Р. Хоаром (1969 г.) и учеными польской логической школы (А. Сальвицкий и др., 1970 г.). Как предусловие, так и постусловие являются предикатами.

Преимущество представления алгоритма в виде преобразователя предикатов состоит в том, что оно дает возможность:

- анализировать алгоритмы как математические объекты;
- дать формальное описание алгоритма, позволяющее интеллектуально охватить

алгоритм;

- синтезировать алгоритмы по представленным спецификациям;
- провести формальное верифицирование алгоритма, т.е. доказать корректность его реализации.

Методология формальной разработки и доказательства корректности алгоритмов в настоящее время хорошо разработана и изложена в целом ряде работ. Вкратце суть этих методов сводится к следующему:

- разработка алгоритма проводится методом последовательной декомпозиции, с разбивкой общей задачи, решаемой алгоритмом, на ряд более мелких подзадач;
- критерием детализации подзадач является возможность их реализации с помощью одной конструкции ветвления или цикла;
- разбиение общей задачи на подзадачи предусматривает формулирование пред- и постусловий для каждой подзадачи с целью их корректного проектирования и дальнейшей верификации.

Для доказательства корректности алгоритма (верификация) формулируется математическая теорема Q{S}R, которая затем доказывается. Доказательство теоремы о корректности принято разбивать на две части. Одна часть служит для доказательства того, что рассматриваемый алгоритм вообще может завершить работу (проводится анализ всех циклов). В другой части доказывается корректность постусловия в предположении, что алгоритм завершает работу.

*Теория безопасных систем (ТСВ).* Понятие «доверенная вычислительная среда» (trusted computing base-TCB) появилось в зарубежной практике обеспечения информационной безопасности достаточно давно. Смысл характеристики «доверенная» можно пояснить следующим образом.

Дискретная природа характеристики «безопасный» (в том смысле, что либо нечто является безопасным, полностью удовлетворяя ряду предъявляемых требований, либо не является, если одно или несколько требований не выполнены) в сочетании с утверждением «ничто не бывает безопасным на сто процентов» подталкивают к тому, чтобы вести более гибкий термин, позволяющий оценивать то, в какой степени разработанная защищенная АС соответствует ожиданиям заказчиков. В этом отношении характеристика «доверенный» более адекватно отражает ситуацию, где оценка, выраженная этой характеристикой (безопасный или доверенный), основана не на мнении разработчиков, а на совокупности факторов, включая мнение независимой экспертизы, опыт предыдущего сотрудничества с разработчиками, и в конечном итоге, является прерогативой заказчика, а

не разработчика.

Доверенная вычислительная среда (ТСВ) включает все компоненты и механизмы защищенной автоматизированной системы, отвечающие за реализацию политики безопасности - комплекс превентивных мер по защите конфиденциальных данных и информационных процессов на предприятии. Политика безопасности включает в себя требования в адрес персонала, менеджеров и технических служб. Основные направления разработки политики безопасности:

- определение какие данные и насколько серьезно необходимо защищать,
- определение кто и какой ущерб может нанести фирме в информационном аспекте,
- вычисление рисков и определение схемы уменьшения их до приемлемой величины.

Все остальные части АС, а также ее заказчик полагаются на то, что ТСВ корректно реализует заданную политику безопасности даже в том случае, если отдельные модули или подсистемы АС разработаны высококвалифицированными злоумышленниками с тем, чтобы вмешаться в функционирование ТСВ и нарушить поддерживаемую ею политику безопасности.

Минимальный набор компонентов, составляющий доверенную вычислительную среду, обеспечивает следующие функциональные возможности:

- взаимодействие с аппаратным обеспечением АС;
- защиту памяти;
- функции файлового ввода-вывода;
- управление процессами.

Дополнение и модернизация существующих компонентов АС с учетом требований безопасности могут привести к усложнению процессов сопровождения и документирования. С другой стороны, реализация всех перечисленных функциональных возможностей в рамках централизованной доверенной вычислительной среды в полном объеме может вызвать разрастание размеров ТСВ и, как следствие, усложнение доказательства корректности реализации политики безопасности. Так, операции с файлами могут быть реализованы в ТСВ в некотором ограниченном объеме, достаточном для поддержания политики безопасности, а расширенный ввод-вывод в таком случае реализуется в той части АС, которая находится за пределами ТСВ. Кроме того, необходимость внедрения связанных с безопасностью функций во многие компоненты АС, реализуемые в различных модулях АС, приводит к тому, что защитные функции распределяются по всей АС, вызывая аналогичную проблему.

Определены следующие этапы разработки защищенной АС:

- определение политики безопасности;
- проектирование модели АС;

- разработка кода АС;
- обеспечение гарантий соответствия реализации заданной политике.

**3. Формальные политики безопасности**

**3.1 Понятие формальной политики безопасности**

Рассматривая вопросы безопасности информации в компьютерных системах можно говорить о наличии некоторых «желательных» состояний данных систем. Эти желательные состояния (описанные в терминах модели собственно компьютерной системы, например, в терминах субъектно-объектной модели) описывают «защищенность» системы. Понятие «защищенности» принципиально не отличается от любых других свойств технической системы, например, «надежной работы», и является для системы внешним, априорно заданным. Особенностью понятия «защищенность» является его тесная связь с понятиями «злоумышленник» (как обозначение внешней причины для вывода системы из состояния «защищенности») или «угроза» (понятие, обезличивающее причину вывода системы из защищенного состояния из-за действий злоумышленника).

При рассмотрении понятия «злоумышленник» практически всегда выделяется объект его воздействия - часть системы, связанная с теми или иными действиями злоумышленника («объект атаки»). Следовательно, можно выделить три компоненты, связанные с нарушением безопасности системы:

1. «злоумышленник» - внешний по отношению к системе источник нарушения свойства «безопасность»;

2. «объект атаки» - часть, принадлежащая системе, на которую злоумышленник производит воздействие;

3. «канал воздействия» - среда переноса злоумышленного воздействия.

Интегральной характеристикой, описывающей свойства защищаемой системы, является политика безопасности - качественное (или качественно-количественное) описание свойств защищенности, выраженное в терминах, описывающих систему. Описание политики безопасности может включать или учитывать свойства злоумышленника и объекта атаки.

Описание политики безопасности включает:

1. Множество возможных операций над объектами.

2.Для каждой пары «субъект-объект» (Si,0j) назначение множества разрешенных операций, являющегося подмножеством всего множества возможных операций. Операции связаны обычно с целевой функций защищаемой системы (т.е. с категорией, описывающей назначение системы и решаемые задачи), например, операциями «создание объекта», «удаление объекта», «перенос информации от произвольного объекта к предопределенному - чтение» и т. д.

Можно сформулировать две аксиомы защищенных компьютерных систем (АС):

*Аксиома 1*. В защищенной АС всегда присутствует активная компонента (субъект), выполняющая контроль операций субъектов над объектами. Данная компонента фактически отвечает за реализацию некоторой политики безопасности.

*Аксиома 2*. Для выполнения в защищенной АС операций над объектами необходима дополнительная информация (и наличие содержащего ее объекта) о разрешенных и запрещенных операциях субъектов с объектами.

В данном случае мы оперируем качественными понятиями «контроль», «разрешенная и запрещенная операция», данные понятия будут раскрыты и проиллюстрированы ниже.

Существует дополнительная аксиома.

*Аксиома 3.* Все вопросы безопасности информации описываются доступами субъектов к объектам.

Важно заметить, что политика безопасности описывает в общем случае нестационарное состояние защищенности. Защищаемая система может изменяться, дополняться новыми компонентами (субъектами, объектами, операциями субъектов над объектами). Очевидно, что политика безопасности должна быть поддержана во времени, следовательно. в процесс изучения свойств защищаемой системы должны быть добавлены процедуры управления безопасностью.

С другой стороны, нестационарность защищаемой АС, а также вопросы реализации политики безопасности в конкретных конструкциях защищаемой системы (например, программирование контролирующего субъекта в командах конкретного процессора компьютера) предопределяют необходимость рассмотрения задачи гарантирования заданной политики безопасности.

В результате, можно сказать, что компьютерная безопасность решает четыре класса взаимосвязанных задач:

1. Формулирование и изучение политик безопасности.

2. Реализация политик безопасности.

3.Гарантирование заданной политики безопасности.

Типовой жизненный цикл АС состоит из следующих стадий:

1. Проектирование АС и проектирование политики безопасности.

2. Моделирование ПБ и анализ корректности ПБ, включающий усыновление адекватности политики безопасности и целевой функции СС.

3. Реализация ПБ и механизмов ее гарантирования, а также процедур и механизмов управления безопасностью.

4. Эксплуатация защищенной системы.

Рассмотрим подробно подходы к решению поставленных задач.

### 3.2. Понятие доступа и монитора безопасности

В теории компьютерной безопасности практически всегда рассматривается модель произвольной АС в виде конечного множества элементов. Указанное множество можно разделить на два подмножества: множество объектов и множество субъектов. Данное разделение основано на свойстве элемента «быть активным» или «получать управление» (применяются также термины «использовать ресурсы» или «пользоваться вычислительной мощностью»). Оно исторически сложилось на основе модели вычислительной системы, принадлежащей фон Нейману, согласно которой последовательность исполняемых инструкций (программа, соответствующая понятию «субъект») находится в единой среде с данными (соответствующими понятию «объект»).

Модели, связанные с реализацией ПБ, не учитывают возможности субъектов по изменению АС, которые могут привести к изменению ее свойств и как предельный случай к полной неприменимости той или иной модели к описанию отношений «субъект-объект» в измененной АС.

Этот факт не является недостатком политики безопасности. Достоверность работы механизмов реализации политики безопасности считается априорно заданной, поскольку в противном случае невозможна формализация и анализ моделей. Однако вопрос гарантий политики безопасности является ключевым как в теории, так и в практике. Рассматривая активную роль субъектов в АС, необходимо упомянуть о ряде важнейших их свойств, на которых базируется излагаемая ниже модель.

Во-первых, необходимо заметить, что человек-пользователь воспринимает объекты и получает информацию о состоянии АС через субъекты, которыми он управляет и которые производят отображение информации в воспринимаемом человеком виде.

Во-вторых, угрозы компонентам АС (АС рассматривается в модели потоков или состояний исходят от субъектов как активной компоненты, порождающей потоки и изменяющей состояние объектов в АС.

В-третьих, субъекты могут влиять друг на друга через изменяемые ими объекты, связанные с другими субъектами, порождая в конечном итоге в системе субъекты (или состояния системы), которые представляют угрозу для безопасности информации или для работоспособности самой системы.

Будем считать разделение АС на субъекты и объекты априорным. Будем считать также, что существует априорный безошибочный критерий различения субъектов и объектов в АС (по свойству активности). Кроме того, считаем в условиях всех утверждений, что декомпозиция АС на субъекты и объекты фиксирована.

Подчеркнем отличие понятия субъекта компьютерной системы от человека-пользователя следующим определением.

Пользователь - лицо (физическое лицо), аутентифицируемое некоторой информацией и управляющее субъектом компьютерной системы через органы управления ЭВМ. Пользователь АС является, таким образом, внешним фактором, управляющим состоянием субъектов: В связи с этим далее будем считать пользовательское управляющее воздействие таким, что свойства субъектов, сформулированные в ниже приводимых определениях, не зависят от него (т. е. свойства субъектов не изменяемы внешним управлением). Смысл данного условия состоит в предположении того факта, что пользователь, управляющий программой, не может через органы управления изменить ее свойства (условие неверно для систем типа компиляторов, средств разработки, отладчиков и др.).

Будем также полагать, что в любой дискретный момент времени множество субъектов АС не пусто (в противном случае соответствующие моменты времени исключаются из рассмотрения и рассматривается отрезки с ненулевой мощностью множества субъектов).

*Аксиома 4*. Субъекты в АС могут быть порождены только активной компонентой (субъектами) из объектов.

Специфицируем механизм порождения новых субъектов следующим определением.

*Определение 1*. Объект Oi называется источником для субъекта Sm, ели существует субъект Sj, в результате воздействия которого на объект Oi в компьютерной системе возникает субъект Sm.

Субъект Sj, порождающий новый субъект из объекта Oi, в свою очередь, называется активизирующим субъектом для субъекта Sm, Sm назовем порожденным объектом.

Введем обозначение: *Create (Sj, Oi)»>Sк* - из объекта Oi порожден объект Sk при активизирующем воздействии субъекта Sj. Create назовем операцией порождения субъектов (см. рис. 1).

Операция Create задает отображение декартова произведения множеств субъектов и объектов на объединение множества субъектов пустым множеством. Заметим также, что в АС действует дискретное время и фактически новый субъект Sk порождается в момент времени t+1 относительно момента t, в который произошло воздействие порождающего субъекта на объект-источник.

Очевидно, что операция порождения субъектов зависит как от свойств активизирующего субъекта, так и от содержания объекта-уточника.

Считаем, что если Create(Sj, Oi)-> NULL (конструкция NULL далее обозначает пустое множество), то порождение нового субъекта из объекта Oi при активизирующем воздействии Sj невозможно. Так, практически во всех операционных средах существует понятие исполняемого файла - объекта, могущего быть источником для порождения субъекта. Например, для MS DOS файл edit.com является объектом источником для порождения субъекта-программы текстового редактора, а порождающим субъектом является, как

правило, командный интерпретатор shell (объект-источник ~ command.com). Из архитектуры фон Неймана следует также, что с любым субъектом связан (или ассоциирован) некоторый объект (объекты), отображающий его состояние, - например, для активной программы (субъекта) ассоциированным объектом будет содержание участка оперативной памяти с исполняемым кодом данной программы.

Определение 2. Объект Oi в момент времени t ассоциирован субъектом Sm, если состояние объекта Oi повлияло на состояние субъекта в следующий момент времени (т.е. субъект Sm использует ин формацию, содержащуюся в объекте Oi).

Введем обозначение "множество объектов {0m}t ассоциировано субъектом Si в момент времени t": Si( {0m}t).

В данном случае определение не в полной мере является формально строгим, поскольку состояние субъекта описывается упорядоченной совокупностью ассоциированных с ним объектов, а ассоциированный объект выделяется по принципу влияния на состояние субъекта, т. е. в определении прослеживается некая рекурсия. С другой стороны, известны рекурсивные определения различных объектов (например, дерева). Зависимость от времени позволяет однозначно выделять ассоциированные объекты том случае, если в начальный момент ассоциированный объект можно определить однозначно (как правило, это вектор исполняемого кода и начальные состояния ряда переменных программы).

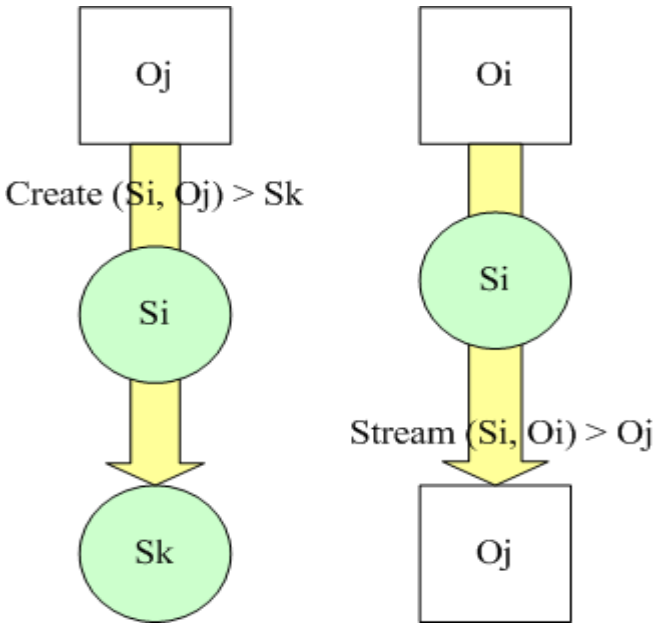



Рис. 3.1. Порождения субъекта и понятие потока

Субъект в общем случае реализует некоторое отображение множества ассоциированных объектов в t-ный момент времени на множество ассоциированных объектов в t+l-ный момент

времени. В связи с этим можно выделить ассоциированные объекты, изменение которых изменяет вид отображения ассоциированных объектов (объекты, содержащие, как правило, код программы - функционально ассоциированные), и ассоциированные объекты-данные (являющиеся аргументом операции, но не изменяющие вида отображения). Далее под ассоциированными объектами понимаются функционально ассоциированные объекты, в иных случаях делаются уточнения.

*Следствие (к определению 2).* В момент порождения субъекта Sm из объекта Oi он является ассоциированным объектом для субъекта Sm.

Необходимо заметить, что объект-источник может быть ассоциированным для активизирующего субъекта, тогда порождение является автономным (т. е. не зависящим от свойств остальных субъектов и объектов). Если же объект-источник является неассоциированным (внешним) для активизирующего субъекта, то порождение не является автономным и зависит от свойств объекта-источника.

Свойство субъекта "быть активным" реализуется и в возможности выполнения действий над объектами. При этом необходимо отметить, что пассивный статус объекта необходимо требует существования потоков информации от объекта к объекту (в противном случае невозможно говорить об изменении объектов), причем данный поток инициируется субъектом.

*Определение 3*. Потоком информации между объектом Om и объектом Oj называется произвольная операция над объектом Oj, реализуемая в субъекте Si и зависящая от Om.

Заметим, что как Oj, так и Om могут быть ассоциированными или ассоциированными объектами, а также «пустыми» объектами (NULL).

Обозначения: *Stream (Si, 0m)-> Oj* - поток информации от объекта Om к объекту Oj. При этом будем выделять источник (Om) и получатель приемник) потока (Oj). В определении подчеркнуто, что поток информации рассматривается не между субъектом и объектом, а между объектами, например, объектом и ассоциированными объектами субъекта либо между двумя объектами), а активная роль субъекта выражается в реализации данного потока (это означает, что операция порождения (отека локализована в субъекте и отображается состоянием его функционально ассоциированных объектов). Отметим, что операция Stream может создавать новый объект или уничтожать его. На рис.2 схематически изображены различные виды потоков.

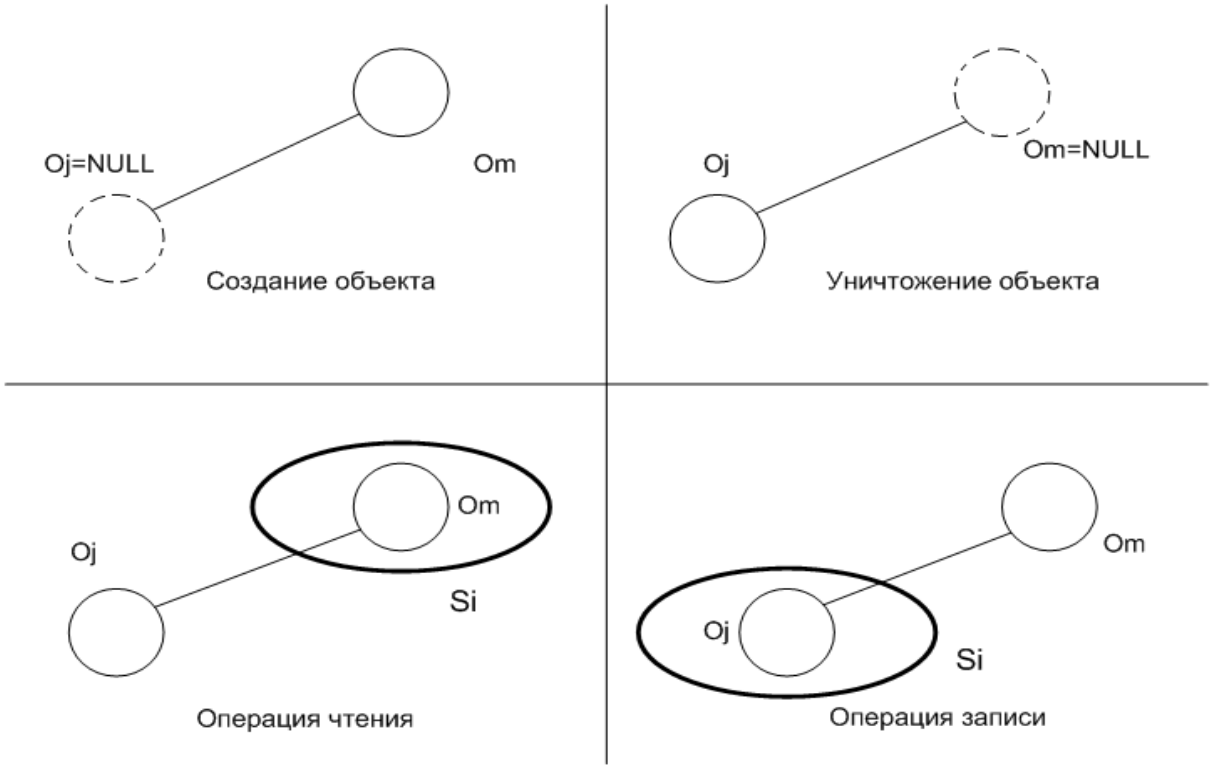



Рис. 3.2. Примеры потоков в АС

Далее будем для краткости говорить о потоке, подразумевая веденное понятие потока информации.

Понятие ассоциированных с субъектом объектов, как легко видеть из нижеизложенного, не является искусственной конструкцией. Корректно говорить о потоках информации можно лишь между одинаковыми сущностями, т.е. объектами. Кроме того, в ассоциированных объектах отображается текущее состояние субъекта. Отображения Stream и Create описываются с точки зрения разделения на субъекты и объекты все события (изменения субъектов и объектов), происходящие в АС.

Из данного определения также следует, что поток всегда инициируется(порождается) субъектом.

*Определение 4*. Доступом субъекта Si к объекту Oj будем называть порождение потока информации между некоторым объектом (например, ассоциированным с субъектом объектами Si(0m)) и объектом Oj .

Выделим все множество потоков P для фиксированной декомпозиции АС на субъекты и объекты во все моменты времени (все множество потоков является объединением потоков по всем моментам дискретного времени) и произвольным образом разобьем его на два непересекающихся подмножества: N и L, P = N U L.

Обозначим

N-подмножество потоков, характеризующее несанкционированный доступ;

L - подмножество потоков, характеризующих легальный доступ.

Дадим некоторые пояснения к разделению множеств L и N. Понятие «безопасности» подразумевает наличие и некоторого состояния «опасности» - нежелательных состояний какой-либо системы (в данном случае АС). Будем считать парные категории типа «опасный - безопасный» априорно заданными для АС и описываемыми политикой безопасности, а результатом применения политики безопасности к АС - разделение на множество «опасных» потоков N и множество «безопасных» L. Деление на L и N может описывать как свойство целостности (потоки из N нарушают целостность АС) или свойство конфиденциальности (потоки из N нарушают конфиденциальность АС), так и любое другое произвольное свойство.

*Определение 5*. Правила разграничения доступа субъектов к объектам есть формально описанные потоки, принадлежащие подмножеству L.

В предлагаемой субъектно-ориентированной модели не производится уточнений известных моделей политик безопасности (политика безопасности описывает только критерии разбиения на множества L и N), но формулируются условия корректного существования элементов АС, обеспечивающих реализацию той или иной политики безопасности. Поскольку критерий разбиения на множества L и N не связан со следующими далее утверждениями (постулируется лишь наличие субъекта, реализующего фильтрацию потоков), то можно говорить об инвариантности субъектно-ориентированной модели относительно любой принятой в АС политики безопасности (не противоречащей условиям утверждений).

*Определение 6*. Объекты Oi и Oj тождественны в момент времени t, если они совпадают как слова, записанные в одном языке.

Например, при представлении в виде байтовых последовательностей объекты 01= (O11, 012, ..., O1m) и 02=(021 022,  , 02k) одинаковы, если m=k и O1i = 02i для всех i от 1 до k (Oij-байты).

Для введения понятия тождественности субъектов условимся о наличии процедуры сортировки ассоциированных объектов, которая позволяет говорить о возможности попарного сравнения. На практике всегда существует алгоритм, обеспечивающий возможность попарного сравнения и зависящий от конкретной архитектуры АС. Например, достаточно легко выделить и попарно сравнивать, например, участки активной памяти, отвечающие коду программ (отличающиеся абсолютным адресом загрузки в оперативную память) или содержанию ценных и массивов.

*Определение 7*. Субъекты Si и Sj тождественны в момент времени попарно тождественны все ассоциированные с ними объекты.

Следствие (из определений 6 и 7). Порожденные субъекты тождественны, если тождественны порождающие субъекты и объекты-

Верность данного следствия вытекает из тождества функционально ассоциированных объектов в порождающих субъектах, которые отвечают за порождение нового субъекта, а также из тождества аргументов (ассоциированных объектов-данных), которые отвечают объектам- источникам.

Для разделения всего множества потоков в АС на подмножества L необходимо существование активной компоненты (субъекта), который:

- активизировался бы при возникновении любого потока;
- производил бы фильтрацию потоков в соответствии с принадлежностью множествам L или N.

Заметим, что если существует Stream (Si, 0j)->0m и существует Stream( Sk, 0m)->0i, то существует и Stream ((Si, Sk), 0j)->0i, т. е. Отношение «между объектами существует поток» является транзитивным (относительно пары субъектов). Именно в этом смысле будем говорить об участи субъекта (Sk) в потоке (если От является ассоциированным объектом субъекта, не тождественного Si). Введем несколько определений.

*Определение 8.* Монитор обращений (МО) - субъект, активизирующийся при возникновении потока от любого субъекта к любому объекту.

Можно выделить два вида МО:

Индикаторный МО - устанавливающий только факт обращения - к объекту.

МО - субъект, функционирующий таким образом, что при возникновении потока от ассоциированного объекта От Si (Si(0m)) к объекту Oj и обратно существует ассоциированный с МО объект 0m0 (в данном случае речь идет об ассоциированных объектах-данных), тождественный объекту От или Si(0m). Содержательный МО полностью участвует в потоке от субъекта к объекту (в том смысле, что информация проходит через его ассоциированные объекты-данные и существует тождественное отображение объекта на какой-либо ассоциированный объект МО).

Теперь сформулируем понятие монитора безопасности (в литературе также применяется понятие монитора ссылок). Это понятие связано с упоминаемой выше задачей фильтрации потоков. Поскольку целью является обеспечение безопасности АС, то и целевая функция монитора — фильтрация с целью обеспечения безопасности (отметим еще раз, что разделение на N и L задано априорно).

*Определение 9.* Монитор безопасности объектов (МБО) -монитор обращений, который разрешает поток, принадлежащий только множеству легального доступа L. Разрешение потока в данном случае понимается как выполнение операции над объектом - получателем потока, а запрещение -как невыполнение (т.е. неизменность объекта -получателя потока).

Монитор безопасности объектов фактически является механизмом реализации политики безопасности в АС. Обратимся теперь к основным моделям работы МБО.

### 3.3. Основные типы формальных политик безопасности

Существуют два типа политики безопасности: дискреционная и мандатная.

Основой *дискреционной (дискретной) политики безопасности* является дискреционное управление доступом (Oiscretion.ary Access Control - OAC), которое определяется двумя свойствами:

- все субъекты и объекты должны быть идентифицированы;
- права доступа субъекта к объекту системы определяются на основании некоторого внешнего по отношению к системе правила.

К достоинствам дискреционной политики безопасности можно отнести относительно простую реализацию соответствующих механизмов защиты. Этим обусловлен тот факт, что большинство распространенных в настоящее время АС обеспечивают выполнение положений именно данной политики безопасности.

В качестве при мера реализаций дискреционной политики безопасности в АС можно привести матрицу доступов, строки которой соответствуют субъектам системы, а столбцы - объектам; элементы матрицы характеризуют права доступа. К недостаткам относится статичность модели. Это означает, что данная политика безопасности не учитывает динамику изменений состояния АС, не накладывает ограничений на состояния системы.

Кроме этого, при использовании дискреционной политики безопасности возникает вопрос определения правил распространения прав доступа и анализа их влияния на безопасность АС. В общем случае при использовании данной политики безопасности перед МБО, который при санкционировании доступа субъекта к объекту руководствуется некоторым набором правил, стоит алгоритмически неразрешимая задача: проверить приведут ли его действия к нарушению безопасности или нет.

В то же время имеются модели АС, реализующих дискреционную политику безопасности, которые предоставляют алгоритмы проверки безопасности.

Так или иначе, матрица доступов не является тем механизмом, который бы позволил реализовать ясную и четкую систему защиты информации в АС. Этим обуславливается поиск других более совершенных политик безопасности.

Основу *мандатной (полномочной) политики безопасности* составляет мандатное управление доступом (Mandatory Access Control - MAC), которое подразумевает, что:

- все субъекты и объекты системы должны быть однозначно идентифицированы;
- задан линейно упорядоченный набор меток секретности;

- каждому объекту системы присвоена метка секретности, определяющая ценность содержащейся в нем информации - его уровень секретности в АС;
- каждому субъекту системы присвоена метка секретности, определяющая уровень доверия к нему в АС - максимальное значение метки секретности объектов, к которым субъект имеет доступ; метка секретности субъекта называется его уровнем доступа.

Основная цель мандатной политики безопасности – предотвращение утечки информации от объектов с высоким уровнем доступа к объектам с низким уровнем доступа, т. е. противодействие возникновению в АС информационных каналов сверху вниз.

Чаще всего мандатную политику безопасности описывают в терминах, понятиях и определениях свойств модели Белла-Лапалуда, которая будет рассмотрена ниже. в рамках данной модели доказывается важное утверждение, указывающее на принципиальное отличие систем, реализующих мандатную защиту, от систем с дискреционной защитой: *если начальное состояние системы безопасно, и все переходы системы из состояния в состояние не нарушают ограничений, сформулированных политикой безопасности, то любое состояние системы безопасно.*

Кроме того, по сравнению с АС, построенными на основе дискреционной политики безопасности, для систем, реализующих мандатную политику, характерна более высокая степень надежности. Это связано с тем, что МБО такой системы должен отслеживать не только правила доступа субъектов системы к объектам, но и состояния самой АС. Таким образом, каналы утечки в системах данного типа не заложены в нее непосредственно (что мы наблюдаем в положениях предыдущей политики безопасности), а могут появиться только при практической реализации системы вследствие ошибок разработчика. В дополнении к этому правила мандатной. .политики безопасности более ясны и просты для пони мания разработчиками и пользователями АС, что также является фактором, положительно влияющим на уровень безопасности системы. С другой стороны, реализация систем с политикой безопасности данного типа довольно сложна и требует значительных ресурсов вычислительной системы.

### 3.4. Разработка и реализация формальных политик безопасности

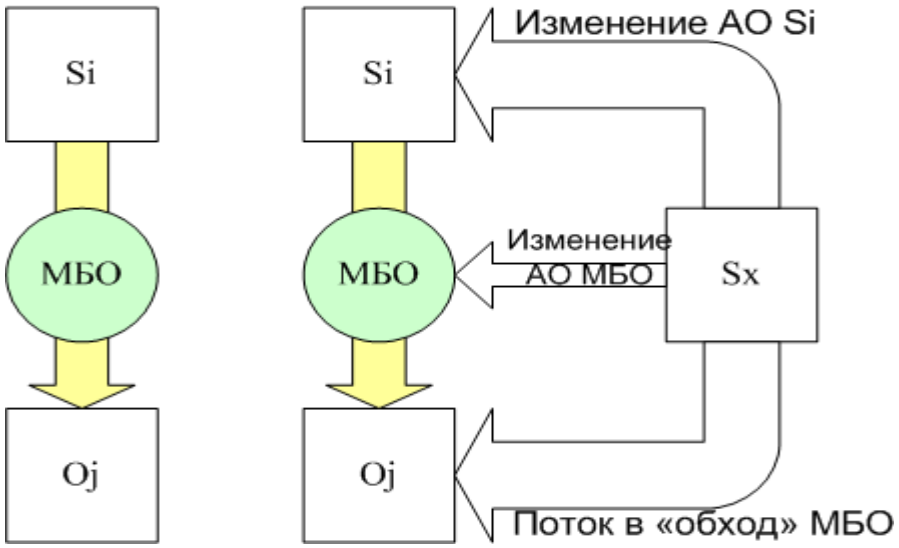



Рис. 3.3. Возможные пути нарушения политики безопасности

Представляется очевидным, что при изменении функционально ассоциированных с субъектом реализации политики безопасности (МБО) объектов могут измениться и свойства самого МБО, заключающиеся в фильтрации потоков, и как следствие могут возникнуть потоки, принадлежащие множеству N. Введем в связи с этим понятие корректности субъектов.

*Определение 10.* Пара субъектов Si и Sj называется не влияющими друг на друга (или корректными относительно друг друга), если в любой момент времени отсутствует поток (изменяющий состояние объекта) между ассоциированным объектом субъекта Si(Osi) и Sj(Osj), причем Osj не является ассоциированным объектом Si, а Osi не является ассоциированным объектом Sj.

Дадим некоторые пояснения к определению: «изменение состояния объекта» трактуется в данном определении как нетождественность объектов в соответствующие моменты времени, но при этом подчеркнуто, что операция изменения объекта локализована в субъекте, с которым этот объект не ассоциирован. Смысл понятия корректности можно пояснить на примере: существующие в едином пространстве ОП программы не должны иметь функциональных возможностей изменения «чужого» вектора кода и состояния переменных.

Вообще говоря, можно сформулировать более жесткое определение.

*Определение 11.* Пара субъектов Si и Sj называется абсолютно не влияющими друг на друга (или абсолютно корректными относительно друг друга), если в условиях определения

10 множества ассоциированных объектов указанных субъектов не имеют пересечения.

Абсолютная корректность легко достижима в случае виртуального адресного пространства.

Определение абсолютной корректности позволяет сформулировать достаточные условия гарантированного осуществления только легального доступа.

*Утверждение 1 (достаточное условие гарантированного выполнения политики безопасности в АС 1).*

Монитор безопасности объектов разрешает порождение потоков только из множества L, если все существующие в системе субъекты абсолютно корректны относительно него и друг друга.

Доказательство. Условие абсолютной корректности (по определению 11) предполагает неизменность функционально ассоциированных объектов МБО (поскольку потоков, изменяющих ассоциированные объекты МБО, не существует). С другой стороны, такие потоки могут появиться при изменении ассоциированных объектов, принадлежащих другим субъектам АС (изменятся свойства субъекта, в том числе (возможно) и по порождению потоков к МБО). Условие корректности субъектов относительно друг друга делает это невозможным (по определению абсолютной корректности). Это, в свою очередь, означает, что МБО реализует только потоки из подмножества L. Утверждение доказано.

Однако сформулированное утверждение накладывает весьма жесткие и трудноисполнимые условия на свойства субъектов в АС. Кроме того, невозможно гарантировать корректность любого субъекта, активизируемого в АС, относительно МБО. В связи с этим логично ограничить множество порождаемых субъектов, которые априорно корректны относительно МБО. В связи с этим введем определение монитора порождения субъектов (по аналогии с монитором обращений) и монитора безопасности субъектов.

*Определение 12.* Монитор порождения субъектов (МПС) - субъект, активизирующийся при любом порождении субъектов.

По аналогии с переходом от МО к МБО введем понятие монитора безопасности субъектов.

*Определение 13.* Монитор безопасности субъектов (МБС) - субъект, который разрешает порождение субъектов только для фиксированного подмножества пар активизирующих субъектов и порождающих объектов.

Воздействие МБС выделяет во всем множестве субъектов S подмножество разрешенных E. Заметим также, что если в подмножество субъектов в момент времени t включается субъект МБС, то первым аргументом операции Create может быть только субъект, входящий во множество субъектов, а аргумент-объект, вообще говоря, любым.

Сформулируем теперь ряд базовых определений, которые в дальнейшем будут

повсеместно использоваться.

*Определение 14*. АС называется замкнутой по порождению субъектов, если в ней действует МБС, разрешающий порождение только фиксированного конечного подмножества субъектов для любых объектов-источников, рассматриваемых для фиксированной декомпозиции АС на субъекты и объекты.

При рассмотрении вопросов реализации защищенных сред будет использоваться термин «замкнутая программная среда», который по существу эквивалентен приведенному выше определению.

Однако замкнутости АС по порождению субъектов недостаточно для описания свойств системы в части защищенности, поскольку необходимо обеспечить корректность порождаемых МБС субъектов относительно его самого и МБО. Механизм замкнутой программной среды сокращает множество возможных субъектов до некоторого множества фиксированной мощности, но при этом допускает существование некорректных субъектов, включенных в замкнутую среду.

Сформулируем определение изолированности АС.

*Определение 15.* Множество субъектов АС называется изолированным (абсолютно изолированным), если в ней действует МБС и субъекты из порождаемого множества корректны (абсолютно корректны) относительно друг друга и МБС.

*Следствие.* Любое подмножество субъектов изолированной (абсолютно изолированной АС), включающее МБС, также составляет изолированную (абсолютно изолированную) среду.

*Следствие*. Дополнение изолированной (абсолютно изолированной) АС субъектом, корректным (абсолютно корректным) относительно любого из .числа входящие в изолированную (абсолютно изолированную) среду, оставляет ее изолированной (абсолютно изолированной).

Теперь возможно переформулировать достаточное условие гарантированного выполнения политики безопасности следующим образом.

*Утверждение 2 (достаточное условие гарантированного выполнения политики безопасности в АС 2).*

Если в абсолютно изолированной АС существует МБО и порождаемые субъекты абсолютно корректны относительно МБО, а также МБС абсолютно корректен относительно МБО, то в такой АС реализуется только доступ, описанный в ПРД. Доказательство. Из определения абсолютной изолированности следует возможность существования в АС только конечного множества субъектов, которые, в свою очередь, корректны относительно МБС (по определению 16 и следствию из него).

Далее, по условию утверждения (корректность МБО относительно любого из

порождаемых субъектов и МБС) ассоциированные объекты могут изменяться только самим МБО, следовательно, в АС реализуются только потоки, принадлежащие множеству L. Утверждение доказано.

Легко видеть, что данное утверждение является более конструктивным относительно предыдущего достаточного условия гарантированной защищенности, поскольку ранее требовалась корректность МБО относительно произвольного субъекта, что практически невозможно. В данном же случае множество субъектов ограничено за счет применения механизма МБС и возможно убедиться в попарной корректности порождаемых субъектов.

При рассмотрении технической реализации изолированности субъектов в АС будет употребляться термин «изолированная программная среда» (ИПС), который описывает механизм реализации изолированности для конкретной программно-аппаратной реализации АС и при соответствующей декомпозиции на субъекты и объекты.

При рассмотрении операции порождения субъекта возникает весьма важная проблема, связанная с тем, что в реальных АС одинаково поименованные объекты могут иметь различное состояние в пространстве (например, быть размещенными в различных каталогах) или во времени.

Предположим, что зафиксировано состояние объекта Om в некоторый момент временит. Будем обозначать состояние объекта Om в момент времени t как 0m[t].

*Определение 16.* Операция порождения субъекта Create(Sk,Om)->Si называется порождением с контролем неизменности объекта, если для любого момента времени t>to, в который активизирована операция порождения объекта Create, порождение субъекта Si возможно только при тождественности объектов 0m[to] и 0m[t].

Следствие. В условиях определения 16 порожденные субъекты Si[tl]H Si[t2] тождественны, если tl>to и t2>to. При tl=t2 порождается один и тот же субъект.

При порождении субъектов с контролем неизменности объекта в АС допустимы потоки от субъектов к объектам-источникам, участвующим в порождении субъектов, с изменением их состояния.

*Утверждение 3 (базовая теорема ИПС)*

Если в момент времени to в изолированной АС действует только порождение субъектов с контролем неизменности объекта и существуют потоки от любого субъекта к любому объекту, не противоречащие условию корректности (абсолютной корректности) субъектов, то в любой момент времени t>to АС также остается изолированной (абсолютно изолированной).

Доказательство. По условию утверждения в АС возможно существование потоков, изменяющих состояние объектов, не ассоциированных в этот момент времени с каким-либо субъектом. Если объект с измененным состоянием не является источником для порождения

субъекта, то множество субъектов изолированной среды нерасширяемо, в противном случае (измененный объект является источником для порождения субъекта) по условиям утверждения (порождение субъекта с контролем) порождение субъекта невозможно. Следовательно, мощность множества субъектов не может превышать той, которая была зафиксирована до изменения состояния любого объекта. Последствию из определения 16 (о замкнутости множества субъектов в ИПС с невозрастанием мощности множества субъектов) получим, что множество субъектов АС изолировано. Утверждение доказано.

Можно сформулировать методологию проектирования гарантированно защищенных АС. Сущность данной методологии состоит в том, что при проектировании защитных механизмов АС необходимо опираться на совокупность приведенных выше (утверждения 1-3) достаточных условий, которые должны быть реализованы для субъектов, что гарантирует защитные свойства, определенные при реализации МБО в АС (т. е. гарантированное выполнение заданной МБО политики безопасности).

Рассмотренная концепция изолированной программной среды является расширением зарубежных подходов к реализации ядра безопасности.

*Ядро безопасности* - специальный компонент механизма защиты, занимающий внешнее по отношению к другим механизмам положение и предназначенный для решения задач общей организации защиты информации и контроля работы других компонентов механизмов защиты. Соответственно такому назначению к ядру предъявляются особые требования, а для создания сформулированны особые подходы. Вообще говоря, идея централизации некоторых, наиболее ответственных процедур защиты информации и особенно - процедур управления механизмами защиты не является новой: возраст этой идеи уже превышает два десятилетия. Правда, первоначально ядро безопасности представлялось как некоторый комплекс программ, выполняющий особые функции защиты и организованный особо тщательно. Поэтому концепция ядра безопасности развивалась как в плане расширения выполняемых функций, так и в плане комплектности подходов к его построению. Ядро безопасности рассматривается как центральный компонент системы защиты и непосредственно выполняющая ряд важных функций защиты, таких как контроль, регистрация, уничтожение, сигнализация и др. Существо названных функций в самом общем виде заключается в следующем. Под контролем понимается систематическая проверка состояния и работоспособности всех средств и механизмов защиты информации, имеющихся в АС. Под регистрацией в современных системах обеспечения безопасности информации понимают совокупность средств и методов, предназначенных для регулярного сбора, фиксации, обработки и выдачи сведений о функционировании механизмов защиты, включая и ведение регистрационных журналов об обращениях к защищаемым данным и программам. Под уничтожением в системах защиты понимается своевременное уничтожение всех тех

данных и программ, которые больше не нужны для дальнейшего функционирования АС, но сохранение которых может послужить причиной несанкционированного получения информации или способствовать такому получению. Отсюда однозначно вытекает важность данной функции. Под сигнализацией понимается решения ряда задач: предупреждение пользователей о необходимости соблюдения мер защиты, информирование службы безопасности о выходе из строя или нарушении или попытке нарушения безопасности и т.п.

Обычно модель функционирования ядра безопасности изображается в виде следующей схемы, представленной на рис. 4.

На рис. 4 "база данных защиты" означает объект, содержащий в себе информацию о потоках множества L (защита по "белому списку" - разрешения на потоки) или N (защита по "черному списку" - запрещение на потоки).

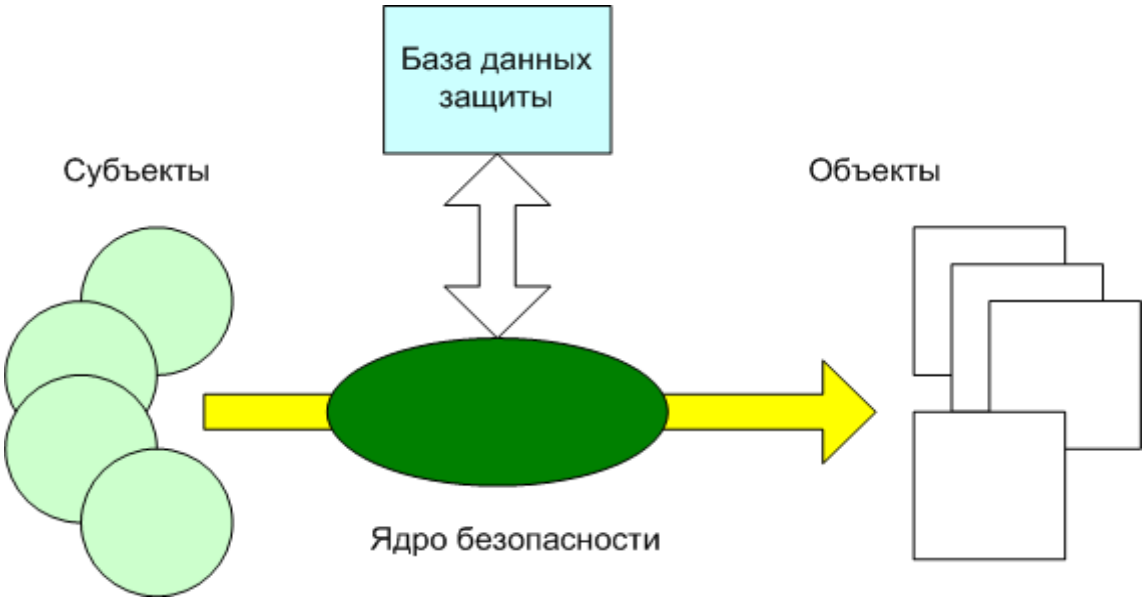



Рис. 3.4. Классическая модель ядра безопасности

Для учета влияния субъектов в АС необходимо рассматривать расширенную схему взаимодействия элементов системы реализаций и гарантирования ПБ.

В рис. 3.5 подчеркнута роль монитора безопасности субъектов при порождении субъектов из объектов. Взаимодействие субъектов и объектов при порождении потоков уточнено введением ассоциированных с субъектом объектов. Конструкция ОУ на схеме обозначает объект управления, т. е. объект, содержащий информацию о разрешенных значениях отображения Stream (об элементах множества L или N) и Create (элементы множества E). Объект управления может быть ассоциирован (ассоциированный объект - данные) как с МБО, такие МБС.

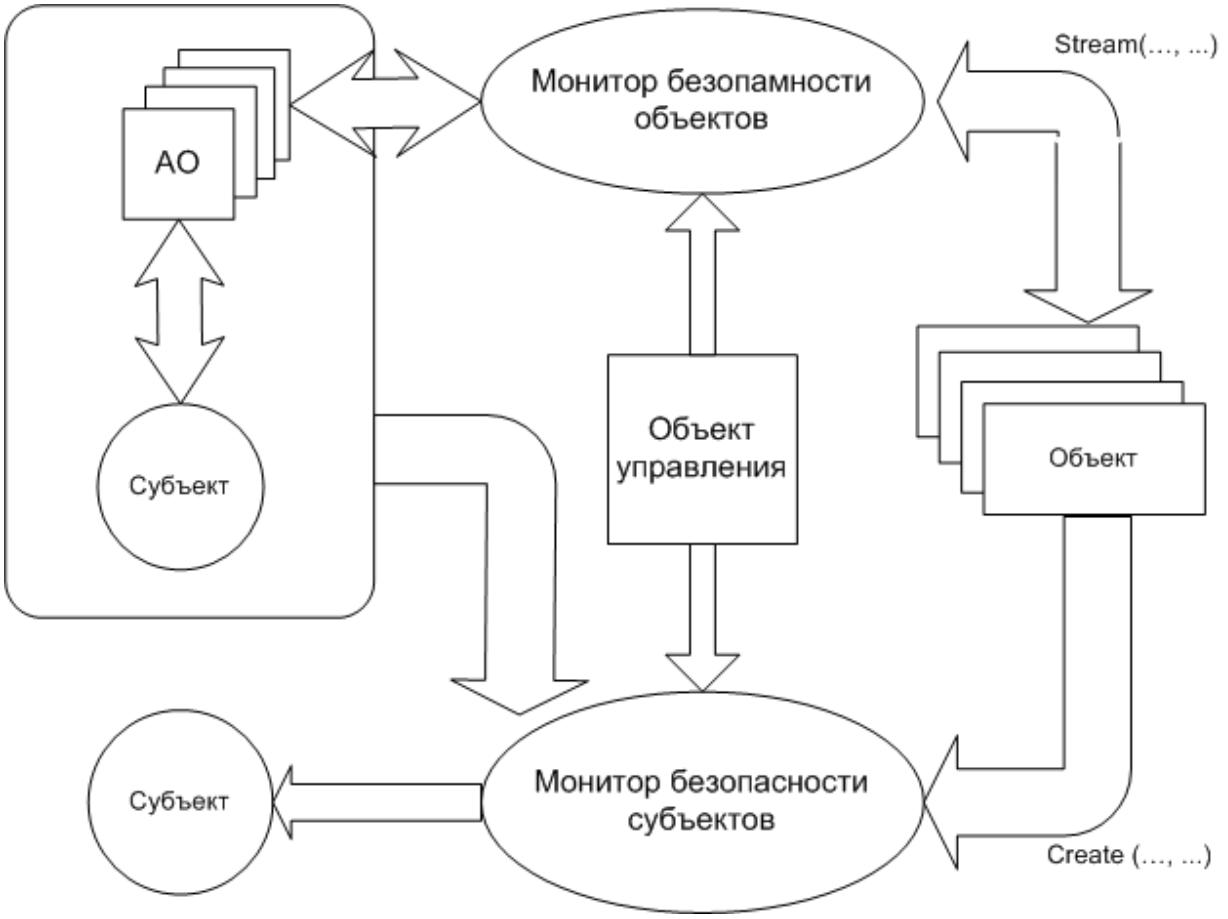



Рис. 3.5. Ядро безопасности с учетом контроля порождения субъектов

Перейдем к описанию практических методов построения ИПС. Целью рассмотрения практических подходов является иллюстрация тезиса о том, что достаточные условия гарантированной защищенности могут быть практически выполнены в реальных АС.

Опираясь на утверждение 3 (базовую теорему ИПС), сформулированное и доказанное в предыдущей части, опишем метод субъектно-объектного взаимодействия в рюмках ИПС для более конкретной архитектуры АС.

Из утверждения 3 следует, что для создания гарантированно защищенной АС (в смысле выполнения заданной политики безопасности) необходимо:

1. Убедиться в попарной корректности субъектов, замыкаемых в ИПС (либо убедиться в корректности любого субъекта относительно МБО и МБС).

2. Спроектировать и реализовать программно (или программно - аппаратно) МБС так, чтобы:

- для любого субъекта и любого объекта производился контроль порождения субъектов (т. е. чтобы реализация МБС соответствовала его определению);
- порождение любого субъекта происходило с контролем неизменности объекта-источника,

3. Реализовать МБО в рамках априорно сформулированной политики безопасности.

Надо заметить, что приводимые выше утверждения верны только тогда, когда описанная и реализованная политика безопасности не нарушает их условий (проверка данного факта зависит от модели ПБ и является отдельной весьма важной задачей).

Кроме того, необходимо обратить внимание на следующее. Объект управления, который является ассоциированным объектом МБС (обычно ассоциированный объект - данные), играет решающую роль в проектировании ИПС. При возможности изменения состояния объекта управления потенциально возможно «размыкание» программной среды, т. е. добавление к множеству разрешенных субъектов дополнительных, реализующих злоумышленные функции. С другой стороны, процесс управления безопасностью подразумевает возможность изменения объекта управления (подробнее в части 3). Возможность изменения объекта управления (реализация потока Stream (субъект управления, АО объекты субъекта управления)->ОУ) должна присутствовать для выделенных субъектов (возможно с дополнительным условием активизации этого субъекта выделенным пользователем (пользователями)).

Важную роль при проектировании ИПС играет свойство АС, заключающееся в поэтапной активизации субъектов из объектов различного уровня представления информации. Рассмотрим в таблице 3.1. иерархию уровней при загрузке операционной системы.

В таблице выделен термин «сектор» для обозначения представления объекта аппаратно-программного уровня. Он обозначает непрерывную последовательность элементов хранения (байт) на материальном носителе, характеризуемую местом расположения.

Термин «файл» обозначает абстрактный объект, построенный по списочной структуре из объектов «сектор». Объекты типа «файл» и «сектор» выделены исключительно исходя из типовой архитектуры объектов АС.

Таблица 3.1. Иерархия уровней при загрузке ОС

| Уровень | Субъект | Локализация | Представление информации | Через какие функции реализуются потоки |
|---|---|---|---|---|
| 0 | Субъект аппаратно-программного уровня | ПЗУ | сектора | через микропрограммы ПЗУ |

| | | | | |
|---|---|---|---|---|
| 1 | Субъект уровня первичной загрузки | Загрузчик ОС | сектора | через Bios или первичный загрузчик |
| 2 | Субъект уровня вторичного загрузчика (драйвер) | драйверы ОС | сектора | через Bios или первичный загрузчик |
| 3 | Субъект уровня ОС | ядро ОС | файлы | через драйверы |
| 4 | Субъект пользовательского уровня | Прикладные приложения | файлы | через ядро ОС |

В общем случае можно говорить о рекурсивной структуре объектов некоторого уровня, вмещающей объекты предыдущего уровня. На нулевом уровне первичный объект (элементарная структура нижнего уровня) в таблице 3.1. соответствует термину «сектор».

С учетом иерархической структуры представления объектов можно говорить о том, что в начальные этапы активизации АС декомпозиция на субъекты и объекты динамически изменяется. Следовательно, основная теорема ИПС может быть применима только на отдельных интервалах времени, когда уровень представления объектов постоянен и декомпозиция фиксирована. Можно утверждать, что ИПС, действующую от момента активизации до момента окончания работы АС, невозможно сформировать в начальный момент активизации АС.

Пусть в АС выделяется конечное число уровней представления объектов U={0, ..., R}, R - максимальный уровень представления объекта.

С точки зрения выполнения условий утверждения 3 имело бы смысл говорить о некотором "стационарном" состоянии АС, когда в отображениях Stream и Create участвуют только объекты уровня R. Тогда реализация МБС может быть значительно упрощена (в том смысле, что все аргументы-объекты операции Create имеют тот же уровень). Необходимо обратить внимание на то, что такое требование, с одной стороны, может накладывать ограничительные условия на свойства прикладного ПО (невозможность инициирования потоков, включающих объекты уровня менее R, прикладными программами), а с другой стороны, быть следствием проектировочных решений реализации субъекта, локализованного в ядре операционной системы (примером является ОС Windows NT 4.0, запрещающая операции ниже уровня "файл" со стороны субъектов прикладного уровня).

Практическая реализация всех операционных систем позволяет выделить две фазы их

работы: активизация субъектов с ростом уровня представления объектов (фаза загрузки или начальная фаза) и фаза стационарного состояния (когда уровень представления объектов не увеличивается). Конечно, необходимо сделать оговорку касающуюся возможности реализации потоков к объектам нижнего уровня (операционные системы типа DOS, в которых возможна операция с любым объектом нижнего уровня (сектор) из программ прикладного уровня).

Тогда практическая реализация ИПС может состоять из двух этапов: предопределенное выполнение начальной фазы, включающее в себя момент активизации МБС (и МБО), и работа в стационарной фазе в режиме ИПС (возможно, с контролем неизменности объектов-источников).

Введем понятие последовательности активизации компонент АС. Смысл вводимых понятий и формулируемых ниже утверждений состоит в необходимости приведения субъектов АС в одно и то же состояние после активизации первичного субъекта аппаратно - программного уровня, или, иначе говоря, в задании предопределенной последовательности активизации субъектов АС.

Обозначим: ZL-последовательность пар (i, j)t (t=0, 1, 2, ...,1-l –моменты времени) длины 1, такие, что Create (Si,0j)[1]->Sm[t+1].

Обозначим также:

Sz - множество всех субъектов, включенных в последовательность ZL,

Oz - множество всех объектов, включенных в последовательность ZL.

Для многопотоковых АС можно рассматривать несколько (возможно, зависимых друг от друга) последовательностей ZL и соответственно множеств Sz и Oz.

Определение 17. Состоянием АС в момент времени t называется упорядоченная совокупность состояний субъектов.

*Утверждение 4 (условие одинакового состояния АС).*

Состояние АС в моменты времени txl и tx2 (txl и tx2 исчисляются для двух отрезков активности АС от нулевого момента активизации АС tol и to2- например, включения питания аппаратной части) одинаково, если:

1.txl=tx2,

2. тождественны субъекты Si[tol] и Si[to2],

3. неизменны все объекты из множества Oz,

4. неизменна последовательность ZL.

Доказательство (по принципу математической индукции)

Верность утверждения при t=1 следует из определения тождественности субъектов.

Пусть утверждение верно для t==k<l.

Тогда в момент времени k+1 могут быть порождены только тождественные субъекты,

поскольку тождественны активизирующие субъекты (по предположению индукции) и по условию утверждения неизменны элементы множества Oz. Длина 1 последовательности ZL определяется:

1. По признаку невозможности управления субъектами, принадлежащими множеству Sz, со стороны пользователя (в противном случае последовательность активизации субъектов может быть изменена).

2. По признаку доступности для контроля неизменности всех объектов из множества Oz.

3. По признаку невозрастания уровня представления информации (в данном случае имеется в виду, что существует момент времени tx такой, что для любого t>tx объект-аргумент Oj операции Stream(Si, Oj) принадлежит одному уровню представления).

Необходимо заметить, что последовательность ZL локализуется в некотором объекте либо совокупности объектов (например, для DOS последовательность активизации субъектов предопределена содержанием файлов AUTOEXEC.BAT и CONFIG.SYS) и неизменность последовательности ZL тождественна неизменности указанных объектов, для ОС Windows NT последовательность активизации компонент определена содержанием соответствующих ключей реестра (registry).

Пусть в последовательности ZL можно выделить zi такое, что для любого Zk, k>i отображений Create и Stream используют только объекты уровня R. Другими словами, с момента времени i наступает стационарная фаза функционирования АС.

В этих условиях, а также при попарной корректности субъектов и действии МБС с контролем неизменности объектов-источников на уровне R с момента времени m>k верно:

*Утверждение 5 (достаточное условие ИПС при ступенчатой загрузке)*

При условии неизменности ZL и неизменности объектов из Oz в АС с момента времени установления неизменности ZL и Oz действует изолированная программная среда.

Доказательство. Необходимо заметить, что все условия утверждения 5 соответствуют утверждению 4. Уточнения касаются структуры последовательности ZL.

Согласно утверждению 4 с момента временило до момента t==l действует изолированная (в рамках) Sz программная среда.

Для доказательства утверждения необходимо убедиться в том, что:

- МБС в момент времени t=m гарантировано активизируется,

- в любой момент t>m программная среда изолирована.

Первое следует из утверждения 4 (при 1=т состояние программной среды всегда будет одинаково, следовательно, всегда будет активизирован субъект МБС). Второе следует из определения МБС и условия теоремы.

С момента времени t==0 до момента времени 1 программная среда изолирована, с момента времени t>m программная среда также изолирована, следовательно, АС

изолирована при любом t>0. Утверждение доказано.

Используя утверждения 3,4 и 5, рассмотрим процесс практического проектирования защищенного фрагмента АС.

Первоначально необходимо убедиться в выполнении условий корректности или абсолютной корректности для субъектов, участвующих в порождении ИПС. Указанные субъекты в основном могут быть локализованы на уровне программно-аппаратной компоненты ЭВМ (программы ПЗУ, загрузчики операционных сред), т. е. работать на уровне, близком к взаимодействию с оборудованием АС, либо на уровне операционной среды. Доказательство корректности субъектов программно-аппаратного уровня значительно отличается от соответствующих доказательств для субъектов прикладного уровня. В связи с этим выделим проверку условий корректности субъектов в два шага. Шагом 1 назовем доказательство корректности субъектов программно-аппаратного уровня. Понятие модуль обозначает реализацию объекта- источника, а совокупность субъекта, порожденного из объекта-источника и всего множества ассоциированных с этим субъектом объектов в течение всего времени существования субъекта, называется, как правило, процессом (или задачей, заданием).

Далее необходимо определить состав программных средств базовой вычислительной среды, т. е. определить конкретную операционную среду, дополнительные программные средства сервиса (например, программные оболочки или средства телекоммуникации) и программные средства поддержки дополнительного оборудования (программы управления принтером и др.). После этого наступает самый трудоемкий этап (Шаг 2), на котором необходимо убедиться в корректности субъектов описанного базового набора программных средств. При этом важно заметить следующее.

В составе ПО АС не должно быть целого класса возможностей -назовем их инструментальными. Прежде всего это возможность изменения состояния ассоциированных объектов со стороны субъекта (например, изменение содержимого оперативной памяти) других субъектов (изменение содержания подразумевает существование операций Stream типа запись), возможность инициирования и прекращения выполнения процессов нестандартным образом (помимо механизмов операционной среды). Кроме того, при реализации МБС и МБО на стационарной фазе функционирования АС необходимо отсутствие в любых субъектах, замкнутых в ИПС, операций порождения потоков Stream к объектам уровня k<R.

Обобщенно достаточные условия к базовому набору ПО можно сформулировать следующим утверждением.

*Утверждение 6 (требования к субъектному наполнению изолированной программной среды)*

Для того чтобы ИПС поддерживалась в течение всего времени активности АС, достаточно, чтобы в составе программного обеспечения, могущего быть инициированным в ИПС, не было функций порождения субъектов и прекращения их работы, кроме заранее предопределенных при реализации МБС, и не существовало возможностей влияния на среду выполнения (под средой выполнения понимается множество ассоциированных объектов) любого процесса, а также инициирования потоков к объектам логического уровня менее R.

Поясним требование невозможности прекращения выполнения субъекта каким-либо иным образом, кроме предопределенного. В данном случае необходимо учитывать, что во множестве субъектов, замкнутых в ИПС, выделены два особых субъекта - МБС и МБО. Прекращение существования МБС означает нарушение условия замкнутости среды, а прекращение существования МБО означает допустимость потоков множества N, т. е. несанкционированный доступ.

Шаг 3 заключается в проектировании и разработке программных или программно-аппаратных средств защиты в АС, а затем и их тестировании. Он подразумевает проектирование и реализацию в заданном множестве субъектов МБС и МБО.

Шаг 4 заключается в "замыкании" всего комплекса программного обеспечения, включая и средства защиты, в изолированную программную среду.

Итак, показано, что основными элементами поддержания изолированности программной среды являются контроль целостности и контроль порождения процессов.

Выше мы уже сформулировали понятия МБС и порождения субъектов с контролем их неизменности. Необходимо заметить, что для достоверного контроля неизменности объекта (т. е. с вероятностью ошибки, равной 0) необходимо убедиться в полном тождестве проверяемого объекта и образца. Из этого следует, что эталон должен содержать не меньше информации, чем проверяемый объект. Из этого в свою очередь следует, что эталонный объект должен быть как минимум одинаковой длины с проверяемым. На практике такой подход может быть применен с серьезными ограничениями (например, для объектов небольшого объема типа программ ПЗУ или загрузчиков ОС).

В связи с этим для контроля целостности применяют объекты, содержащие информацию, зависящую от всего содержания объекта, но тем не менее значительно меньшего объема, вычисленную при помощи класса функций типа «хэш-функций». Очевидно, что в этом случае процесс установления неизменности объекта становится вероятностным.

Исходя из данного факта невозможно говорить о гарантированных (детерминировано) свойствах системы (поскольку неизменность объекта гарантируется лишь с некоторой вероятностью, не равной 1). Следовательно, все условия утверждений выполняются с некоторой вероятностью, зависящей от свойств применяемых для контроля целостности хэш-функций. Для подчеркивания изменившихся условий будем говорить далее не о

контроле неизменности объекта, а о контроле целостности (КЦ) объекта.

Необходимо отметить также, что в процедуре контроля неизменности (которая теперь принимает вероятностный характер) участвуют как минимум два объекта: объект контроля и эталонный объект (хэш-значение), а также субъект, реализующий хэш-функцию и производящий сравнение.

Поэтому для субъекта контроля целостности важным является выполнение следующих условий:

- качественный алгоритм контроля целостности (термин «качественный» будет пояснен ниже);

- контроль реальных данных (т. е. отображение состояния контролируемого и эталонного объемов в ассоциированные объекты-данные субъекта контроля целостности, совпадающее с тождественным).

Поясним подробнее второй пункт. Контроль целостности всегда сопряжен с чтением данных (т. е. с инициированием потоков от объектов к ассоциированным объектам-данным субъекта контроля целостности, причем потоки могут соответствовать различному уровню представления информации - чтение по секторам, по файлам и т. д.). Например, встроенный в BIOS ПЭВМ субъект (практически это программная закладка - см. ниже) может навязывать при чтении вместо одного сектора другой или редактировать непосредственно буфер, в который были прочитаны данные. Аналогичный эффект может быть вызван субъектами операционной среды, например, субъектами, локализованными в первичных загрузчиках ОС. С другой стороны, даже контроль самого BIOS может происходить "под наблюдением" какой-либо дополнительной аппаратуры и не показать его изменения. Аналогичные эффекты могут возникать и при обработке файла. Цель организации режима чтения реальных данных состоит в тождественном отображении параметров чтения на АО субъекта чтения (поток от АО субъекта КЦ к АО субъекта чтения) и тождественном отображении считываемого объекта (в соответствии с параметрами, переданными субъекту чтения) к ассоциированным объектам-данным субъекта КЦ.

Поясним теперь понятие качественного КЦ с точки зрения математических свойств функции КЦ. Предположим, что имеется некоторый объект F и некоторый алгоритм H, преобразующий объект F в некоторый объект M, который представляется словом того же языка, но меньшей длины. Этот алгоритм таков, что при случайном равновероятном выборе двух объектов F1 и F2 из множества возможных соответствующие им объекты MI=H(F1) и M2==H(F2) с высокой вероятностью различны. Тогда проверка целостности данных строится так: рассматриваем объект F, по известному алгоритму H строим K=H(F) и сравниваем M, заранее вычисленное как M = H(F), с K. При совпадении считаем объект неизменным. Алгоритм H называют, как правило, хэш-функцией, или реже контрольной суммой, а число

M - хэш-значением.

Качество КЦ определяется в данном случае выполнением следующих условий:

1. По известному объекту M=H(F) нахождение другого объекта G, не тождественного F, такого, что M==H(G), является задачей с трудоемкостью не менее заданной Th.

2. Объект M должен быть недоступен для изменения.

3. Длина объекта M должна обеспечивать условную вероятность P(H(Fi)=H(F2)/Fi не тождествен F2) не более заданной Pь.

Поясним смысл этих условий. Пусть программа злоумышленника изменила объект F (статическое искажение). Тогда, вообще говоря, хэш-значение M для данного объекта изменится. Если субъекту злоумышленника доступен для изменения объект M (существует соответствующий поток), то он может по известному алгоритму H вычислить новое хэш-значение для измененного объекта и заместить им исходное.

Пусть хэш-значение недоступно, тогда можно попытаться так построить измененный объект, чтобы хэш-значение его не изменилось; принципиальная возможность этого имеется, поскольку отображение, задаваемое алгоритмом хэширования H, не биективно (неоднозначно).

Таким образом, при условии недоступности хэш-значения для изменения и доступности для изменения объекта-источника трудоемкость нарушения ИПС с КЦ объектов-источников (т. е. возможность породить субъект из объекта-источника, не тождественного исходному объекту) совпадает с Tн. При однократной попытке инициировать субъект из случайно равновероятно выбранного объекта-источника вероятность нарушения ИПС (успешное порождение субъекта) не превосходит Ph. Итак, «качество» ИПС определяется свойствами хэш-функции H, а именно: величинами Tн и Pн.

Обобщим приводимые выше рассуждения в методе "безопасной загрузки", или ступенчатого контроля. Он заключается в постепенном установлении неизменности компонент программно-аппаратной среды:

1. Сначала проверяется неизменность программ ПЗУ, при положительном исходе через проверенные на целостность программы ПЗУ считывается загрузочный сектор и драйверы операционной системы (по секторам) и их неизменность также проверяется, кроме того, проверяется целостность объекта, определяющего последовательность активизации компонент;

2. Через функции чтения, проверенной ОС, инициируется процесс контроля порождения процессов (реализация МБС);

3. Инициирование процесса контроля доступа к объектам завершает проектирование гарантировано защищенной АС.

Рассматривая вопросы программно-технической реализации ИПС, необходимо заметить,

что мощность множества субъектов в некотором сегменте АС (выделенном по признаку принадлежности одной ЭВМ) с момента включения питания до момента запуска процессов пользователя увеличивается. Первоначально активизируются субъекты аппаратно-программного уровня (программы ПЗУ), затем указанные субъекты порождают из объектов-источников данного уровня (это, как правило, сектора внешних носителей информации) субъектов уровня операционной среды.

Субъекты уровня операционной среды, как уже отмечалось, также делятся на два подуровня: нижний уровень — субъекты — первичные загрузчики ОС (работающие с информацией уровня секторов) и верхний уровень - субъекты-драйверы (порождаемые субъектами - первичными загрузчиками из объектов-секторов), работающие с объектами уровня «файл» (последовательности секторов). На этапе перехода от субъектов-загрузчиков к субъектам-драйверам происходит переход и к другой декомпозиции АС на объекты (от секторов к файлам). Указанная иерархия действует в любой известной на сегодняшний день АС и естественным образом предопределяет архитектуру, в рамках которой формируется и функционирует ИПС.

Например, аппаратная архитектура ПЭВМ типа IBM PC задает следующие этапы активизации различных субъектов АС. При включении питания ПЭВМ происходит тестирование ОП, инициализация таблицы векторов прерываний и поиск расширений BIOS. При их наличии управление передается на них. После отработки расширений BIOS в память считывается первый сектор дискеты или винчестера и управление передается на него (образуется код загрузчика), затем код загрузчика считывает драйверы операционной системы, далее интерпретируются файлы конфигурации, подгружается командный интерпретатор и выполняется файл автозапуска.

При реализации ИПС на нее должна быть возложена функция контроля запусков программ и контроля целостности.

При описании методологии проектирования ИПС упоминалась проблема контроля реальных данных. Эта проблема состоит в том, что контролируемая на целостность информация может представляться по-разному на разных уровнях.

Внедренный в систему субъект может влиять на процесс чтения-записи данных на уровне файлов (или на уровне секторов) и предъявлять системе контроля некоторые другие вместо реально существующих данных. Этот механизм неоднократно реализовался в STELS-вирусах. Однако верно утверждение.

*Утверждение 7 (достаточное условие чтения реальных данных*)

Если субъект, обслуживающий процесс чтения данных (т. е. указанный субъект инициируется запрашивающим данные субъектом и участвует в потоке), содержал только функции тождественного отображения данных на ассоциированные объекты-данные любого

субъекта, инициирующего поток чтения, и целостность объекта-источника для этого субъекта зафиксирована, то при его последующей неизменности чтение с использованием порожденного субъекта будет чтением реальных данных.

Доказательство. Верность утверждения следует из определения тождественности субъекта и из условия утверждения, гарантирующего неизменность объекта-источника.

Необходимо и здесь сделать оговорку о вероятностном характере установления неизменности и говорить, что чтение реальных данных возможно с вероятностью, определяемой алгоритмом КЦ.

Метод ступенчатого контроля не противоречит утверждениям 4 и 5 и предусматривает разделение последовательности активизации компонент ZL на подпоследовательности с одинаковым уровнем представления информации.

Реализация метода ступенчатого контроля целостности должна удовлетворять условиям утверждения 4.

Опишем практическую реализацию сформулированных методов.

Выше было сказано о том, что субъект контроля неизменности объектов, входящих в процедуры активизации АС и объектов, описывающих последовательность активизации компонент, должен быть активен уже на этапе работы субъектов аппаратно-программного уровня, но его объект-источник технически не может быть проверенна неизменность. В связи с этим подчеркнем весьма важный факт для любых реализаций ИПС.

*Аксиома 5.* Генерация ИПС рассматривается в условиях неизменности конфигурации тех субъектов АС, которые активизируются до старта процедур контроля целостности объектов Oz и последовательности ZL. Неизменность данных субъектов обеспечивается внешними по отношению к самой АС методами и средствами. При анализе или синтезе защитных механизмов свойства указанных субъектов являются априорно заданными.

При решении практических вопросов генерации ИПС можно выделить три самостоятельных направления.

Первое из них связано с использованием внешних по отношению к АС субъектов (как правило, размещенных на внешнем носителе), целостность которых гарантируется методами хранения или периодического контроля. Предопределенность активизации субъектов, локализованных на внешних носителях, обеспечивается свойствами субъектов аппаратно-программного уровня (например, возможно установить такую аппаратную конфигурацию ПЭВМ, при которой будет происходить загрузка операционной системы с ГМД).

Второе направление связано с локализацией ИПС в рамках территориально ограниченного рабочего места (как правило, ПЭВМ) и использует аппаратную поддержку для задания предопределенной последовательности активизации субъектов. Данное направление, как правило, включает и аппаратную поддержку аутентификации

пользователей.

Третье направление связано с реализацией метода доверенной загрузки операционной среды с использованием уже имеющихся в ней механизмов реализации и гарантирования ПБ.

Необходимо заметить, что в различные интервалы активности АС субъектами могут управлять различные пользователи, для которых множество разрешенных субъектов E различно, в связи с этим будем говорить о множестве Ei для i-го пользователя АС.

Будем также подразумевать, что перед установлением однозначного соответствия множества Ei пользователю i происходит процедура его аутентификации.

Ниже будут кратко рассмотрены все способы реализации ИПС. Говоря о первом из них необходимо отметить, что в его рамках можно рассматривать конфигурацию ИПС в двух вариантах:

- при локализации всех объектов-источников для порождения ИПС в рамках одного или нескольких внешних носителей;
- при локализации части объектов-источников на внешнем носителе, а части - во внешней памяти рабочего места.

Вторая конфигурация характеризуется потенциальной возможностью нарушения изолированности, состоящей в том, что активизация субъектов из объектов-источников, не принадлежащих внешнему носителю, может производиться вне рамок ИПС. В качестве примера можно рассмотреть ситуацию, когда программы запускаются в рамках операционной среды, загруженной с дискеты. С другой стороны, запуск указанных программ возможен и при загрузке ОС с другого носителя (в частности, с носителей рабочего места), и при этом возможна активизация и тех модулей, которые находятся на дискете.

Следовательно, основной задачей при использовании внешнего носителя для генерации ИПС является обеспечение невозможности активизации любого субъекта из объекта-источника внешнего носителя вне рамок зафиксированной для этого носителя последовательности активизации компонент ИПС.

Наиболее ранний описанный способ проектирования ИПС в рамках подхода с использованием внешнего носителя получил название «невидимой дискеты». Этот способ заключается в том, что все объекты, принадлежащие множеству Oz, и объекты, описывающие последовательность ZL, помещаются на внешний носитель, с которого может быть произведена загрузка операционной системы (обычно дискета). Неизменность объектов обеспечивается физической защитой носителя от записи.

Кроме того, использование специальной технологии не позволяет использовать объекты (в том числе и обеспечить выполнение программ) без загрузки ОС именно с этой дискеты.

Практически такая дискета выглядит достаточно нетривиально: будучи помещенной в дисковод ПЭВМ она выглядит как неформатированная (или, вином варианте, пустая). После загрузки с такой "пустой" дискеты пользователь сразу «погружается» в заданную программу и работает с ней, обращаясь в том числе и к данным на винчестере и запуская программы с локальных несменяемых носителей рабочего места с предварительным контролем неизменности соответствующих им объектов-источников (исполняемых файлов).

Предлагаемый способ позволяет исключить использование изготовленной дискеты без загрузки с нее. Дополнив загружаемую с такой дискеты операционную среду программами проверки целостности, можно добиться соблюдения всех требований изолированности программно-аппаратной среды.

Как следует из утверждения 5, одним из важнейших условий поддержания ИПС является невозможность изменения последовательности активизации компонент.

В данном случае целостность объектов, содержащих последовательность активизации компонент, гарантируется физическим запретом записи на дискету,

Важной проблемой является невозможность прерывания процесса активизации компонент, В ряде операционных сред для этого имеются штатные возможности, предусмотренные для обеспечения защиты от ошибок пользователя, сформировавшего некорректную последовательность активизации компонент ОС. В связи с этим должны быть приняты меры, гарантирующие пассивность органов управления в период отработки последовательности ZL (например, аппаратная блокировка клавиатуры с момента активизации модифицированного BOOT до момента окончания активизации субъектов множества Sz).

Описанный метод позже был реализован во внешних носителях типа CD-ROM, которые позволили значительно (на два порядка) увеличить информационную емкость носителя и загружать с него развитые операционные среды типа OS/2. Однако однократность записи существенно снижает гибкость построения ИПС таким методом.

Неудобство использования загрузочной дискеты и ее быстрый износ обусловили возникновение следующего способа проектирования ИПС.

Откажемся от рассмотрения загрузочной дискеты и рассмотрим ПЭВМ с загрузкой ОС с устройства локального хранения (винчестера) и дополнительным аппаратным устройством изолирования среды.

Рассмотрим два этапа - этап установки ИПС и этап эксплуатации ИПС. Предположим существование N пользователей, каждый i-ный из которых характеризуется некоторой персональной информацией Ki, не известной другим пользователям и хранящейся на некотором материальном носителе (например, устройстве сенсорной памяти типа Touch Memory). Существует также администратор системы с ИПС, который знает все Ki и

единолично проводит этап установки. Пользователи (владельцы Ki) же участвуют только в этапе эксплуатации.

Процесс установки ИПС состоит из следующих действий:

1. В ПЭВМ устанавливается аппаратный модуль, включающий в себя устройство и программы ПЗУ данного устройства (субъекты аппаратно-программного уровня), реализующие:

- операции сервиса аутентифицирующего носителя пользователя Ci (как минимум его чтение);
- аутентификацию пользователя с номером inc введенному им Ki; 1- чтение массива данных, содержащего множество доступных для пользователя i объектов-источников (исполняемых модулей) Fil, Fi2, …,Fim, составляющих Oz, а также объект, содержащий ZL;
- вычисление информации Mil, Mi2, ... Mim, фиксирующей целостность объектов-источников Fil, ..., Fim каждого объекта-источника (информация Mij должна удовлетворять требованиям хэш-значений и, возможно, зависеть от Ki), Mij=H(Ki, Fj)
- блокирование устройств управления и предотвращение загрузки операционной среды с внешнего носителя.

2. Администратор определяет для пользователя i набор потенциально возможных для активизации субъектов Ei, Ei={Pil, ..., Pimi}, i==l, ...,N. Create (Pik, Fj)->Pij, mi - число разрешенных к запуску задач для i-го пользователя.

3. Администратор формирует (и заносит на носитель) или считывает с носителя для i-го пользователя его Ki и вычисляет значения для последующего контроля целостности Mijr== H(Ki, Fjr) где H- функция КЦ (хэш-функция).

4. Администратор проделывает действия 2 и 3 для всех N пользователей.

5. Администратор устанавливает в АС МБС с объектом-источником Fипс и фиксирует его целостность. Установка модуля происходит с учетом условий утверждения 5.

6. Администратор фиксирует целостность объекта, содержащего ZL.

Процесс эксплуатации состоит из следующих действий.

1. Включение питания и активизация аппаратного модуля:

а) Идентификация пользователя i по Ki.

При успехе выполняется п. б), при неудаче ПЭВМ блокируется.

б) Проверка целостности всех установленных в ПЭВМ ПЗУ. При положительном исходе выполняется п. в), при неудаче ПЭВМ блокируется.

в) Чтение по секторам файлов операционной среды и проверка их целостности.

г) Чтение как файла Fипс (с помощью функций операционной среды) и проверка его целостности. Вариантом может быть чтение Fипс по секторам.

д) Активизация процесса контроля Рипс. Create(Sx,Fипс)->Fипс. Активизация МБО.

е) Запуск избранной задачи i-го пользователя (может не выполняться).

2.РаботавИПС.

Запуск каждого процесса Ps сопровождается проверками:

а) Принадлежит ли Ps к множеству разрешенных для i (Ei) если да, то выполняется п. б), иначе запуск игнорируется.

б) Совпадает ли G==H(Ki, Fs,) с M=H(Ki, Fs), вычисленной администратором.

в) При положительном исходе б) задача запускается, иначе запуск игнорируется.

Легко видеть, что условия изолированности среды выполнены. Кроме того, в данном случае реализован механизм ступенчатого контроля, обеспечивающий чтение реальных данных.

При дополнении в ИПС реализации МБО и выполнении условий, предъявленных выше, к субъектам, входящим в ИПС, сформированная программная среда будет гарантированно защищенной в рамках политики безопасности, реализованной в МБО.

Используя утверждение 4, об одинаковости состояний АС после активизации проверенных на неизменность субъектов в неизменной последовательности, можно описать метод доверенной загрузки компонент операционной среды (кратко «метод доверенной загрузки»).

Пусть предопределен порядок загрузки компонентов ОС (под загрузкой компонентов ОС понимается активизация различных субъектов ОС из соответствующих объектов-источников различного уровня иерархии). Процедуру загрузки ОС назовем доверенной, если:

- установлена неизменность компонент ОС (объектов), участвующих в загрузке (иными словами - объектов, принадлежащих множеству Oz), причем неизменность установлена до порождения первого субъекта из ZL;
- установлена неизменность объектов, определяющих последовательность активизации компонент ОС (с учетом нескольких уровней иерархии), неизменность обеспечена в течение заданного интервала времени; состояние указанных объектов не может быть изменено никем, кроме предопределенного пользователя (пользователей) АС (это условие соответствует неизменности последовательности ZL).

Легко видеть, что процедура доверенной загрузки обеспечивает одинаковое состояние АС после выполнения загрузки (согласно утверждению 4).

Основная техническая проблема при реализации доверенной загрузки состоит в доступе к объектам высшего уровня иерархии ОС (файлам) до загрузки ядра данной ОС (загружаемую ОС далее будем называть пользовательской). Однако при возможности генерации ИПС для какой-либо иной ОС (далее будем называть ее базовой) можно

предложить итеративную реализацию доверенной загрузки с использованием ресурсов указанной ОС.

Рассмотрим реализацию доверенной загрузки ОС на основе генерации ИПС для одной из операционных сред вычислительной системы. Предположим, что имеется базовая операционная система, для которой возможна полноценная генерация ИПС. Пусть в вычислительной Системе существуют еще операционные системы Os1, 0s2, ..., OSn. Ставится задача доверенного запуска операционной среды OSj. Пусть в базовой операционной системе имеется некоторое условно называемое "шлюзовое ПО" между базовой операционной системой и OSj. Функции шлюзового ПО заключаются в обеспечении доступа к файловой системе операционной системы OSj (т. е. объектам уровня R).

Пусть также пользователь i имеет физический доступ к комплекту технических средств (рабочему месту) сети (ЭВМ) Tm, на котором установлена операционная система OSj. При использовании комплекта Tm пользователем i.

1. Происходит аутентификация пользователя i (по его индивидуальной информации).

2. Проверяются права пользователя по использованию аппаратной компоненты комплекта Tm.

3. Контролируется целостность (на основе информации пользователя Ki либо без нее) всех объектов базовой ОС, размещенных на некотором носителе, локально или удаленно (через технические средства ЛВС) связанном с Тт.

4. Загружается базовая операционная система и контролируется целостность шлюзового ПО.

5. Загружается шлюзовое ПО (при этом становится доступной как минимум в режиме чтения файловая структура OSj, размещенная локально на Tm).

6. Контролируется целостность объектов уровней, меньших Rj (Rj - максимальный уровень представления объектов в OSj) для OSj (см. выше).

7. Контролируется целостность объектов уровня Rj (файлов) OSj.

8. Контролируется целостность объекта, задающего последовательность загрузки компонент.

9. Осуществляется принудительная загрузка (инициируется предопределенный в силу целостности объектов Oz и последовательности ZL порядок загрузки компонент ОС) проверенной на целостность OSj.

*Утверждение 8 (условия генерации ИПС при реализации метода*)

Пусть ядро ОС содержит МБО и МБС, инициируемые в ОС субъекты попарно корректны, их объекты-источники принадлежит множеству проверяемых на неизменность в ходе доверенной загрузки, МБО запрещает изменение любого объекта-источника и выполнена процедура доверенной загрузки ОС. Тогда после инициирования ядра ОС

генерируется ИПС.

Доказательство. Процедура доверенной загрузки по построению обеспечивает неизменность Oz и ZL, по условию утверждения для порождения субъектов разрешены только объекты-источники, принадлежащие 0z, неизменность объектов-источников по условию гарантируется свойствами МБО. Следовательно, выполнены условия утверждения 5 и генерируется ИПС. Утверждение доказано.

## 4. Математические модели информационной безопасности

Модель информационной безопасности - формальное выражение политики безопасности.

Формальные модели необходимы и используются достаточно широко, потому что только с их помощью можно доказать безопасность системы опираясь при этом на объективные и неопровержимые постулаты математической теории. модели безопасности позволяют обосновать жизнеспособность системы и определяют базовые принципы ее архитектуры и используемые при ее построении технологические решения Основная цель создания политики безопасности информационной системы и описания ее в виде формальной модели — это определение условий, которым должно подчиняться поведение системы, выработка критерия безопасности и проведение формального доказательства соответствия системы этому критерию при соблюдении установленных правил и ограничений.

Кроме того, формальные модели безопасности позволяют решить еще целый ряд задач возникающих в ходе проектирования, разработки и сертификации защищенных систем, поэтому их используют не только теоретики информационной безопасности, но и другие категории специалистов, участвующих в процессе создания и эксплуатации защищенных информационных систем (производители, потребители, эксперты-квалификаторы).

Производители защищенных информационных систем используют модели безопасности в следующих случаях:

- при составлении формальной спецификации политики безопасности разрабатываемой системы;
- при выборе и обосновании базовых принципов архитектуры защищенной системы, определяющих механизмы реализации средств защиты;
- в процессе анализа безопасности системы в качестве эталонной модели;
- при подтверждении свойств разрабатываемой системы путем формального доказательства соблюдения политики безопасности.

Потребители путем составления формальных моделей безопасности получают возможности довести до сведения производителей свои требования в четко определённой и непротиворечивой форме, а также оценить соответствие защищенных систем своим потребностям. Эксперты по квалификации в ходе анализа адекватности реализации политики безопасности в защищенных системах используют модели безопасности в качестве эталонов.

Все рассматриваемые модели безопасности основаны на следующих базовых представлениях:

1. Система является совокупностью взаимодействующих сущностей — субъектов и объектов. *Б*езопасность обработки информации и обеспечивается путем решения задачи управления доступом субъектов к объектам в соответствии с заданным набором правил и ограничений, которые образуют политику безопасности. Считается, что система безопасна, если субъекты не имеют возможности нарушить правила политики безопасности.

2. Все взаимодействия в системе моделируются установлением отношений определенного типа между субъектами и объектами. Множество типов отношений определяется в виде набора операций, которые субъекты могут производить над объектами.

3. Все операции контролируются монитором взаимодействий и либо запрещаются, либо разрешаются в соответствии с правилами политики безопасности.

4. Политика безопасности задается в виде правил, в соответствии с которыми должны осуществляться все взаимодействия между субъектами и объектами. Взаимодействия, приводящие к нарушению этих правил, пресекаются средствами контроля доступа и не могут быть осуществлены.

5. Совокупность множеств субъектов, объектов и отношений между ними (установившихся взаимодействий) определяет состояние системы. Каждое состояние системы является либо безопасным, либо небезопасным в соответствии с предложенным в модели критерием безопасности.

6. Основной элемент модели безопасности — это доказательство утверждения (теоремы) о том, что система, находящаяся в безопасном состоянии, не может перейти в небезопасное состояние при соблюдении всех установленных правил и ограничений.

### 4.1. Классификация математических моделей информационной безопасности по основным видам угроз

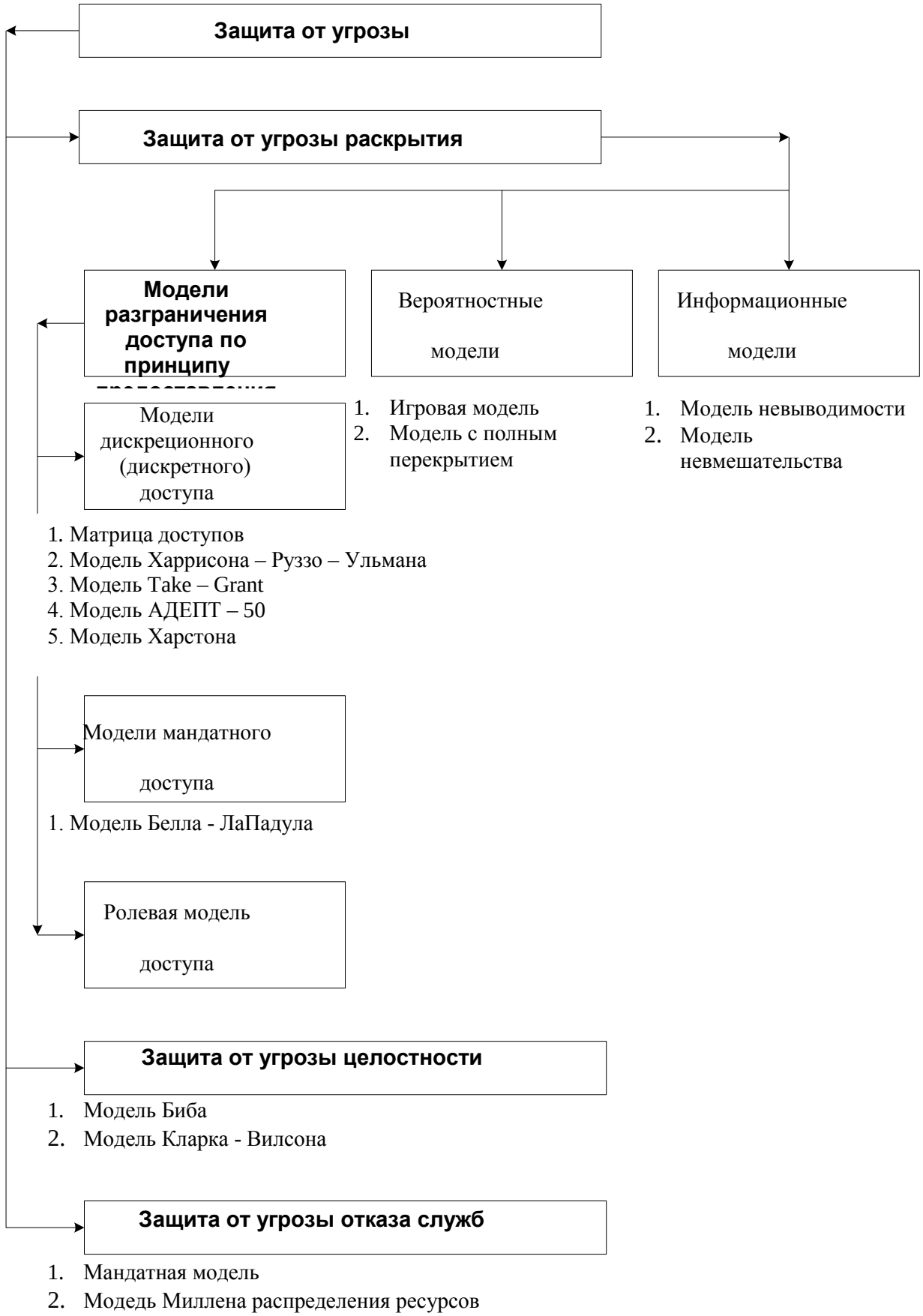



Рис. 4.1. – Классификация моделей информационной безопасности

## 4.2. Модели разграничения доступа (защита от угрозы раскрытия информации)

### 4.2.1. Описание системы защиты с помощью матрицы доступа

Пусть O - множество объектов, S - множество субъектов, $S \subseteq O$. Пусть $U=\{U_1,...,U_m\}$ - множество пользователей. Определим отображение: own: $0 \rightarrow U$.

В соответствии с этим отображением каждый объект объявляется собственностью соответствующего пользователя. Пользователь, являющийся собственником объекта, имеет все права доступа к нему, а иногда и право передавать часть или все права другим пользователям. Кроме того, собственник объекта определяет права доступа других субъектов к этому объекту, то есть политику безопасности в отношении этого объекта. Указанные права доступа записываются в виде матрицы доступа, элементы которой - суть подмножества множества R, определяющие доступы субъекта S, к объекту $0_i$(i = 1, 2,...,; j = 1, 2,... ).

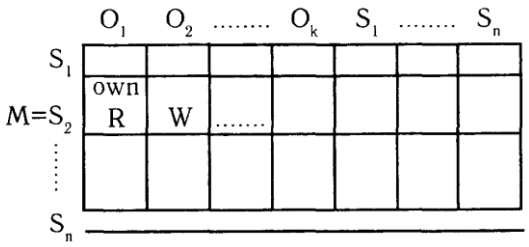



Рис. 4.2. Матрица доступов

Существует несколько вариантов задания матрицы доступа.

1. Листы возможностей: Для каждого субъекта $S_i$ создается лист (файл) всех объектов, к которому имеет доступ данный объект.

2. Листы контроля доступа: для каждого объекта создается список всех субъектов, имеющих право доступа к этому объекту.

Дискреционная политика связана с исходной моделью таким образом, что траектории процессов в вычислительной системе ограничиваются в каждом доступе. Причем вершины каждого графа разбиваются на классы и доступ в каждом классе определяется своими правилами каждым собственником. Множество неблагоприятных траекторий $N$ для рассматриваемого класса политик определяется наличием неблагоприятных состояний, которые в свою очередь определяются запретами на некоторые дуги. Дискреционная политика наиболее исследована. Существует множество разновидностей этой политики. Однако многих проблем защиты эта политика решить не может. Одна из самых существенных слабостей этого класса политик - то, что они не выдерживают атак при помощи «троянского коня». Это означает, в частности, что система защиты, реализующая дискреционную политику, плохо защищает от проникновения вирусов в систему и других средств скрытого разрушающего воздействия. Покажем на примере принцип атаки "Троянским конем" в случае дискреционной политики.

Пример 1: Пусть $U_1$ - некоторый пользователь, а $U_2$ - пользователь-злоумышленник, $O_1$ - объект, содержащий ценную информацию, $O_2$ - программа с «троянским конем» T, и M - матрица доступа, которая имеет вид:

| | $O_1$ | $O_2$ |
|---|---|---|
| $U_1$ | own<br>r<br>w | <br><br>w |
| $U_2$ | | own<br>r<br>w |

Рис. 4.3.

Проникновение программы происходит следующим образом. Злоумышленник $U_2$ создает программу $O_2$ и, являясь ее собственником, дает $U_1$ запускать ее и писать в объект $O_2$ информацию. После этого он инициирует каким-то образом, чтобы $U_1$ запустил эту программу (например, $O_2$ - представляет интересную компьютерную игру, которую он предлагает $U_1$ для развлечения). $U_1$ запускает $O_2$ и тем самым запускает скрытую программу T, которая обладая правами $U_1$ (т.к.была запущена пользователем $U_1$), списывает в себя информацию, содержащуюся в $O_1$. После этого хозяин $U_2$ объекта $O_2$, пользуясь всеми правами, имеет возможность считать из $O_2$ ценную информацию объекта $O_1$.

Следующая проблема дискреционной политики -это автоматическое определение прав. Так как объектов много, то задать заранее вручную перечень прав каждого субъекта на доступ к объекту невозможно. Поэтому матрица доступа различными способами агрегируется, например, оставляются в качестве субъектов только пользователи, а в соответствующую ячейку матрицы вставляются формулы функций, вычисление которых определяет права доступа субъекта, порожденного пользователем, к объекту O. Разумеется, эти функции могут изменяться во времени. В частности, возможно изъятие прав после выполнения некоторого события. Возможны модификации, зависящие от других параметров.

Одна из важнейших проблем при использовании дискреционной политики - это проблема контроля распространения прав доступа. Чаще всего бывает, что владелец файла передает содержание файла другому пользователю и тот, тем самым, приобретает права собственника на информацию. Таким образом, права могут распространяться, и даже, если исходный владелец не хотел передавать доступ некоторому субъекту S к своей информации в O, то после нескольких шагов передача прав может состояться независимо от его воли. Возникает задача об условиях, при которых в такой системе некоторый субъект рано или поздно получит требуемый ему доступ. Эта задача исследовалась в модели "take-grant", когда

форма передачи или взятия прав определяются в виде специального права доступа (вместо own).

**4.2.2. Дискреционная модель «Хиррисона–Руззо-Ульмана»**

Модель безопасности Харрисона-Руззо-Ульмана, являющаяся классической дискреционной моделью, реализует произвольное управление доступом субъектов к объектам и контроль за распространением прав доступа.

В рамках этой модели система обработки информации представляется в виде совокупности активных сущностей — субъектов (множество S), которые осуществляют доступ к информации, пассивных сущностей — объектов (множество O), содержащих защищаемую информацию, и конечного множества прав доступа $R = \{r_{1p} .... r_{n}\}$, означающих полномочия на выполнение соответствующих действий (например, чтение, запись, выполнение).

Поведение системы моделируется с помощью понятия состояния. Пространство состояний системы образуется декартовым произведением множеств составляющих ее объектов, субъектов и прав — OxSxR. Текущее состояние системы Q в этом пространстве определяется тройкой, состоящей из множества субъектов, множества объектов и матрицы прав доступа M, описывающей текущие права доступа субъектов к объектам, — Q=(S,O,M). Строки матрицы соответствуют субъектам, а столбцы — объектам, поскольку множество объектов включает в себя множество субъектов, матрица имеет вид прямоугольника. Любая ячейка матрицы M[s,o] содержит набор прав субъекта s к объекту o, принадлежащих множеству прав доступа R. Поведение системы во времени моделируется переходами между различными состояниями. Переход осуществляется путем внесения изменений в матрицу M с помощью команд.

В классической модели допустимы только следующие элементарные операции:

enter r into M[s,o] (добавление субъекту s права r для объекта o)

delete r from M[s,o] (удаление у субъекта s права r для объекта o)

create subject s (создание нового субъекта s)

create object o (создание нового объекта o)

destroy subject s (удаление существующего субъекта S)

destroy object o (удаление существующего объекта o)

Применение любой элементарной операции op в системе, находящейся в состоянии Q=(S,O,M) влечет за собой переход в другое состояние $Q'=(S',O',M^{I})$, которое отличается от предыдущего состояния Q по крайней мере одним компонентом.

Операция enter вводит право r в существующую ячейку матрицы доступа. Содержимое каждой ячейки рассматривается как множество, т.е. если это право уже имеется, то ячейка не изменяется. Операция называется enter монотонной, поскольку она только добавляет права

в матрицу доступа и ничего не удаляет. Действие операции delete противоположно действию операции enter. Она удаляет право из ячейки матрицы доступа, если оно там присутствует. Поскольку содержимое каждой ячейки рассматривается как множество, delete не делает ничего, если удаляемое право отсутствует в указанной ячейке. Поскольку delete удаляет информацию из матрицы доступа, она назьшается немонотонной операцией. Операции create subject и destroy subject представляют собой аналогичную пару монотонной и немонотонной операции.

Заметим, что для каждой операции существует еще и предусловие ее выполнения: для того чтобы изменить ячейку матрицы доступа с помощью операций enter пли delete необходимо, чтобы эта ячейка существовала, т. е. чтобы существовали соответствующие субъект и объект. Предусловиями операций создания create subject/object, является отсутствие создаваемого субъекта/объекта, операций удаления destroy subject/object — наличие субъекта/объекта. Если предусловие любой операции не выполнено, то ее выполнение безрезультатно.

Формальное описание системы $\sum(Q,R,C)$ состоит из следующих элементов:

- конечный набор прав доступа $R = \{r_1, ..., r_n\}$;
- конечные наборы исходных субъектов $So = \{s_1, \ldots. s_i\}$ и объектов $O_0 = \{o_1, ..., o_m\}$, где $So \subseteq O_0$;
- исходная матрица доступа, содержащая права доступа субъектов к объектам — $M_o$;
- конечный набор команд $O\{aj(x_1, x_k)\}$, каждая из которых состоит из условий выполнения и интерпретации в терминах перечисленных элементарных операций.

Поведение системы во времени моделируется с помощью последовательности состояний {Qj}, в которой каждое последующее состояние является результатом применения некоторой команды из множества С к предыдущему $Q_{n+1} = C_n(Q_n)$.Каждое состояние определяет отношения доступа, которые существуют между сущностями системы в виде множества субъектов, объектов и матрицы прав. Поскольку для обеспечения безопасности необходимо наложить запрет на некоторые отношения доступа, для заданного начального состояния системы должна существовать возможность определить множество состояний, в которые она сможет из него попасть. Это позволит задавать такие начальные условия (интерпретацию команд С, множества объектов Оо, субъектов So и матрицу доступа $M_o$), при которых система никогда не сможет попасть в состояния, не желательные с точки зрения безопасности. Следовательно, для построения системы с предсказуемым поведением необходимо для заданных начальных условий получить ответ на вопрос: сможет ли некоторый субъект s когда-либо приобрести право доступа r для некоторого объекта о?

Критерий безопасности модели Харрисона–Руззо-Ульмана формулируется следующим образом:

*Для заданной системы начальное состояние Qo = (So,Oo,Mo) является безопасным относительно права r, если не существует применимой к Qo последовательности команд, в результате которой право r будет занесено в ячейку матрицы M, в которой оно отсутствовало в состоянии* $Q_0$.

Смысл данного критерия состоит в том, что для безопасной конфигурации системы субъект никогда не получит право г доступа к объекту, если он не имел его изначально.

Из критерия безопасности следует, что для данной модели ключевую роль играет выбор значений прав доступа и их использование в условиях команд. Хотя модель не налагает никаких ограничений на смысл прав и считает их равнозначными, те из них, которые участвуют в условиях выполнения команд, фактически представляют собой не права доступа к объектам (как, например, чтение и запись), а права управления доступом, или права на осуществление модификации ячеек матрицы доступа. Таким образом, по сути дела данная модель описывает не только доступ субъектов к объектам, а распространение прав доступа от субъекта к субъекту, поскольку именно изменение содержания ячеек матрицы доступа определяет возможность выполнения команд, в том числе команд, модифицирующих саму матрицу доступа, которые потенциально могут привести к нарушению критерия безопасности.

Необходимо отметить, что с точки зрения практики построения защищенных систем модель Харрисона – Руззо - Ульмана является наиболее простой в реализаций и эффективной в управлении, поскольку не требует никаких сложных алгоритмов, и позволяет управлять полномочиями пользователей с точностью до операции над объектом, чем и объясняется ее распространенность среди современных систем. Кроме того, предложенный в данной модели критерий безопасности является весьма сильным в практическом плане, поскольку позволяет гарантировать недоступность определенной информации для пользователей, которым изначально не выданы соответствующие полномочия.

Однако, Харрисон, Руззо и Ульман доказали, что в общем случае не существует алгоритма, который может для произвольной системы, ее начального состояния Qo = ($So,0_0,M_0$) и общего права r решить, является ли данная конфигурация безопасной. Доказательство опирается на свойства машины Тьюринга, с помощью которой моделируется последовательность переходов системы из состояния в состояние.

Как уже было сказано, все дискреционные модели уязвимы по отношению к атаке с помощью «троянского коня», поскольку в них контролируются только операции доступа субъектов к объектам, а не потоки информации между ними. Поэтому, когда "троянская" программа, которую нарушитель подсунул некоторому пользователю, переносит

информацию из доступного этому пользователю объекта в объект, доступный нарушителю, то формально никакое правило дискреционной политики безопасности не нарушается, но утечка информации происходит.

Таким образом, дискреционная модель Харрисона – Руззо - Ульмана в своей общей постановке не дает гарантий безопасности системы, однако именно она послужила основой для целого класса моделей политик безопасности, которые используются для управления доступом и контроля за распространением прав во всех современных системах.

**4.2.3. Модель «Take-Grant»**

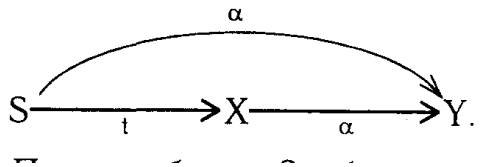
Модель распространения прав доступа Take–Grant, предложенная впервые в 1976г., используется для анализа систем дискреционного разграничения доступа, в первую очередь для анализа путей распространения прав доступа в таких системах. В качестве основных элементов модели используются граф доступа и правила его преобразования. Цель модели – дать ответ на вопрос о возможности получения прав доступа субъектом системы на объект в состоянии, описываемом графом доступа. В настоящее время данная модель получила продолжение как расширенная модель Take–Grant, в которой рассматриваются пути возникновения информационных потоков в системах с дискреционным разграничением доступа.

Перейдем к формальному описанию модели. Обозначим: O - множество объектов (файлы), S – множество активных субъектов (пользователи); R={r, w, c} - множество доступов, где r - читать, w - писать, c - вызывать. Допускается, что субъект X может иметь права $\alpha \subseteq R$ на доступ к объекту Y, эти права записываются в матрице контроля доступов. Кроме этих прав мы введем еще два: право take (t) – право брать права доступа и право grant (g) – право давать права доступа, которые также записываются в матрицу контроля доступов субъекта к объектам. Можно считать, что эти права определяют возможности преобразования одних графов состояний в другие. Преобразование состояний, то есть преобразование графов доступов, проводятся при помощи команд. Существует 4 вида команд, по которым один граф доступа преобразуется в другой.

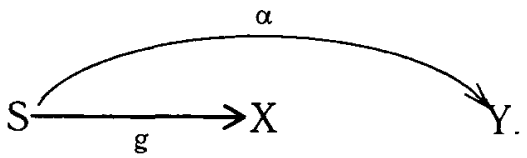
1. Take (брать). Пусть S - субъект, обладающий правом t к объекту X и $\alpha \subseteq R$ - некоторое право доступа объекта X к объекту Y. Тогда возможна команда "S take $\alpha$ forY from X". В результате выполнения этой команды в множество прав доступа субъекта S к объекту Y добавляется право $\alpha$. Графически это означает, что, если в исходном графе доступов G был подграф

$$S \xrightarrow{t} X \xrightarrow{\alpha} Y$$

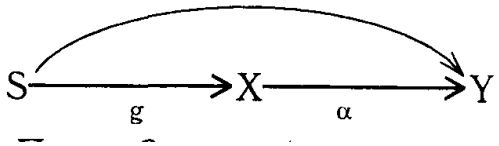
то в новом состоянии G', построенном по этой команде t, будет подграф




2. Grant (давать). Пусть субъект S обладает правом $g$ к объекту X и правом $\alpha \subseteq R$ к объекту Y. Тогда возможна команда "S grant α for Y to X". В результате выполнения этой команды граф доступов G преобразуется в новый граф G', который отличается от G добавленной дугой (X Y). Графически это означает, что если в исходном графе G был подграф




то в новом состоянии G будет подграф:




3. Create (создавать). Пусть S - субъект, $\beta \subseteq R$. Команда "S create P for new object X" создает в графе новую вершину X и определяет P как права доступов S к X. То есть по сравнению с графом G в новом состоянии G' добавляется подграф вида

$$S \xrightarrow{\beta} X$$

4. Remove (удалить). Пусть S - субъект и X - объект, $\beta \subseteq R$. Команда "S remove P for X" исключает права доступа P из прав субъекта S к объекту X. Графически преобразования графа доступа G в новое состояние G' в результате этой команды можно изобразить следующим образом:

$$S \xrightarrow{p} X, S \xrightarrow{p/\beta} X$$

Под безопасностью будем понимать возможность или невозможность произвольной фиксированной вершине P получить доступ $\alpha \in R$ к произвольной фиксированной вершине X путем преобразования текущего графа G некоторой последовательностью команд в граф G', где указанный доступ разрешен.

*Определение.* В графе доступов G вершины P и S называются tg-связными, если существует путь в G, соединяющий P и S, безотносительно ориентации дуг, но такой, что каждое ребро этого пути имеет метку, включающую t или $g$.

Примем без доказательств следующие теоремы.

*Теорема 1. Субъект P может получить доступа к, объекту X, если существует субъект S, имеющий доступ a, к вершине X такой, что субъекты P и S связаны произвольно ориентированной дугой, содержащей хотя бы одно из прав t или g*

*Теорема. 2. Пусть в системе все объекты являются субъектами. Тогда субъект P может получить доступ a к субъекту X тогда и только тогда, когда выполняются условия:*

1. Существует субъект S такой, что в текущем графеG есть дуга $S \xrightarrow{\alpha} X$ .
2. S tg-связна с P.

Перечисленный правила «Брать», «Давать», «Создавать», «Уничтожать» для отличия от правил расширенной модели Take – Grant будем называть де – юре правилами.

**4.2.4. Расширенная модель Take–Grant**

В расширенной модели Take–Grant рассматриваются пути и стоимости возникновения информационных потоков в системах с дискреционным разграничением доступа.

В классической модели Take–Grant по существу рассматриваются два права доступа: t и g, а так же четыре правила (правила де-юре) преобразования графа доступов. В расширенной модели дополнительно рассматриваются два права: на чтение r (read) и на запись w (write), а так же шесть правил (правила де-факто) преобразования графа доступов: pose, spy, find, pass и два правила без названия.

В результате применения к графу доступов правил де–факто в него добавляются мнимые дуги, помеченные r или w и изображаемые пунктиром (рисунок ). Вместе с дугами графа, соответствующими правам r и w (реальными дугами), мнимые дуги указывают на направления информационных каналов в системе.

Состояние системы описывается его графом. Переход из состояния в состояние определяется операциями или правилами преобразования графа доступов. Преобразование графа G а граф G’ в результате выполнения правила op обозначим $G \mid_{op} G'$.

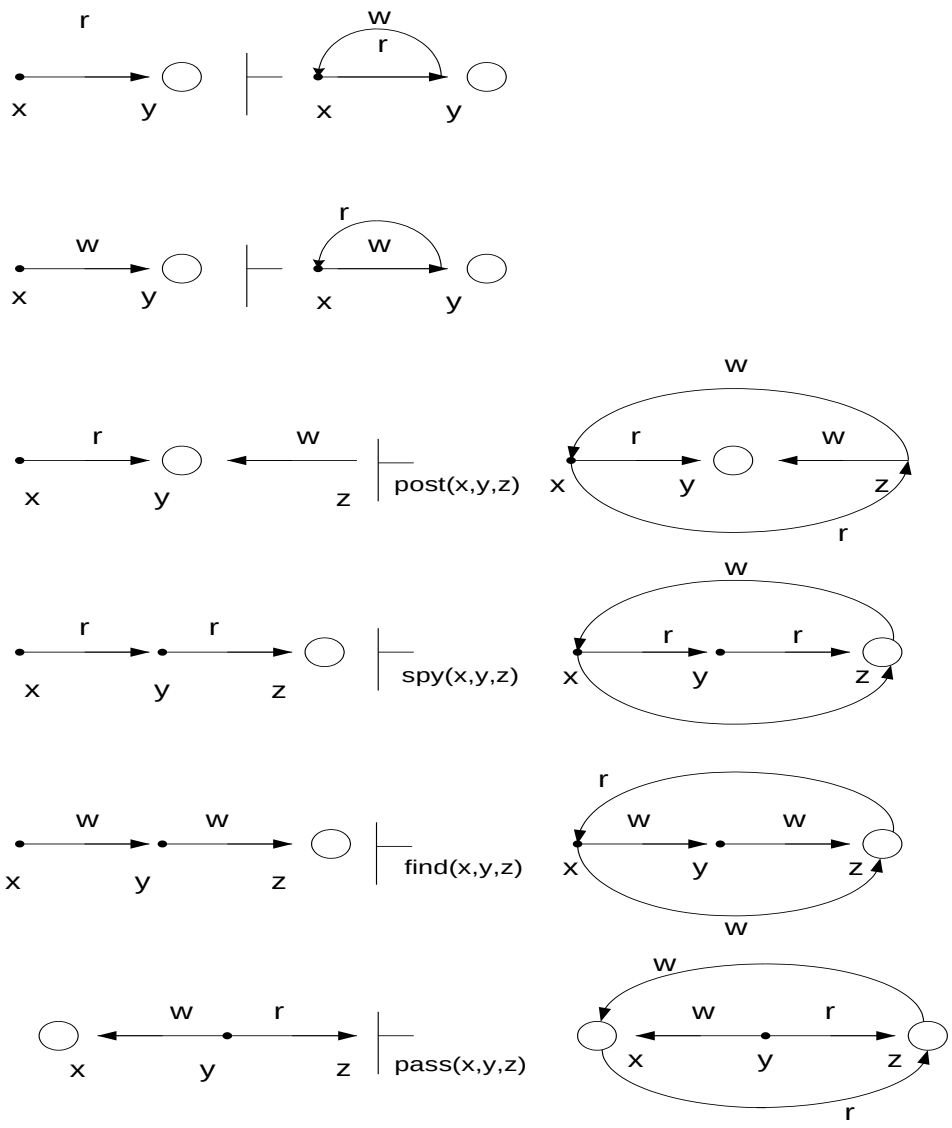



Рис. 4.4. Правила де–факто

К мнимым дугам нельзя применять правила де – юре преобразования графа доступов. Информационные каналы нельзя брать или передавать другим объектам системы.

Проблемы взаимодействия – центральный вопрос при похищении прав доступа.

Каждое правило де–юре требует для достижения своей цели участия одного субъекта, а для реализации правила де–факто необходим один или два субъекта. Желательно во множестве всех субъектов выделить подмножество так называемых субъектов - заговорщиков – участников процессов передачи прав или информации. В небольших системах эта задача легко решаема. Многократное просматривая граф доступов и применяя к нему все возможные правила де–юре и де–факто, можно найти замыкание графа доступов, которое будет содержать дуги, соответствующие всем информационным каналам системы. Однако, если граф доступов большой, то найти его замыкание весьма сложно.

Допустим, факт нежелательной передачи прав или информации состоялся. Каков наиболее вероятный путь его осуществления? В классической модели Take–Grant не дается прямого ответа.

Предположим, что чем больше узлов на пути между вершинами, по которым произошла передача прав доступа или возник информационный поток, тем меньше вероятность использования этого пути. Например, на рисунке 4 видно, что интуитивно наиболее вероятный путь передачи информации от субъекта z к субъекту x лежит через объект y. В тоже время злоумышленник может специально использовать более длинный путь.

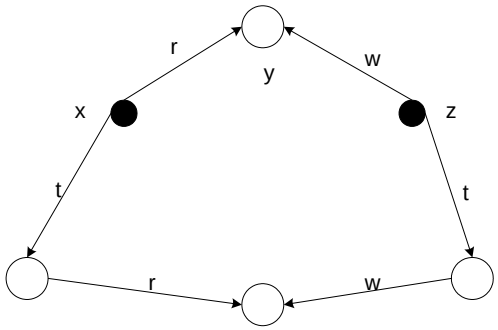



Рис. 4.5. Пути возникновения информационного канала от z к x

Таким образом, в расширенную модель Take–Grant можно включить понятие вероятности и стоимости пути передачи прав или информации. Путям наименьшей стоимости соответствует наивысшая вероятность и их исследуют в первую очередь.

К моделям дискреционного пита так же относятся модель АДЕПТ-50 и модель Харстона. Дадим им краткую характеристику.

### 4.2.5. Модель АДЕПТ–50

В данной модели представлены четыре типа сущностей (любая именованная составляющая компьютерной системы): пользователи(u), задания(j), терминалы(t) и файлы(f), причем каждая сущность описывается тройкой: (L,F,M), где режим M - набор видов доступа, полномочия F – группа пользователей, имеющих право на доступ к определенному объекту.

Сформулируем правила этой модели:

1. Пользователь u получает доступ к системе$\Leftrightarrow$ u$\in$ U.

2. Пользователь u получает доступ к терминалу t$\Leftrightarrow$ u $\in$ F(t), т.е. в том случае когда пользователь имеет право использовать терминал t.

3. Пользователь получает доступ к файлу j⇔ A(j) ≥A(f), C(j)⊇ C(f) , M(j) ⊇M, f ∈ F(f) т.е. в случае:

- привилегии выполняемого задания шире привилегий файла или равны им;
- пользователь является членом F(f).

Т.е. пользователь получает доступ к объекту тогда, когда он принадлежит группе пользователей, имеющих доступ к этому объекту, и его задание шире или равны привилегии объекта. Например, наивысшее полномочие доступа к файлу пользователя «сов. секретно», выполняющего задание с «конфиденциального» терминала будет «конфиденциально».

**4.2.6. Модель Харстона**

Модель имеет пять основных наборов:

A – установленных полномочий;

U - пользователей;

E – операций;

R – ресурсов;

S – состояний.

Область безопасности будет выглядеть как произведение: A×U×E×R×S. Процесс организации доступа можно описать алгоритмически. Он будет состоять из следующих процедур:

1. Вызвать все вспомогательные программы необходимые для предварительного принятия решения.

2. Определить из U те группы, к которым принадлежит u. Затем выбрать из P (набор установленных полномочий) спецификации полномочий, которым соответствует u. Этот набор полномочий F(u) определяет привилегию пользователя u.

3. Из P определить набор полномочий F(e) , устанавливающие e как основную операцию. Такой набор называется привилегией e.

4. Определить из P набор F(R) (привилегию единичного ресурса) – полномочия, определяющие поднабор ресурсов из $R^1$(определенных единиц ресурсов), имеющие общие элементы с R.

5. Удостоверится, что R полностью включается в D(q) =F(u)∩ F(e)F(R) (домен полномочий).

6. Разбить D(q) на эквивалентные классы, так чтобы два полномочия попадали в эквивалентный класс тогда и только тогда, когда они специфицируют одну единицу ресурса. Новый набор полномочий F(u,q) – привилегия пользователя u по отношению к запросу q .

7. Вычислить EAC – условие фактического доступа, соответствующего запросу q.

8. Оценить EAC и принять решение о доступе:

- разрешить доступ к R , если R перекрывается;
- отказать в доступе в противном случае.

9. Произвести запись необходимых событий.
10. Вызвать все программы необходимые для принятия решения.
11. Выполнить все вспомогательные программы.
12. Если решение о доступе – положительное, завершить физическую обработку.

Т.е. пользователь может получить (или не получить) доступ к информации предварительно пройдя соответствующие этапы идентификации (определение группы, его полномочий, условия фактического доступа и т.д.).

Данная модель не всегда необходима в полном объеме. Например, во время регистрации пользователя системы необходим пункт 2 и 6.

### 4.2.7. Мандатная модель Белла-ЛаПадулы

Мандатная модель управления доступом основана на правилах секретного документооборота, принятых в государственных и правительственных учреждениях многих стран. Основным положением политики Белла - ЛаПадулы, взятым ими из реальном жизни, является назначение всем участникам процесса обработки защищаемой информации, и документам, в которых она содержится, специальной метки, например, секретно, сов. секретно и т. д, получившей название уровня безопасности. Все уровни безопасности упорядочиваются с помощью установленного отношения доминирования, например, уровень сов. секретно считается более высоким чем уровень секретно, или доминирует над ним. Контроль доступа осуществляется в зависимости от уровней безопасности взаимодействующих сторон на основании двух простых правил:

1. Уполномоченное лицо (субъект) имеет право читать только те документы, уровень безопасности которых не превышает его собственный уровень безопасности.

2. Уполномоченное лицо (субъект) имеет право заносить информацию только в те документы, уровень безопасности которых не ниже его собственного уровня безопасности.

Первое правило обеспечивает защиту информации, обрабатываемой более доверенными (высокоуровневыми) лицами, от доступа со стороны менее доверенных (низкоуровневых). Второе правило (далее мы увидим, что оно более важное) предотвращает утечку информации (сознательную или несознательную) со стороны высокоуровневых участников процесса обработки информации к низкоуровневым.

Таким образом, если в дискреционных моделях управление доступом происходит путем наделения пользователей полномочиями осуществлять определенные операции над определенными объектами, то мандатные модели управляют доступом неявным образом

— с помощью назначения всем сущностям системы уровнен безопасности, которые определяют все допустимые взаимодействия между ними.

Система в модели безопасности Белла–ЛаПадулы, как и другие модели, представляется в виде множеств субъектов S, объектов O (множество объектов включает множество субъектов, ScO) и прав доступа read и write. В мандатной модели рассматриваются только эти два вида доступа, и, хотя она может быть расширена введением дополнительных прав (например, правом на добавление информации, выполнение программ и т.д.), все они будут отображаться в базовые (чтение и запись)..Использование столь жесткого подхода, не позволяющего осуществлять гибкое управление доступом, объясняется тем, что в мандатной модели контролируются не операции, осуществляемые субъектом над объектом, а потоки информации, которые могут быть только двух видов: либо от субъекта к объекту (запись), либо от объекта к субъекту (чтение).

Уровни безопасности субъектов и объектов задаются с помощью функции уровня безопасности F: $S \cup O \rightarrow L$, которая ставит в соответствие каждому субъекту и объекту уровень безопасности, принадлежащий множеству уровней безопасности L

**4.2.8. Решетка уровней безопасности**

Решетка уровней безопасности -— это формальная алгебра (L, <, •, ⊕), где L — базовое множество уровней безопасности, а оператор < определяет частичное нестрогое отношение порядка для элементов этого множества, т.е. оператор < — антисимметричен, транзитивен и рефлексивен. Отношение < на L:

1. рефлексивно, если $\forall a \in L: a < a$;

2. антисимметрично, если $\forall\ a_1, a_2 \in L: (a_1<a_2 \wedge a_2<a_1) \Rightarrow a_1 = a_2$;

3.транзитивно,если $\forall\ a_1, a_2, a_3 \in L: (a_1<a_2 \wedge a_2<a_3) \Rightarrow a_1<a_3$.

Другое свойство решетки состоит в том, что для каждой пары a1 и a2 элементов множества L можно указать единственный элемент наименьшей верхней границы и единственный элемент наибольшей нижней границы. Эти элементы также принадлежат L.

Смысл этих определений заключается в том, что для каждой пары элементов всегда можно указать единственный элемент, ограничивающий ее сверху или снизу таким образом, что между ними и этим элементом не будет других элементов.

Функция уровня безопасности F назначает каждому субъекту и объекту некоторый уровень безопасности из L, разбивая множество сущностей системы на классы, в пределах которых их свойства с точки зрения модели безопасности являются эквивалентными. Тогда оператор < определяет направление потоков информации, то есть, если F(A) < F(B), то информация может передаваться от элементов класса A элементам класса B.

Покажем, почему в модели Белла-ЛаПадулы для описания отношения доминирования на множестве уровней безопасности используется решетка.

Если информация может передаваться от сущностей класса A к сущностям класса B, а также от сущностей класса B к сущностям класса A, то классы A и B содержат одноуровневую информацию и с точки зрения безопасности эквивалентны одному классу (AB). Поэтому для удаления избыточных классов необходимо, чтобы отношение < было антисимметричным.

Если информация может передаваться от сущностей класса A сущностям класса B, а также от сущностей класса B к сущностям класса C, то очевидно, что она будет также передаваться от сущностей класса A к сущностям класса C. Таким образом, отношение < должно быть транзитивным.

Так как класс сущности определяет уровень безопасности содержащейся в ней информации, то псе сущности одного и того же класса содержат с точки зрения безопасности одинаковую информацию. Следовательно, нет смысла запрещать потоки информации между сущностями одного и того же класса. Более того, из чисто практических соображений нужно предусмотреть возможность для сущности передавать информацию самой себе. Следовательно, отношение < должно быть рефлексивным.

Использование решетки для описания отношений между уровнями безопасности позволяет использовать в качестве атрибутов безопасности (элементов множества L) не только целые числа, для которых определено отношение "меньше или равно", но и более сложные составные элементы. Например, в государственных организациях достаточно часто в качестве атрибутов безопасности используется комбинации, состоящие из уровня безопасности, представляющие собой целое число, и набора категорий из некоторого множества.

### 4.2.9. Классическая мандатная модель Белла–ЛаПадулы

В мандатных моделях функция уровня безопасности F вместе с

решеткой уровней определяют все допустимые отношения доступа между сущностями системы, поэтому множество состояний системы V представляется в виде набора упорядоченных пар (F,M), где M - это матрица доступа, отражающая текущую ситуацию с правами доступа субъектов к объектам, содержание которой аналогично матрице прав доступа в модели Харрисона – Руззо –У льмана, но набор прав ограничен правами read и write. Модель системы $\Sigma(v_0,R,T)$ состоит из начального состояния $v_0$, множества запросов R и функции перехода $T:(VxR)\rightarrow V$, которая в ходе выполнения запроса переводит систему из одного состояния в другое. Система, находящаяся в состоянии $v \in V$, при получении запроса $r \in R$, переходит в следующее состояние $v^* = T(v, r)$.Состояние v достижимо в системе

$\sum(v_0,R,T)$ тогда и только тогда, когда существует последовательность $<(r0,Vo),...,(r_n\text{-}_1,Vn\text{-}_1).(r_n,v)>$ такая, что $T(r_i\ v_i) = v_{i+1}$ для $0<i<n$.

Как и для дискреционной модели состояния системы делятся на безопасные, в которых отношения доступа не противоречат установленным в модели правилам, и небезопасные, в которых эти правила нарушаются и происходит утечка информации.

Белл и ЛаПадула предложили следующее определение безопасного состояния:

1. Состояние (F,M) называется безопасным по чтению (или просто безопасным) тогда и только тогда, когда для каждого субъекта, осуществляющего в этом состоянии доступ чтения к объекту, уровень безопасности этого субъекта доминирует над уровнем безопасности этого объекта.

2. Состояние (F,M) называется безопасным по записи(или * - безопасным) тогда и только тогда, когда для каждою субъекта, осуществляющего в этом состоянии доступ записи к объекту, уровень безопасности этого объекта доминирует над уровнем безопасности этого субъекта.

3. Состояние безопасно тогда и только тогда, когда оно безопасно и по чтению, и по записи.

В соответствии с предложенным определением безопасного состояния критерий безопасности системы выглядит следующим образом:

Система $\sum(v_0,R,T)$ безопасна тогда и только тогда, когда ее начальное состояние $v_0$ безопасно и вct состояния, достижимые из $v_0$ путем применения конечной последовательности запросов из R безопасны.

Белл и ЛаПадула доказали теорему, формально доказывающую безопасность системы при соблюдении определенных условий, получившую название основной теоремы безопасности.

**Основная теорема безопасности Белла-ЛаПадулы [3]**

Система Z(Vo,R,T) безопасна тогда и только тогда, когда:

а) начальное состояние. $v_0$ безопасно и

б) для любого состояния v, достижимого из $v_0$ путем применения конечной последовательности запросов из R таких, что T(v,r) = v*, v = (F,M) и v* = (F*,M*) для каждого $s \in S$ и $o \in O$ выполняются следующие условия:

1. если $read \in M^*[s,o]$ и $read \notin M[s,o]$, то $F^*(s) > F^*(o)$;

2. если $read \in M[s,o]$ и $F^*(s) < F^*(o)$, то $read \notin M^*[s,o]$;

3. если $write \in M^*[s,o]$ и $write \notin M[s,o]$, то $F^*(o) > F^*(s)$;

4. если $write \in M[s,o]$ и $F^*(o) < F^*(s)$, то $write \notin M^*[s,o]$.

Таким образом, теорема утверждает, что система с безопасным начальным состоянием является безопасной тогда и только тогда, когда при любом переходе системы из одного состояния в другое не возникает никаких новых и не сохраняется никаких старых отношений доступа, которые будут небезопасны по отношению к функции уровня безопасности нового состояния. Формально эта теорема определяет все необходимые и достаточные условия, которые должны быть выполнены для того, чтобы система, начав свою работу в безопасном состоянии, никогда не достигла небезопасного состояния.

### 4.2.10. Безопасная функция перехода

Недостаток основной теоремы безопасности Белла-ЛаПадулы состоит в том, что ограничения, накладываемые теоремой на функцию перехода, совпадают с критериями безопасности состояния, поэтому данная теорема является избыточной по отношению к определению безопасного состояния. Кроме того, из теоремы следует только то, что все состояния, достижимые из безопасного состояния при определенных ограничения, будут в некотором смысле безопасны, по при этом не гарантируется, что они будут достигнуты без потери свойства безопасности в процессе осуществления перехода. Поскольку у нас нет никаких определенных ограничений на вид функции перехода, кроме указанных в условиях теоремы, и допускается, что уровни безопасности субъектов и объектов могут изменяться, то можно представить такую гипотетическую систему (она получила название Z-системы), в которой при попытке низкоуровневого субъекта прочитать информацию из высокоуровневого объекта будет происходить понижение уровня объект до уровня субъекта и осуществляться чтение. Функция перехода Z-сиегемы удовлетворяет ограничениям основной теоремы безопасности, и все состояния такой системы также являются безопасными в смысле критерия Белла - ЛаПадулы, но вместе с тем в этой системе любой пользователь сможет прочитать любой файл, что, очевидно, несовместимо с безопасностью в обычном понимании.

Следовательно, необходимо сформулировать теорему, которая бы не только констатировала безопасность всех достижимых состояний для системы, соответствующей определенным условиям, но и гарантировала бы безопасность в процессе осуществлении переходов между состояниями. Для этого необходимо регламентировать изменения уровней безопасности при переходе от состояния к состоянию с помощью дополнительных правил.

Такую интерпретацию мандатной модели осуществил Мак-Лин, предложивший свою формулировку основной теоремы безопасности, основанную не на понятии безопасного состояния, а на понятии безопасного перехода.

Функция перехода является безопасной тогда и только тогда, когда она одновременно безопасна и по чтению и по записи и когда она изменяет только один из компонентов состояния, и эти изменения не приводят к нарушению безопасности системы.

Теорема безопасности Мак-Лина. Система безопасна в любом состоянии и в процессе переходов между ними, если ее начальное состояние является безопасным, а ее функция перехода удовлетворяет критерию Мак- Лина.

Обратное утверждение неверно. Система может быть безопасной по определению Белла-ЛаПадулы, но не иметь безопасной функции перехода.

Такая формулировка основной теоремы безопасности предоставляет в распоряжение разработчиков защищенных систем базовый принцип их построения, в соответствии с которым для того, чтобы обеспечить безопасность системы как в любом состоянии, так и в процессе перехода между ними, необходимо реализовать для нее такую функцию перехода, которая соответствует указанным условиям.

**4.2.11. Уполномоченные субъекты**

Формулировка основной теоремы безопасности в интерпретации Мак-Лина позволяет расширить область ее применения по сравнению с классической теоремой Белла-ЛаПадулы, однако, используемый критерий безопасности перехода не всегда соответствует требованиям контроля доступа, возникающим на практике. Поскольку в процессе осуществления переходов могут изменяться уровни безопасности сущностей системы, желательно контролировать этот процесс, явным образом разрешая или запрещая субъектам осуществлять подобные переходы. Для решения этой задачи Мак-Лин расширил базовую модель путем выделения подмножества уполномоченным субъектов, которым разрешается инициировать переходы, в результате которых у сущностей системы изменяются уровни безопасности. Система с уполномоченными субъектами также описывается множествами S, O, L, смысл которых совпадает с аналогичными понятиями модели Белла-ЛаПадулы, а ее состояние также описывается набором упорядоченных пар (F,M), причем функция перехода F и матрица отношений M доступа играют ту же роль. Новым элементом модели является функция управления уровнями C: SuO > P(S) (здесь и далее P(S) обозначает множество всех подмножеств S). Эта функция определяет подмножество субъектов, которым позволено изменять уровень безопасности, для заданного объекта или субъекта. Модель системы $\sum(v_o,R, T^a$ состоит из начального состояния vo, множества запросов R и функции перехода $T^a$, которая переводит систему из состояния в состояние по мере выполнения запросов.

С точки зрения модели уполномоченных субъектов система

$\sum(v_o,R, T^a)$ считается безопасной в том случае, если:

1. Начальное состояние $v_0$ и все состояния, достижимые из него путем применения конечного числа запросов из R являются безопасными по критерию Белла - ЛаПадулы;

2. Функция перехода $T^a$ является авторизованной функцией перехода согласно предложенному определению.

### 4.2.12. Модель совместного доступа

Практическое применение всех представленных формулировок мандатной модели безопасности ограничено еще одним фактором — они не учитывают широко распространенные в государственных учреждениях правила, согласно которым доступ к определенной информации или модификация ее уровня безопасности могут осуществляться только в результате совместных действий нескольких пользователей (т. н. групповой доступ).

Для того, чтобы мандатная модель предусматривала совместный доступ необходимо модифицировать се следующим образом. Вместо множества субъектов системы S будем рассматривать множество непустых подмножеств S, которое обозначим как $S=P(S)\backslash\{\varnothing\}$. Расширим матрицу прав доступа, отражающую текущее состояние доступа в системе, путем добавления в нее строк, содержащих права групповых субъектов, и обозначим ее как M Кроме функции уровня безопасности $F:SuO\rightarrow L$ для групповых субъектов вводятся дополнительные функции: $F^L:S\rightarrow L$ такая, что $F^L(s)$ есть наибольшая нижняя граница множества $\{F(s) / s\in S\}$ и $F^H:S\rightarrow L$, такая, что $F^H(s)$ есть наименьшая верхняя граница множества$\{F(s) / s\in S\}$.

Критерии безопасности состояния для такой системы формулируются следующим образом:

1. Состояние системы является безопасным но чтению тогда и только тогда, когда для каждого индивидуального или группового субъекта, имеющего в этом состоянии доступ чтения к объекту, наибольшая нижняя граница множества уровней безопасности этого субъекта доминирует над уровнем безопасности этого объекта: $\forall s\in S$, $\forall$ $o\in O$, $read\in M[s,o] \rightarrow F^L(s)>F(o)$.

2. Состояние системы является безопасным по записи тогда и только тогда, когда для каждого индивидуального или группового субъекта, имеющего в этом состоянии доступ записи к объекту, уровень безопасности этого объекта доминирует над наименьшей верхней границей множества уровней безопасности этого субъекта: $\forall s\in S$, $\forall$ $o\in O$, write $\in M[s,o]->F(o)> F^H(s)$.

Тогда теорема Белла-ЛаПадулы для совместного доступа формулируется следующим образом [3]:

Система$\sum(vo,R, T)$ безопасна тогда и только тогда, когда:

а) начальное состояние $v_0$ безопасно и

б) функция перехода T takoda, чго для любого состояния v, достижимого из $v_0$ путем применения конечной последовательности запросов из R, таких, что T(v,r) = v*, $v=((F,F^H,F^L),M)$ и $v^*=((F^*,F^{*H},F^{*L})^*,M^*)$ для каждого $\forall s\in S$, $\forall$ $o\in O$ выполняются следующие условия:

1. если read $\in$ M*[s,o] и read $\notin$ M[s,o], то $F^L$*(s)> F*(o);

2. если read $\in$ M[s,o] и $F^L$*(s)<F*(o), то read $\notin$ M* [s,o];

3. если write $\in$ M*[s,o] и write $\notin$ M[s,o], то F*(o)> $F^H$*(s);

4. если write $\in$ M[s,o] и F*(o)<$F^H$*(s), то write $\notin$ M* [s,o].

**4.2.13 Применение мандатных моделей**

В завершении обзора мандатных моделей необходимо отметить трудности, которые связаны с их применением на практике. Все мандатные модели, как и модель Белла - ЛаПалулы, используют только два права доступа – чтение и запись. Па практике информационные системы поддерживают значительно более широкий спектр операций над информацией, например, создание, удаление, передачи и т. д. Следовательно, для того чтобы применить мандатную модель к реальной системе, необходимо установить подходящее соответствие между чтением и записью и операциями, реализованными в конкретной системе. Самым простым примером непрактичности мандатной модели является невозможность ее применения для сетевых взаимодействий — нельзя построить распределенную систему, в которой информация передавалась бы только в одном направлении, потому что всегда будет существовать обратный поток информации, содержащий ответы на запросы, подтверждения получения и т.д.

Поэтому, когда и системе используется мандатная политика, все взаимодействия рассматриваются только на достаточно высоком уровне абстракции, на котором не учитываются детали реализации операций доступа. Такой подход позволяет отобразить любое множество разнообразных операций доступа в обобщенные операции чтения и записи. Для оценки возможности нарушений безопасности с использованием методов, основанных на несоответствии этих абстрактных операций и реальных механизмов доступа, применяется анализ т.н. скрытых каналов утечки информации. Целью этих исследований является выявление тех способов, с помощью которых информация может передаваться в обход правил мандатной модели.

Чем больше потоков информации мы поставим под контроль мандатной модели, тем менее гибкой будет наша система, но и тем меньше потоков информации придется исследовать в процессе анализа скрытых каналов.

В заключение обзора мандатной модели управления доступом необходимо отметить, что хотя она является базовой моделью безопасности, составляющей основу теории зашиты информации, однако ее применение на практике связано с серьезными трудностями: Поэтому в реальной жизни она используется только в системах, обрабатывающих классифицированную информацию, и применяется только в отношении ограниченного подмножества субъектов и объектов.

### 4.2.14. Ролевая политика безопасности

Ролевая политика безопасности представляет собой существенно усовершенствованную модель Харрисона–Руззо-Ульмана, однако ее нельзя отнести ни к дискреционным, ни к мандатным, потому что управление доступом в ней осуществляется как на основе матрицы прав доступа для ролей, так и с помощью правил, регламентирующих назначение ролей пользователям и их активацию во время сеансов. Поэтому ролевая модель представляет собой совершенно особый тип политики, основанной на компромиссе между гибкостью управления доступом, характерной для дискреционных моделей, и жесткостью правил контроля доступа, присущей мандатным моделям.

В ролевой модели классическое понятие субъект замещается понятиями пользователь и роль. Пользователь -— это человек, работающий с системой и выполняющим определенные служебные обязанности. Роль — это активно действующая в системе абстрактная сущность, с которой связан ограниченный, логически связанный набор полномочий, необходимых для осуществления, определенной деятельности. Самым распространенным примером роли является присутствующий почти в каждой системе административный бюджет (например root для UNIX и Administrator для Windows NT), который обладает специальными полномочиями и может использоваться несколькими пользователями.

Ролевая политика распространена очень широко, потому что она, в отличие от других более строгих и формальных политик, очень близка к «реальной жизни». Ведь на самом деле работающие в системе пользователи действуют не от своего личного имени они всегда осуществляют определенные служебные обязанности, т.е. выполняют некоторые роли, которые никак не связаны с их личностью.

Поэтому вполне логично осуществлять управление доступом и назначать полномочия не реальным пользователям, а абстрактным (не персонифицированным) ролям, представляющим участников определенного процесса обработки информации. Такой подход к политике безопасности позволяет учесть разделение обязанностей и полномочий между участниками прикладного информационного процесса, т. к. с точки зрения ролевой политики имеет значение не личность пользователя, осуществляющего доступ к информации, а то, какие полномочия ему необходимы для выполнения его служебных обязанностей. Например, в реальной системе обработки информации могут работать системный администратор, менеджер баз данных и простые пользователи.

В такой ситуации ролевая политика позволяет распределить полномочия между этими ролями и соответствии с их служебными обязанностями: роли администратора назначаются специальные полномочия, позволяющие ему контролировать работу системы и управлять ее конфигурацией, роль менеджера баз данных позволяет осуществлять управление сервером БД, а права простых пользователей ограничиваются

минимумом, необходимым для запуска прикладных программ. Кроме того, количество ролей в системе может не соответствовать количеству реальных пользователей — один пользователь, если на нем лежат различные обязанности, требующие различных полномочий, может выполнять (одновременно или последовательно) несколько ролей, а несколько пользователей могут пользоваться одной и тон же ролью, если они выполняют одинаковую работу .

При использовании ролевой политики управление доступом осуществляется в две стадии:, во-первых, для каждой роли указывается набор полномочий, представляющий набор прав доступа к объектам, и, во-вторых, каждому пользователю назначается список доступных ему ролей. Полномочия назначаются ролям в соответствии с принципом наименьших привилегий, из которого следует, что каждый пользователь должен обладать только минимально необходимым для выполнения своей работы набором полномочий.

Ролевая модель описывает систему в виде следующих множеств [3]:

- U - множество пользователей;
- R - множество ролей;
- P - множество полномочий на доступ к объектам, представленное, например, и виде матрицы прав доступа;
- S - множество сеансов работ пользователей с системой.

Для перечисленных множеств определяются следующие отношения (рис. 4.6.):

$PA \subseteq PxR$ - отображает множество полномочии на множество ролей, устанавливая для каждой роли набор присвоенных ей полномочий;

$UA \subseteq UxR$ - отображает множество пользователей на множество ролей, определяя для каждого пользователя набор доступных ему ролей.

Правила управления доступом ролевой политики безопасности определяются следующими функциями:

user: $S \rightarrow U$ - для каждого сеанса S эта функция определяет пользователя, который осуществляет этот сеанс работы с системой: user(s) = u

roles : $S \rightarrow P(R)$ - lля каждого сеанса S эта функция определяет набор ролей из множества R которые могут быть одновременно доступны пользователю в этом сеансе: $roles(s)=\{r_i \mid (user(s), r_i) \in UA\}$;

permissions : $S \rightarrow P$ - для каждого сеанса S эта функция задает набор доступных в нем полномочии, который определяется как совокупность полномочий всех ролей, задействованных в этом сеансе: $permissions(s) = U_{r \in roles(s)}\{Pi, (Pi, r) \in PA\}$

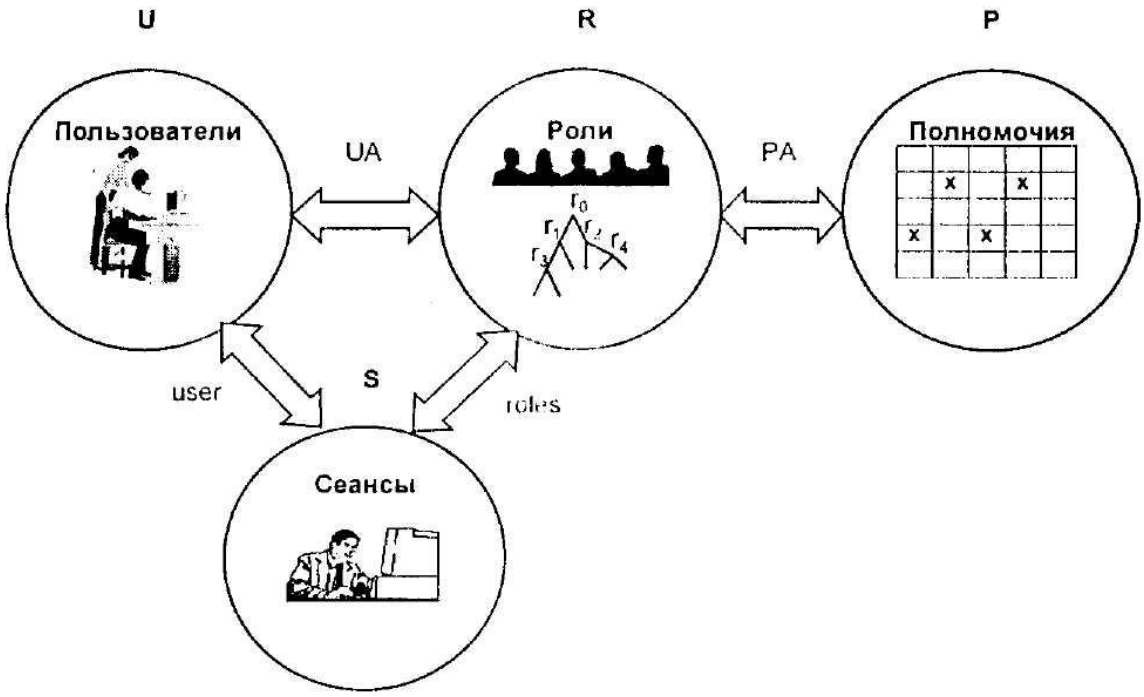



Рис.4.6. Ролевая модель управления доступом.

В качестве критерия безопасности ролевой модели используется следующее правило: *система считается безопасной, если любой пользователь системы, работающий в сеансе S, может осуществлять действия, требующие полномочия p только в том случае, если* p ∈ permissions(s*)*.

Из формулировки критерия безопасности ролевой модели следует, что управление доступом осуществляется главным образом не с помощью назначения полномочий ролям, а путем задания отношения UA, назначающего роли пользователям, и функции roles, определяющей доступный в сеансе набор ролей. Поэтому многочисленные интерпретации ролевой модели различаются видом функции user, roles и permission, а также ограничениями, накладываемыми на отношения PA и UA. В качестве примеров рассмотрим ролевую политику управления доступом с иерархической организацией ролей, а также несколько наиболее часто встречающихся типовых ограничений на отношения PA и UA и функции user и roles.

Иерархическая организация ролей представляет собой наиболее распространенный тип ролевой модели поскольку она очень точно отражает установившееся в реальном мире отношение подчиненности между участниками процессом обработки информации и разделение между ними сфер ответственности. Роли в иерархии упорядочиваются по уровню предоставляемых полномочий. Чем выше роль находится в иерархии, тем больше с ней связано полномочий, поскольку считается, что если пользователю присвоена некоторая роль, то ему автоматически назначаются и все подчиненные ей по иерархии роли. Иерархия ролей допускает множественное наследование.

Каждому пользователю назначается некоторое подмножество иерархии ролей, а в каждом сеансе доступна совокупность полномочий ролей, составляющих фрагмент этой иерархии. Такой подход позволяет существенно упростить управление доступом за счет неявного назначения полномочий, поскольку в реальной жизни, как правило, пользователи жестко упорядочены по степени ответственности, соответствующей уровню полномочий, которыми они обладают. Причем, более доверенные пользователи, стоящие па служебной лестнице выше, всегда обладают всеми полномочиями менее доверенных, подчиненным им. Иерархия ролей в точности отражает эту ситуацию.

Другие реализации ролевой политики безопасности также связаны с введением различных ограничений на отношения PA, UA, и функции user, roles и permissions. Главным для этих ограничений является то, что все они отражают специфику распределения полномочий и сфер ответственности между участниками различных процессов обработки информации. Рассмотрим несколько примеров, демонстрирующих богатые возможности применения ролевой модели управления доступом:

1. Взаимоисключающие роли. Множество ролей разбивается на подмножества, объединяющие роли, которые не могут быть назначены пользователю одновременно и считают несовместимыми. Таким образом пользователю может быть назначено только по одной роли из каждого подмножества несовместимых ролей.)

Взаимоисключающие роли реализуют, т. н. статическое разделение обязанностей, когда конфликт несовместимости полномочий разрешается на стадии назначения ролей. Такая политика хорошо подходит для системы обработки информации, в которой пользователям запрещается совмещать определенные обязанности. Например, в банковской системе одному и тому же пользователю не могут быть одновременно назначены роли оператора, отвечающего за выполнение определенных операций, и аудитора, осуществляющего контроль за их выполнением.

2. Ограничения на одновременное использование ролей в рамках одной сессии. В этом случае множество ролен также разбивается на подмножества несовместимых ролей, но отношение UA может назначить пользователю любую комбинацию ролен. Однако в ходе сеанса работы с системой пользователь может одновременно активировать не более одной роли из каждого подмножества несовместимых ролей.

Поскольку в процессе сеанса пользователь может переключаться между различными ролями, он должен при этом избегать конфликтов несовместимости между ними, эта политика получила название динамического разделения обязанностей. Такая политика является более гибкой по сравнению со статическим разделением обязанностей, поскольку позволяет реализовать более сложные схемы контроля доступа. В частности она позволяет запретить пользователю, обладающему значительным набором ролей и полномочий,

пользоваться ими всеми одновременно. В определенных ситуациях это позволяет защититься от атаки «троянского коня» — например, пользователю можно запретить одновременно осуществлять доступ к ценной информации и запускать «недоверенные» программы, внесенные в систему другими пользователями. Правильно подобранные ограничения на одновременное использование ролей позволяют реализовать контроль за информационными потоками, что вообще - то характерно для мандатных моделей безопасности.

3. Количественные ограничения при назначении ролей и полномочий. Эта модель предназначена для тех случаев, когда роль может быть назначена только ограниченному числу пользователей, и/или предоставление некоторых полномочии допускается только для ограниченного числа ролей.

Смысл данных условий состоит и том, что благодаря ограничению количества пользователей, осуществляющих те или иные операции, сужается круг лиц, на которых лежит ответственность за совершение соответствующих действий. Например, в системе не должно быть более одного администратора, или, скажем, право уничтожать документы может быть назначено только одной роли.

4. Группирование ролей и полномочий. Роли и полномочия, которые дополняют друг друга, и назначение которых по отдельности не имеет смысла, объединяются в группы, которые могут быть назначены только целиком. Для этого вводятся дополнительные правила, в соответствии с которыми любая роль может быть назначена пользователю только в том случае, если ему уже присвоен определенный набор ролен, а роль может быть наделена полномочием только тогда, когда с ней уже связан определенный набор полномочии.

Введение подобных ограничений упрощает администрирование системы в тех случаях, когда полномочия должны предоставляться определенным набором, или когда назначение ролей должно производится в определенной последовательности. Например, предоставлять доступ к некоторым объектам (скажем личным каталогам) имеет смысл только сразу и по чтению и по записи. Типичным примером группирования ролей является ситуация, когда некоторый пользователь, осуществляющий руководство работой других пользователей, должен обладать полномочиями, равными совокупности полномочий всех своих подчиненных, т.е. роль руководителя образует одну группу с ролями исполнителей. Следует отметить, что иерархия ролей является частным случаем группирования ролей и полномочий.

Поскольку все перечисленные варианты ограничений, а также любые другие могут использоваться в различных комбинациях, ролевая модель очень легко адаптируется для каждого конкретного случая, что является ее основным преимуществом перед другими

моделями. Ролевая политика предоставляет широкий простор для разработчиков систем управления доступом, - с одной стороны, использование матрицы прав доступа может превратить ее в разновидность дискреционной модели, но, с другой с троны, применение жестких правил распределения ролей между сеансами и пользователями, а также полномочий между ролями, позволяет построить на ее основе полноценную нормативную политику. Следовательно, свойства системы, построенной в соответствии с ролевой моделью, определяются исключительно характером используемых ограничений и могут находиться в очень широком диапазоне, что не позволяет провести формальное доказательство безопасности модели для общего случая.

Подводя итоги свойств ролевой политики управления доступом, следует констатировать, что в отличие от других политик она практически не гарантирует безопасность с помощью формального доказательства, а только определяет характер ограничений, соблюдение которых и служит критерием безопасности системы. Такой подход позволяет получать простые и понятные правила контроля доступа, которые легко могут быть применены на практике, но лишает систему доказательной теоретической базы. В некоторых ситуациях это обстоятельство затрудняет использование ролевой политики, однако, в любом случае, оперировать ролями гораздо удобнее, чем субъектами, поскольку это более соответствует распространенным технологиям обработки информации, предусматривающим разделение обязанностей и сфер ответственности между пользователями. Кроме того, ролевая политика может использоваться одновременно с другими политиками безопасности, когда полномочия ролей, назначаемых пользователям, контролируются дискреционной или мандатной политикой, что позволяет строить многоуровневые схемы контроля доступа.

**4.2.15. Вероятностные модели**

Модели этого типа исследуют вероятность преодоления системы защиты за определенное время. Достоинство моделей – числовая оценка стойкости системы защиты, недостаток – изначальное допущение того, что система может быть вскрыта.

Задача модели – минимизация преодоления системы защиты.

**Игровая модель**

Модель строится по следующему принципу. Разработчик создает первоначальный вариант системы защиты. После это злоумышленник начинает его преодолевать. Если к моменту времени T, в который злоумышленник преодолел систему защиты, у разработчика не будет нового варианта система защиты – преодолена. Если нет, то процесс продолжается. Т. е. Модель описывает процесс эволюции системы защиты в течении времени.

**Модель системы безопасности с полным перекрытием**

В данной модели точно определяется каждая область, требующая защиты, оцениваются средства обеспечения безопасности, их эффективность и вклад в обеспечение безопасности во всей вычислительной системе. С каждым объектом O, требующим защиты, связывается некоторое множество действий, к которым может прибегать злоумышленник для получения несанкционированного доступа к объекту. Основной характеристикой набора угроз T является вероятность появления каждого из злоумышленных действий. В реальной системе эти вероятности можно вычислить с ограниченной степенью точности.

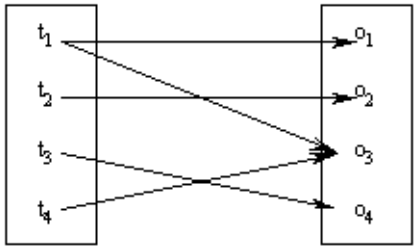



Рис. 4.7. Множество отношений объект-угроза

Множество отношений объект-угроза образуют двухдольный граф, в котором ребро <ti oj> существует тогда и только тогда, когда ti ($\forall ti \in T$) является средством получения доступа к объекту oi ($\forall oi \in O$). Связь между объектами и угрозами типа "один ко многим", т.е. одна угроза может распространяться на любое число объектов и объект может быть уязвим со стороны более чем одной угрозы. Цель защиты состоит в том, чтобы перекрыть каждое ребро графа и воздвигнуть барьер для доступа по этому пути.

Завершает модель третий набор, включающий средства безопасности M, которые используются для защиты информации в вычислительной системе. Идеально каждое mk ($\forall mk \in M$) должно устранять некоторое ребро <ti oj> из графа на рисунке. Набор M средств обеспечения безопасности преобразует двухдольный граф в трехдольный граф. В защищенной системе все ребра представляются в виде <ti mk> и <mk oj>. Любое ребро в форме <ti oj> определяет незащищенный объект. Одно и то же средство обеспечения безопасности может перекрывать более одной угрозы и (или) защищать более одного объекта. Отсутствие ребра <ti oj> не гарантирует полного обеспечения безопасности (хотя наличие такого ребра дает потенциальную возможность несанкционированного доступа за исключением случая, когда вероятность появления ti равна нулю).

**Понятие системы с полным перекрытием**

Система с полным перекрытием – система в которой имеются средства защиты на каждый путь проникновения [1].

Пусть:

T – набор угроз;

O – набор защищаемых объектов;

M – набор средств обеспечения безопасности;

V – набор уязвимых мест – отображение T×O на набор упорядоченных пар $V = \{t_i, O\}_i$, представляющих собой пути проникновения в систему;

B – набор барьеров – отображение T×O×M или V×M на набор упорядоченных троек $\{t_i\ o_j\ m_k\}$, представляющих собой точки, в которых требуется осуществить защиту.

Если $\{t_i\ o_j\} \in V$ предусматривает $\{t_i\ o_j\ m_k\} \in B$, то j ий объект защищен.

Основное преимущество данного типа моделей состоит в возможности численного получения оценки степени надежности системы защиты информации. Данный метод не специфицирует непосредственно модель системы защиты информации, а может использоваться только в сочетании с другими типами моделей систем защиты информации.

### 4.2.16. Информационные модели

Потоковые модели определяют ограничения на отношение ввода/вывода системы, которые достаточны для реализации системы. Данные модели являются результатом применения шенноновской теории информации к проблеме безопасности систем. К данным моделям относятся модели невмешательства и невыводимости.

**Модель невмешательства**

Невмешательство – ограничение, при котором ввод высокоуровнего пользователя не может смешиваться с выходом низкоуровнего пользователя. Модель невмешательства рассматривает систему, как состоящую из четырех объектов: высокий ввод, низкий ввод, высокий вывод, низкий вывод.

Рассмотрим систему, вывод которой пользователю u определен функцией out(u, hist.read(u)), где hist.read(u) – история ввода системы (traces), чей последний ввод был read(u) - команда чтения, исполненная пользователем u. Безопасность определена в терминах очищения (purge) историй ввода, где purge удаляет команды, исполненные пользователем, чей уровень безопасности не доминирует над уровнем безопасности u.

Для определенных систем, модель невмешательства особенно хороша в том, что если последовательность входа X не смешивается с последовательностью вывода У, и X независима от ввода других пользователей, то I(X, У)=0, где I(X, У) — взаимная для X и У информация.

**Модель невыводимости**

Модель невыводимости выражается в терминах пользователей и информации, связанных с одним из двух возможных уровней секретности (высокий и низкий).

Система считается невыводимо безопасной, если пользователи с низким уровнем безопасности не могут получить информацию с высоким уровнем безопасности в результате

любых действий пользователей с высоким уровнем безопасности. Т.е. утечка информации не может произойти в результате посылки высокоуровневыми пользователями низкоуровневым пользователям высокоуровневой информации.

Такое определение предусматривает неспособность низкоуровневых пользователей к использованию доступной им информации для получения высокоуровневой информации, но не защищает высокоуровневых пользователей от просмотра низкоуровневыми пользователями. Оно просто требует, чтобы низкоуровневые пользователи не были способны использовать доступную им информацию для получения высокоуровневой информации.

### 4.3 Модели контроля целостности

#### 4.3.1. Модель Биба

**Мандатная модель целостности Биба**

Данную модель часто называют инверсией модели Бела – Лападула и следовательно основные правила этой модели просто переворачивают правила модели Бела – Лападула: NRU→ «нет чтения снизу(NRD)» и NRD→ «нет записи наверх(NWU)».

Правило NRD оприделяется как запрет субъектами на чтение информации из объекта с более низким уровнем целостности. Правило NWUопределяется как запрет субъектам на запись информации в объект с более высоким уровнем целостности.

Одним из преимуществ этой модели является то, что она унаследовала многие важные характеристики БЛМ, включая ее простоту и интуитивность. Это значит, что проектировщики реальных систем могут легко понять суть этих правил и использовать их для принятия решений при проектировании. Кроме того, поскольку мандатная модель целостности Биба, подобно БЛМ, основана на простой иерархии, ее легко объяснить и изобразить пользователям системы.

С другой стороны, модель представляет собой очевидное противоречие с правилами NRU и NWD. Это значит, что если необходимо построить систему, которая предотвращает угрозы, как секретности, так и целостности, то одновременное использование правил моделей БЛМ и Биба может привести к ситуации, в которой уровни безопасности и целостности будут использоваться противоположными способами.

**Модель понижения уровня субъекта**

Вторая модель Биба заключается в небольшом ослаблении правила чтения снизу.

Здесь субъекту разрешается осуществлять чтение снизу, но в результате такого чтения уровень целостности субъекта понижается до уровня целостности объекта. В этой модели, не накладывается ни каких ограничений на то, что может прочитать субъект, и она подразумевает монотонное изменение уровней целостности.

**Модель понижения уровня объекта**

Последняя модель Биба реализуется в ослаблении правила записи наверх. Модель разрешает совершать запись наверх, но в результате, уровень целостности объекта понижается до уровня целостности субъекта, осуществляющего запись. В этой модели также, не накладывается ни каких ограничений на то, что может прочитать или записать субъект, она также подразумевает монотонное изменение уровней целостности и не содержит ни каких механизмов для повышения уровня целостности объекта.

В практическом применении модель Биба слишком сильно полагается на понятие доверенных процессов. То есть, проблема необходимости создания доверенных процессов для повышения или понижения целостности субъектов или объектов является весьма существенной. Следует отметить тот факт, что данная модель не предусматривает механизмов повышения целостности, что ведет к монотонному снижению целостности системы.

**4.3.2. Модель Кларка–Вилсона**

Эта модель была создана в 1987г Кларком и Вилсоном. Ее созданию способствовал анализ методов управления коммерческими организациями целостностью своих бумажных ресурсов в неавтоматизированном офисе.

Введем некоторые обозначения:

D – конечное множество данных;

CDI – ограниченные элементы данных;

UDI – неограниченные элементы данных,

Причем: $D = CDI \cup UDI$, $CDI \cap UDI = \varnothing$.

Субъекты включены в модель как множество компонент, инициирующие процедуры преобразования (ПП) – любые ненулевые последовательности элементарных действий (элементарное действие - переход состояния, вызывающий изменения некоторых элементов данных). ПП могут быть представлены в виде функции, ставящих в соответствие субъект и элемент данных с новым элементом данных следующим образом: ПП: субъекты $xD \rightarrow D$.

ПП – действия, которые выполняют субъекты (способные изменить определенные данные) над данными.

У данной модели, как и у других моделей, существуют свои правила. Рассмотрим их.

Правило1: в системе должны иметься процедуры утверждения целостности ( IVP (Пример-проверка контрольной суммы) – утверждают, что данный CDI имеет надлежащий уровень целостности, утверждающие любой CDI.

Правило2: применение любого ПП к любому CDI должно сохранять целостность CDI.

Правило3: только ПП может вносить изменения в CDI.

Правило4: субъекты могут инициировать только определенные ПП над определенными CDI.

Правило5: соответствующая политика в отношении разделения обязанностей субъектов. Т.е. компьютерная система определяет такую политику, чтобы не позволить субъектам изменять CDI без соответствующего вовлечения других субъектов.

Правило 6: некоторые специальные ТР могут превращать UDI в CDI.

Это правило позволяет определенным ПП получать на вход UDI и после соответствующего повышения целостности выдавать на выходе CDI.

Правило 7: каждое применение CDI должно регистрироваться в специальном CDI, в который может производиться только добавление информации, достаточной для восстановления картины о процессе работы этого CDI. Т.е. применение специального регистрационного журнала.

Правило 8: система должна распознавать субъекты, пытающая инициализировать ПП.

Это правило определяет механизмы предотвращения атак, при которых один субъект пытается выдать себя за другого.

Правило 9: система должна разрешать производить изменения в списках авторизации только специальным субъектам.

Данные правила определяют как может быть проверена целостность как и кем могут изменятся CDI, и как UDI могут быть превращены вCDI. Т.е. здесь происходит отслеживание всех изменений и тех, кто пытается внести эти изменения.

Преимущество модели в том, что она основана на проверенных временем бизнес – методов обращении с бумажными ресурсами. Недостатком является трудность реализации VIP и методов предотвращения CDI от искажения целостности.

Основным преимуществом данной модели является то, что она основана на проверенных временем бизнес методах обращения с бумажными ресурсами. Поэтому ее не следует рассматривать как академическое исследование, а скорее как комплекс существующих методов. Модель Кларка–Вилсона также предоставляет исследователям методы работы с целостностью, отличные от традиционных уровне - ориентированных подходов, таких как модели Белла–Лападула и Биба.

Основным недостатком модели является то, что IVP и методы предотвращения CDI от искажения целостности нелегко реализовать в реальных компьютерных системах.

### 4.4. Механизм защиты от угрозы отказа в обслуживании

#### 4.4.1. Мандатная модель

Мандатная модель включает в себя многие характеристики моделей Белла–Лападула и Биба.

Субъектам системы соответствуют приоритеты, которые могут быть одинаковы, ниже или выше по сравнению с приоритетом любого другого субъекта. Объектам соответствуют степени критичности, имеющие аналогичную иерархическую структуру. Субъект может требовать услугу у вычислительной системы, запрашивая доступ к объектам системы. Говорят, что субъект получает отказ в обслуживании, если его запрос зарегистрирован, но не удовлетворен в течение соответствующего MWT (максимальное время ожидания).

Рассмотрим правила, описывающие эту модель.

1. Правило «никаких отказов вверх» (NDU): ни каким объектам с более низким приоритетом не позволено отказывать в обслуживании субъектам с более высокими приоритетами. Но некоторым субъектам с более высоким приоритетом (например администратору) должна предоставляться возможность отказывать в обслуживании объектам с более низким приоритетом, если первые того желают.

2. Правило NDU(C) – обобщение NDU: субъекты с более низким приоритетом не должны препятствовать запросам услуг субъектов с более высокими приоритетами, производимых через объекты из конкретного множества C. Услуги, предоставляемые для объектов, находящихся в C, никогда не должны устаревать.

Главное преимущество этих правил – введение понятия приоритета. Недостаток – эти правила имеют смысл для систем с несколькими приоритетами.

**4.4.2. Модель Миллена – модель распределения ресурсов**

В основе модели лежит идея о том, что для выполнения нужного задания субъектам необходимы определенные временные и пространственные требования к ресурсам. Отказ происходит только в том случае, если распределение пространства и времени для некоторого процесса не отвечает соответствующим требованиям.

Введем некоторые обозначения:

P - множество активных процессов;

R - множество пассивных ресурсов;

C – некоторая фиксированная граница (обозначает максимальное число единиц для всех типов ресурсов);

$A_p$ – вектор распределения – число единиц ресурса, выделенных для процесса p в некотором состоянии;

CPU – ресурс, используемый для формирования информации о том является ли процесс текущим или застывшим. Если $A_p$(CPU) =1, то истинным является running(p), если $A_p$(CPU) = 0, то - asleep(p);

$S_{Qp}$ – вектор пространственных требований - число единиц каждого ресурса, выделенных процессом p для выполнения необходимого задания в некотором состоянии;

T(p) – функция, показывающая когда в последний раз изменились часы для процесса, с целью отражения реального времени;

$^{T}Q_p$ - вектор временных требований – объем времени, необходимого каждому ресурсу процесса p для выполнения работы.

Далее представим восемь правил, необходимых для описания модели.

1. Сумма единиц выделенных ресурсов для всех процессов из P должна быть меньше системной границы C, т.е. $S\ A_p \le C$.

2. Текущие процессы должны иметь нулевые пространственные требования, т.е.

If running(p) then $^{S}Q_p = 0$.

3. В некотором состоянии процесс является текущим и остается текущим и в следующем состоянии, т. е. If running(p) and running(p)$^1$ then $A_p\ ^1 = A_p$ .

4. Часы процесса изменяются только с изменением CPU, т.е. if $A_p$ (CPU)$^1$ = $A_p$ (CPU), then T(p)$^1$ = T(p).

5. Часы процесса изменяются только для того, чтобы отразить увеличение во времени, т. е. if $A_p$ (CPU)$^1 \neq A_p$ (CPU) then T(p)$^1$ > T(p).

6. Пространственные требования устанавливаются для застывших процессов, т.е. if asleep(p) then $^{S}Q_p{}^1 = {}^{S}Q_p + A_p - A_p\ ^1$.

7. Временные требования для застывших процессов не устанавливаются, т.е. if asleep(p) then $^{T}Q_p{}^1 = {}^{T}Q_p$.

8. Переходы в результате которых процесс останавливается, перераспределяют только ресурсы CPU, т.е. If running(p) and asleep (p)$^1$ then $A_p\ ^1 = A_p$ - CPU.

## 5. Основные критерии защищенности АС. Классы защищенности

### 5.1. Стандарт оценки безопасности компьютерных систем TCSEC («Оранжевая книга»)

"Критерии оценки безопасности компьютерных систем" (Trusted Computer System Evaluation Criteria - TCSEC) [8], получившие неформальное "Оранжевая книга" (по цвету обложки первоначального издания), были разработаны и опубликованы Министерством обороны США в 1983г. с целью определения требований безопасности, предъявляемых к аппаратному, программному и специальному программному и информационному обеспечению компьютерных систем, и выработки методологии и технологии анализа степени поддержки политики безопасности в компьютерных системах в основном военного назначения.

"Оранжевая книга" поясняет понятие безопасной системы, которая управляет, посредством соответствующих средств, доступом к информации, так что только должным образом авторизованные лица или процессы, действующие от их имени, получают право читать, писать, создавать и удалять информацию. Очевидно, однако, что абсолютно

безопасных систем не существует, что это абстракция. Любую систему можно "взломать", если располагать достаточно большими материальными и временными ресурсами. Есть смысл оценивать лишь степень доверия, которое разумно оказать той или иной системе

**Общая структура требований TCSEC**

В «Оранжевой книге» предложены три категории требований безопасности: политика безопасности, аудит и корректность, в рамках которых сформулированы шесть базовых требований безопасности. Первые четыре требования направлены непосредственно на обеспечение безопасности информации, а два последних - на качество средств защиты. Рассмотрим эти требования подробнее.

**Политика безопасности**

Требование 1. *Политика безопасности.* Система должна поддерживать точно определенную политику безопасности. Возможность доступа субъектов к объектам должна определяться на основании их идентификации и набора правил управления доступом. Там, где это необходимо, должна использоваться политика мандатного управления доступом, позволяющая эффективно реализовать разграничение доступа к информации различного уровня конфиденциальности.

Требование 2. *Метки.* С объектами должны быть ассоциированы метки безопасности, используемые в качестве исходной информации для процедур контроля доступа. Для реализации мандатного управления доступом система должна обеспечивать возможность присваивать каждому объекту метку или набор атрибутов, определяющих степень конфиденциальности (гриф секретности) объекта и режимы доступа к этому объекту.

**Подотчетность**

Требование 3. *Идентификация и аутентификация.* Все субъекты должны иметь уникальные идентификаторы. Контроль доступа должен осуществляться на основании результатов идентификации субъекта и объекта доступа, подтверждения подлинности их идентификаторов (аутентификации) и правил разграничения доступа. Данные, используемые для идентификации и аутентификации, должны быть защищены от несанкционированного доступа, модификации и уничтожения и должны быть ассоциированы со всеми активными компонентами компьютерной системы, функционирование которых критично с точки зрения безопасности.

Требование 4. *Регистрация и учет.* Для определения степени ответственности пользователей за действия в системе, все происходящие в ней события, имеющие значение с точки зрения безопасности, должны отслеживаться и регистрироваться в защищенном протоколе (т.е. должен существовать объект компьютерной системы, потоки от которого и к которому доступны только субъекту администрирования). Система регистрации должна осуществлять анализ общего потока событий и выделять из него только те события, которые оказывают влияние на безопасность для

сокращения объема протокола и повышения эффективности его анализа. Протокол событий должен быть надежно защищен от несанкционированного доступа, модификации и уничтожения.

**Гарантии (корректность)**

Требование 5. *Контроль корректности функционирования средств защиты.* Средства защиты должны содержать независимые аппаратные и/или программные компоненты, обеспечивающие работоспособность функций защиты. Это означает, что все средства защиты, обеспечивающие политику безопасности, управление атрибутами и метками безопасности, идентификацию и аутентификацию, регистрацию и учет, должны находиться под контролем средств, проверяющих корректность их функционирования. Основной принцип контроля корректности состоит в том, что средства контроля должны быть полностью независимы от средств защиты.

Требование 6. *Непрерывность защиты.* Все средства защиты (в том числе и реализующие данное требование) должны быть защищены от несанкционированного вмешательства и/или отключения, причем эта защита должна быть постоянной и непрерывной в любом режиме функционирования системы защиты и компьютерной системы в целом. Данное требование распространяется на весь жизненный цикл компьютерной системы. Кроме того, его выполнение является одной из ключевых аксиом, используемых для формального доказательства безопасности системы.

**Классы защищенности компьютерных систем по TCSEC**

«Оранжевая книга» предусматривает четыре группы критериев, которые соответствуют различной степени защищенности: от минимальной (группа D) до формально доказанной (группа А). Каждая группа включает один или несколько классов. Группы D и А содержат по одному классу (классы D и А соответственно), группа С - классы С1, С2, а группа В три класса - В1, В2, В3, характеризующиеся различными наборами требований защищенности. Уровень защищенности возрастает от группы D к группе А, а внутри группы - с увеличением номера класса. Таким образом имеем всего шесть классов безопасности - С1, С2, Bl, В2, В3, А1. Усиление требований осуществляется с постепенным смещением акцентов от положений, определяющих наличие в системе каких-то определенных механизмов защиты, к положениям обеспечивающих высокий уровень гарантий того, что система функционирует в соответствии требованиям политики безопасности.

Чтобы система в результате процедуры сертификации могла быть отнесена к некоторому классу, ее политика безопасности и гарантированность должны удовлетворять приводимым ниже требованиям. Поскольку при переходе к каждому следующему классу требования только добавляются, мы будем выписывать лишь то новое, что присуще данному классу, группируя требования в согласии с предшествующим изложением.

Группа D. Минимальная защита

Класс D. Минимальная защита. Класс D зарезервирован для тех систем, которые были представлены на сертификацию (оценку), но по какой-либо причине ее не прошли.

Группа C. Дискреционная защита

Группа C характеризуется наличием дискреционного управления доступом и аудитом действий субъектов.

Класс C1. Системы на основе дискреционного разграничения доступа. TCB (доверительная база вычислений) систем, соответствующих этому классу защиты, удовлетворяет неким минимальным требованиям безопасного разделения пользователей и данных. Она определяет некоторые формы разграничения доступа на индивидуальной основе, т.е. пользователь должен иметь возможность защитить свою информацию от ее случайного чтения или уничтожения. Пользователи могут обрабатывать данные как по отдельности, так и от имени группы пользователей.

*Политика безопасности*. Надежная вычислительная база должна управлять доступом именованных пользователей к именованным объектам. Механизм управления (права для владельца/группы/прочих, списки управления доступом) должен позволять пользователям специфицировать разделение файлов между индивидами и/или группами.

*Подотчетность.* Пользователь должен идентифицировать себя, прежде чем выполнять какие – либо действия, контролируемые надежной вычислительной базой. Для аутентификации должен использоваться какой – либо защитный механизм, например, пароли. Аутентификационная информация должна быть защищена от несанкционированного доступа.

*Гарантии*. Надежная вычислительная база должна поддерживать область для собственного выполнения, защищенную от внешних воздействий (в частности, от изменения команд и/или данных) и от попыток слежения за ходом работы. Ресурсы, контролируемые базой, могут составлять определенное подмножество всех субъектов и объектов системы. Защитные механизмы должны быть протестированы на предмет соответствия их поведения системной документации. Тестирование должно подтвердить, что у неавторизованного пользователя нет очевидных способов обойти или разрушить средства защиты надежной вычислительной базы.

*Документация:*

- Руководство пользователя по средствам безопасности: отдельный фрагмент документации (глава, том) должен описывать защитные механизмы, предоставляемые надежной вычислительной базой, и их взаимодействие между собой, содержать рекомендации по их использованию.

- Руководство администратора по средствам безопасности: руководство должно содержать сведения о функциях и привилегиях, которыми управляет системный администратор посредством механизмов безопасности.
- Тестовая документация: разработчик системы должен представить экспертному совету документ, содержащий план тестов, процедуры прогона тестов и результаты тестов.
- Описание архитектуры: должны быть описаны подход к безопасности, используемый производителем, и применение этого подхода при реализации надежной вычислительной базы. Если база состоит из нескольких модулей, должен быть описан интерфейс между ними.

Класс С2. Системы, построенные на основе управляемого дискреционного разграничения доступа.

Системы, сертифицированные по данному классу, должны удовлетворять всем требованиям, изложенным в классе С1. Однако, системы класса С2 поддерживают более тонкую, чем в классе С1, политику дискреционного разграничения доступа, делающую пользователя индивидуально ответственным за свои действия после процедуры аутентификации в системе, а также аудит событий, связанных с безопасностью системы.

*Политика безопасности.* В дополнение к С1, права доступа должны гранулироваться с точностью до пользователя. Механизм управления должен ограничивать распространение прав доступа - только авторизованный пользователь (например, владелец объекта) может предоставлять права доступа другим пользователям. Все объекты должны подвергаться контролю доступа. При выделении хранимого объекта из пула ресурсов надежной вычислительной базы необходимо ликвидировать все следы предыдущих использований.

*Подотчетность*. В дополнение к С1, каждый пользователь системы должен уникальным образом идентифицироваться. Каждое регистрируемое действие должно ассоциироваться с конкретным пользователем.

Надежная вычислительная база должна создавать, поддерживать и защищать журнал регистрационной информации, относящейся к доступу к объектам, контролируемым базой. Должна быть возможность регистрации следующих событий:

- использование механизма идентификации и аутентификации,
- внесение объектов в адресное пространство пользователя (например, открытие файла, запуск программы);
- удаление объектов;
- действия системных операторов, системных администраторов, администраторов безопасности;
- другие события, затрагивающие информационную безопасность.

Каждая регистрационная запись должна включать следующие поля:

- дата и время события;
- идентификатор пользователя;
- тип события;
- результат действия (успех или неудача).

Для событий идентификации/аутентификации регистрируется также идентификатор устройства (например, терминала). Для действий с объектами регистрируются имена объектов. Системный администратор может выбирать набор регистрируемых событий для каждого пользователя.

*Гарантии*. В дополнение к С1, надежная вычислительная база должна изолировать защищаемые ресурсы в той мере, как это диктуется требованиями контроля доступа и подотчетности. Тестирование должно подтвердить отсутствие очевидных недостатков в механизмах изоляции ресурсов и защиты регистрационной информации.

*Документация*. Руководство администратора по средствам безопасности в дополнение к С1, должны описываться процедуры обработки регистрационной информации и управления файлами с такой информацией, а также структура записей для каждого типа регистрируемых событий.

Группа В. Мандатное управление доступом

Основные требования этой группы - мандатное (полномочное) управление доступом с использованием меток безопасности, реализация некоторой формальной модели политики безопасности, а также наличие спецификаций на функции ТСВ. В системах этой группы постепенно к классу В3 должен быть реализован монитор ссылок (или МБО), который должен контролировать все доступы субъектов к объектам системы.

Класс В1. Системы класса В1 должны удовлетворять требованиям класса С2. Кроме того, должны быть выполнены следующие дополнительные требования.

*Политика безопасности*. Надежная вычислительная база должна управлять метками безопасности, ассоциируемыми с каждым субъектом и хранимым объектом. Метки являются основой функционирования механизма принудительного управления доступом. При импорте непомеченной информации соответствующий уровень секретности должен запрашиваться у авторизованного пользователя и все такие действия следует протоколировать.

Метки должны адекватно отражать уровни секретности субъектов и объектов. При экспорте информации метки должны преобразовываться в точное и однозначно трактуемое внешнее представление, сопровождающее данные. Каждое устройство ввода/вывода (в том числе коммуникационный канал) должно трактоваться как

одноуровневое или многоуровневое. Все изменения трактовки и ассоциированных уровней секретности должны протоколироваться.

Надежная вычислительная база должна обеспечить проведение в жизнь принудительного управления доступом всех субъектов ко всем хранимым объектам. Субъектам и объектам должны быть присвоены метки безопасности, являющиеся комбинацией упорядоченных уровней секретности, а также категорий. Метки являются основой принудительного управления доступом. Надежная вычислительная база должна поддерживать, по крайней мере, два уровня секретности. Субъект может читать объект, если его (субъекта) метка безопасности доминирует над меткой безопасности объекта, то есть уровень секретности субъекта не меньше уровня секретности объекта и все категории объекта входят в метку безопасности субъекта. Субъект может писать в объект, если метка безопасности объекта доминирует над меткой субъекта. Надежная вычислительная база должна контролировать идентификационную и аутентификационную информацию. При создании новых субъектов (например, процессов) их метки безопасности не должны доминировать над меткой породившего их пользователя.

*Подотчетность*. В дополнение к С2, надежная вычислительная база должна поддерживать метки безопасности пользователей, должны регистрироваться операции выдачи на печать и ассоциированные внешние представления меток безопасности. При операциях с объектами, помимо имен, регистрируются их метки безопасности. Набор регистрируемых событий может различаться в зависимости от уровня секретности объектов.

*Гарантии*. В дополнение к С2, надежная вычислительная база должна обеспечивать взаимную изоляцию процессов путем разделения их адресных пространств. Группа специалистов, полностью понимающих конкретную реализацию надежной вычислительной базы, должна подвергнуть описание архитектуры, исходные и объектные коды тщательному анализу и тестированию. Цель должна состоять в выявлении всех дефектов архитектуры и реализации, позволяющих субъекту без должной авторизации читать, изменять, удалять информацию или приводить базу в состояние, когда она перестает обслуживать запросы других субъектов Все выявленные недостатки должны быть исправлены или нейтрализованы, после чего база подвергается повторному тестированию, чтобы убедиться в отсутствии старых или новых недостатков. Должна существовать неформальная или формальная модель политики безопасности, поддерживаемой надежной вычислительной базой. Модель должна соответствовать основным посылкам политики безопасности на протяжении всего жизненного цикла системы.

*Документация*. Руководство администратора по средствам безопасности в дополнение к С2 должно описывать функции оператора и администратора, затрагивающие безопасность, в том числе действия по изменению характеристик пользователей. Должны быть

представлены рекомендации по взаимодействию друг с другом, по безопасной генерации новых версий надежной вычислительной базы.

Должно быть представлено неформальное или формальное описание модели политики безопасности, проводимой в жизнь надежной вычислительной базой. Необходимо наличие аргументов в пользу достаточности избранной модели для реализации политики безопасности. Должны быть описаны защитные механизмы базы и их место в модели.

Класс B2. Структурированная защита. Выполняются все требования класса защиты B1. Кроме того, в системах класса B2 TCB основывается на четко определенной и хорошо документированной формальной модели политики безопасности, требующей, чтобы мандатная и дискреционная системы разграничения доступа были распространены на все субъекты и объекты компьютерной системы. TCB должна быть четко структурирована на элементы, критичные с точки зрения безопасности и некритичные. Интерфейс TCB должен быть хорошо определен и ее проект и конечный результат должны быть подвергнуты полной проверке и тестированию. Механизм аудита должен быть усилен, введен контроль за конфигурацией; системы. Система должна быть устойчива к внешнему проникновению.

*Политика безопасности*. В дополнение к B1, помечаться должны все ресурсы системы прямо или косвенно доступные субъектам. Надежная вычислительная база должна немедленно извещать терминального пользователя об изменении его метки безопасности. Пользователь может запросить информацию о своей метке. Надежная вычислительная база должна поддерживать присваивание всем подключенным физическим устройствам минимального и максимального уровня секретности. Эти уровни должны использоваться при проведении в жизнь ограничений, налагаемых физической конфигурацией системы (например, расположением устройств).

Все ресурсы системы (в том числе ПЗУ, устройства ввода/вывода) должны иметь метки безопасности и служить объектами принудительного управления доступом.

*Подотчетность*. Надежная вычислительная база должна поддерживать надежный коммуникационный путь к себе для пользователя, выполняющего операции начальной идентификации и аутентификации. Инициатива в общении по этому пути должна исходить исключительно от пользователя. В дополнение к B1, должна быть возможность регистрировать события, связанные с организацией тайных каналов с памятью.

*Гарантии*. В дополнение к B1, надежная вычислительная база должна быть внутренне структурирована на хорошо определенные, относительно независимые модули. Надежная вычислительная база должна эффективно использовать имеющееся оборудование для отделения элементов, критически важных с точки зрения защиты, от прочих компонентов системы. Модули базы должны проектироваться с учетом принципа минимизации привилегий. Для защиты логически раздельных хранимых объектов должны использоваться

аппаратные средства, такие как сегментация. Должен быть полностью определен пользовательский интерфейс к надежной вычислительной базе и все элементы базы.

Системный архитектор должен тщательно проанализировать возможности по организации тайных каналов с памятью и оценить максимальную пропускную способность каждого выявленного канала.

Система должна поддерживать разделение функций оператора и администратора.

В дополнение к B1, должна быть продемонстрирована относительная устойчивость надежной вычислительной базы к попыткам проникновения. Модель политики безопасности должна быть формальной. Для надежной вычислительной базы должны существовать описательные спецификации верхнего уровня, точно и полно определяющие ее интерфейс.

В процессе разработки и сопровождения надежной вычислительной базы должна использоваться система конфигурационного управления, обеспечивающая контроль за изменениями в описательных спецификациях верхнего уровня, иных архитектурных данных, реализационной документации, исходных текстах, работающей версии объектного кода, тестовых данных и документации. Конфигурационное управление должно обеспечивать соответствие друг другу всех аспектов текущей версии надежной вычислительной базы. Должны предоставляться средства генерации новых версий базы по исходным текстам и средства для сравнения версий, чтобы убедиться в том, что произведены только запланированные изменения.

*Документация.* В дополнение к B1, должны быть указаны модули надежной вычислительной базы, содержащие механизмы проверки обращений. Должна быть описана процедура безопасной генерации новой версии базы после внесения изменений в исходные тексты.

В дополнение к C1, тесты должны подтверждать действенность мер по уменьшению пропускной способности тайных каналов передачи информации.

Модель политики безопасности должна быть формальной и доказательной. Должно быть показано, что описательные спецификации верхнего уровня точно отражают интерфейс надежной вычислительной базы. Должно быть показано, как база реализует концепцию монитора обращений, почему она устойчива к попыткам отслеживания ее работы, почему ее нельзя обойти и почему она реализована корректно, Должна быть описана структура базы, чтобы облегчить ее тестирование и проверку соблюдения принципа минимизации привилегий. Документация должна содержать результаты анализа тайных каналов передачи информации и описание мер протоколирования, помогающих выявлять каналы с памятью.

Класс В3. Домены безопасности. В системах класса В3 ТСВ должна удовлетворять всем требованиям предыдущего класса и дополнительно требованиям монитора ссылок, который должен быть:

- защищен от несанкционированного изменения или порчи;
- обрабатывать все обращения;
- прост для анализа и тестирования.

ТСВ должна быть структурирована таким образом, чтобы исключить код, не имеющий отношения к безопасности системы. Дополнительно должно быть обеспечено:

- поддержка администратора безопасности;
- расширение механизма аудита с целью сигнализации о любых событиях, связанных с безопасностью;
- поддержка процедуры восстановления системы.

*Политика безопасности*. В дополнение к С2, должны обязательно использоваться списки управления доступом с указанием разрешенных режимов. Должна быть возможность явного указания пользователей или их групп, доступ которых к объекту запрещен.

*Подотчетность.* В дополнение к В2, надежный коммуникационный путь может формироваться по запросу, исходящему как от пользователя, так и от самой базы. Надежный путь может использоваться для начальной идентификации и аутентификации, для изменения текущей метки безопасности пользователя и т.п. Общение по надежному пути должно быть логически отделено и изолировано от других информационных потоков. Должна быть возможность регистрации появления или накопления событий, несущих угрозу политике безопасности системы.

Администратор безопасности должен немедленно извещаться о попытках нарушения политики безопасности. А система, в случае продолжения попыток, должна пресекать их наименее болезненным способом.

*Гарантии*. В дополнение к В2, надежная вычислительная база должна быть спроектирована и структурирована таким образом, чтобы использовать полный и концептуально простой защитный механизм с точно определенной семантикой. Этот механизм должен играть центральную роль во внутренней структуризации надежной вычислительной базы и всей системы. База должна активно использовать разделение по уровням, абстракцию и инкапсуляцию данных. Значительные инженерные усилия должны быть направлены на уменьшение сложности надежной вычислительной базы и на вынесение из нее модулей, не являющихся критически важными с точки зрения защиты.

Должна быть специфицирована роль администратора безопасности. Получить права администратора безопасности можно только после выполнения явных, протоколируемых

действий. Не относящиеся к защите действия администратора безопасности должны быть по возможности ограничены.

Должны существовать процедуры и/или механизмы, позволяющие произвести восстановление после сбоя или иного нарушения работы без ослабления защиты.

Должна быть продемонстрирована устойчивость надежной вычислительной базы к попыткам проникновения. Не должно быть выявлено архитектурных недостатков. Допускается выявление лишь небольшого числа исправимых недостатков реализации. Должна существовать обоснованная уверенность, что немногие недостатки остались невыявленными.

*Документация.* Руководство администратора по средствам безопасности в дополнение к B2, должна быть описана процедура, обеспечивающая безопасность начального запуска системы и возобновления ее работы после сбоя. Должно быть неформально продемонстрировано соответствие между описательными спецификациями верхнего уровня и реализацией надежной вычислительной базы.

Группа А. Верифицированная защита

Данная группа характеризуется применением формальных методов верификации, корректности работы механизмов управления доступом (дискреционного и мандатного). Требуется, чтобы было формально показано соответствие архитектуры и реализации ТСВ требованиям безопасности.

Класс А1. Формальная верификация. Критерий защиты класса А1 не определяет дополнительные по сравнению с классом В3 требования к архитектуре или политике безопасности компьютерной системы. Дополнительным свойством систем, отнесенных к классу А1, является проведенный анализ ТСВ на соответствие формальным высокоуровневым спецификациям и использование технологий проверки с целью получения высоких гарантий того, что ТСВ функционирует корректно.

Наиболее важные требования к классу А1 можно объединить в пять групп.

1. Формальная модель политики безопасности должна быть четко определена и документирована, должно быть дано математическое доказательство того, что модель соответствует своим аксиомам и что их достаточно для поддержания заданной политики безопасности.

2. Формальная высокоуровневая спецификация должна включать абстрактное определение выполняемых ТСВ функций и аппаратный и (или) встроенный программный механизм для обеспечения разделения доменов.

3. Формальная высокоуровневая спецификация ТСВ должна демонстрировать соответствие модели политики безопасности с использованием, где это возможно,

формальной технологии (например, где имеются проверочные средства) и неформальной во всех остальных случаях.

4. Должно быть неформально показано и обратное - соответствие элементов ТСВ формальной высокоуровневой спецификации. Формальная высокоуровневая спецификация должна представлять собой универсальный механизм защиты, реализующий политику безопасности. Элементы этого механизма должны быть отображены на элементы ТСВ.

5. Должны быть использованы формальные технологии для выявления и анализа скрытых каналов. Неформальная технология может быть использована для анализа скрытых временных каналов. Существование оставшихся в системе скрытых каналов должно быть оправдано.

Более строгие требования предъявляются к управлению конфигурацией системы и конкретному месту дислокации (развертывания) системы

Перечисленные требования не затрагивают группы Политика безопасности и Подотчетность и сконцентрированы в группе Гарантии с соответствующим описанием в группе Документация.

### 5.2. Концепции защиты автоматизированных систем и средств вычислительной техники по руководящим документам Гостехкомиссии РФ

В 1992 г. Гостехкомиссия (ГТК) при Президенте Российской Федерации разработала и опубликовала пять руководящих документов [9], посвященных вопросам защиты информации в автоматизированных системах (АС) ее обработки. Основой этих документов является концепция защиты средств вычислительной техники (СВТ) и АС от несанкционированного доступа к информации, содержащая систему взглядов ГТК на проблему информационной безопасности и основные принципы защиты компьютерных систем. С точки зрения разработчиков данных документов, основная задача средств безопасности - это обеспечение защиты от несанкционированного доступа к информации. Определенный уклон в сторону поддержания секретности информации объясняется тем, что данные документы были разработаны в расчете на применение в информационных системах силовых структур РФ.

Структура требований безопасности

Руководящие документы ГТК состоят из пяти частей.

1. Защита от несанкционированного доступа к информации. Термины и определения.
2. Концепция защиты СВТ и АС от НСД к информации.
3. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.

4. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации.

5. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД в автоматизированных системах и средствах вычислительной техники.

Наибольший интерес представляют вторая, третья и четвертая части. Во второй части излагается система взглядов, основных принципов, которые закладываются в основу проблемы защиты информации от НСД. Руководящие документы ГТК предлагают две группы требований к безопасности - показатели защищенности СВТ от НСД и критерии защищенности АС обработки данных. Первая группа позволяет оценить степень защищенности отдельно поставляемых потребителю компонентов АС и рассматривается в четвертой части, а вторая рассчитана на более сложные комплексы, включающие несколько единиц СВТ, и представлена в третьей части руководящих документов.

**Классы защищенности АС**

В третьей части руководящих документов ГТК дается классификация АС и требований по защите информации в АС различных классов. При этом определяются:

1. Основные этапы классификации АС:

разработка и анализ исходных данных;

выявление основных признаков АС, необходимых для классификация

сравнение выявленных признаков АС с классифицируемыми;

присвоение АС соответствующего класса защиты информации от НСД.

2. Необходимые исходные данные для классификации конкретной АС:

перечень защищаемых информационных ресурсов АС и их уровень конфиденциальности;

перечень лиц, имеющих доступ к штатным средствам АС с указанием их уровня полномочий;

матрица доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам АС;

режим обработки данных в АС.

3. Признаки, по которым производится группировка АС в различные классы:

наличие в АС информации различного уровня конфиденциальности;|

уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;

режим обработки данных в АС: коллективный или индивидуальный.

Документы ГТК устанавливают девять классов защищенности АС от НСД, распределенных по трем группам. Каждый класс характеризуется определенной

совокупностью требований к средствам защиты. В пределах каждой группы соблюдается иерархия классов защищенности АС. Класс, соответствующий высшей степени защищенности для данной группы, обозначается индексом NA, где N- номер группы (от 1 до 3). Следующий класс обозначается NБ и т.д.

Третья группа включает АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса - ЗБ и ЗА.

Вторая группа включает АС, в которых пользователи имеют одинаковые полномочия доступа ко всей информации, обрабатываемой и хранимой в АС на носителях различного уровня конфиденциальности. Группа содержит два класса -2Б и 2А.

Первая группа включает многопользовательские АС, в которых одновременно обрабатывается и хранится информация разных уровней конфиденциальности. Не все пользователи имеют равные права доступа.. Группа содержит пять классов - 1Д, 1 Г, 1 В, 1Б и 1А.

В табл. 5.2 приведены требования к подсистемам защиты для каждого класса защищенности.

На разработку этих документов наибольшее влияние оказал критерий TCSEC ("Оранжевая книга"), однако это влияние в основном отражается в ориентированности этих документов на защищенные системы силовых структур и в использовании единой универсальной шкалы оценки степени защищенности.

К недостаткам руководящих документов ГТК относятся: ориентация на противодействие НСД и отсутствие требований к адекватности реализации политики безопасности. Понятие "политика безопасности" трактуется исключительно как поддержание режима секретности и отсутствие НСД. Из-за этого средства защиты ориентируются только на противодействие внешним угрозам, а к структуре самой системы и ее функционированию не предъявляется четких требований. Ранжирование требований по классам защищенности по сравнению с остальными стандартами информационной безопасности максимально упрощено и сведено до определения наличия или отсутствия заданного набора механизмов защиты, что существенно снижает гибкость требований и возможность их практического применения. Несмотря на указанные недостатки, документы ГТК заполнили "правовой вакуум" в области стандартов информационной безопасности в России и оперативно решили проблему проектирования и оценки качества защищенных АС.

### 5.3. Критерии оценки безопасности информационных технологий (Common Criteria)

**Основные понятия**

«Критериев оценки безопасности информационных технологий» [10] (издан 1 декабря 1999 года) - самый полный и современный среди оценочных стандартов. Этот международный стандарт стал итогом почти десятилетней работы специалистов нескольких стран, он вобрал в себя опыт существовавших к тому времени документов национального и межнационального масштаба.

По историческим причинам данный стандарт часто называют «Общими критериями» (или даже ОК). Мы также будем использовать это сокращение.

«Общие критерии» на самом деле являются метастандартом, определяющим инструменты оценки безопасности информационной системы (ИС) и порядок их использования. В отличие от «Оранжевой книги», ОК не содержат предопределенных «классов безопасности». Такие классы можно строить, исходя из требований безопасности, существующих для конкретной организации и/или конкретной информационной системы.

С программистской точки зрения ОК можно считать набором библиотек, помогающих писать содержательные «программы» – задания по безопасности, типовые профили защиты и т.п. Программисты знают, насколько хорошая библиотека упрощает разработку программ, повышает их качество. Без библиотек, «с нуля», программы не пишут уже очень давно; оценка безопасности тоже вышла на сопоставимый уровень сложности, и «Общие критерии» предоставили соответствующий инструментарий.

Как и «Оранжевая книга», ОК содержат два основных вида требований безопасности:

- функциональные, соответствующие активному аспекту защиты, предъявляемые к функциям безопасности и реализующим их механизмам;
- требования доверия, соответствующие пассивному аспекту, предъявляемые к технологии и процессу разработки и эксплуатации.

Требования безопасности предъявляются, а их выполнение проверяется для определенного объекта оценки – аппаратно-программного продукта или информационной системы.

Очень важно, что безопасность в ОК рассматривается не статично, а в привязке к жизненному циклу объекта оценки. Выделяются следующие этапы:

- определение назначения, условий применения, целей и требований безопасности;
- проектирование и разработка;
- испытания, оценка и сертификация;
- внедрение и эксплуатация.

В ОК объект оценки рассматривается в контексте среды безопасности, которая характеризуется определенными условиями и угрозами.

В свою очередь, угрозы характеризуются следующими параметрами:

- источник угрозы;
- метод воздействия;
- уязвимые места, которые могут быть использованы;
- ресурсы (активы), которые могут пострадать.

Уязвимые места могут возникать из-за недостатка в:

- требованиях безопасности;
- проектировании;
- эксплуатации.

Слабые места по возможности следует устранить, минимизировать или хотя бы постараться ограничить возможный ущерб от их преднамеренного использования или случайной активизации.

Чтобы структурировать пространство требований, в «Общих критериях» введена иерархия класс – семейство – компонент - элемент.

Классы определяют наиболее общую, «предметную» группировку требований (например, функциональные требования подотчетности).

Семейства в пределах класса различаются по строгости и другим нюансам требований.

Компонент – минимальный набор требований, фигурирующий как целое.

Элемент – неделимое требование.

Между компонентами ОК могут существовать зависимости. Они возникают, когда компонент сам по себе недостаточен для достижения цели безопасности. Но не все комбинации компонентов имеют смысл.

Как указывалось выше, с помощью библиотек могут формироваться два вида нормативных документов: профиль защиты и задание по безопасности.

Профиль защиты (ПЗ) представляет собой типовой набор требований, которым должны удовлетворять продукты и/или системы определенного класса (например, операционные системы на компьютерах в правительственных организациях).

Задание по безопасности содержит совокупность требований к конкретной разработке, выполнение которых обеспечивает достижение поставленных целей безопасности.

Выше мы отмечали, что в ОК нет готовых классов защиты. Сформировать классификацию в терминах «Общих критериев» – значит определить несколько иерархически упорядоченных (содержащих усиливающиеся требования) профилей защиты, в максимально возможной степени использующих стандартные функциональные требования и требования доверия безопасности.

Выделение некоторого подмножества из всего множества профилей защиты во многом носит субъективный характер. По целому ряду соображений (одним из которых является желание придерживаться объектно-ориентированного подхода) целесообразно, на наш

взгляд, сформировать сначала отправную точку классификации, выделив базовый (минимальный) ПЗ, а дополнительные требования компоновать в функциональные пакеты.

Функциональный пакет – это неоднократно используемая совокупность компонентов, объединенных для достижения определенных целей безопасности. «Общие критерии» не регламентируют структуру пакетов, процедуры верификации, регистрации и т.п., отводя им роль технологического средства формирования ПЗ.

Базовый профиль защиты должен включать требования к основным (обязательным в любом случае) возможностям. Производные профили получаются из базового путем добавления необходимых пакетов расширения, то есть подобно тому, как создаются производные классы в объектно-ориентированных языках программирования.

**Функциональные требования**

Функциональные требования сгруппированы на основе выполняемой ими роли или обслуживаемой цели безопасности. Всего в «Общих критериях» представлено 11 функциональных классов, 66 семейств, 135 компонентов. Это, конечно, значительно больше, чем число аналогичных сущностей в «Оранжевой книге».

Перечислим классы функциональных требований ОК:

- идентификация и аутентификация;
- защита данных пользователя;
- защита функций безопасности (требования относятся к целостности и контролю данных сервисов безопасности и реализующих их механизмов);
- управление безопасностью (требования этого класса относятся к управлению атрибутами и параметрами безопасности);
- аудит безопасности (выявление, регистрация, хранение, анализ данных, затрагивающих безопасность объекта оценки, реагирование на возможное нарушение безопасности);
- доступ к объекту оценки;
- приватность (защита пользователя от раскрытия и несанкционированного использования его идентификационных данных);
- использование ресурсов (требования к доступности информации);
- криптографическая поддержка (управление ключами);
- связь (аутентификация сторон, участвующих в обмене данными);
- доверенный маршрут/канал (для связи с сервисами безопасности).

Опишем подробнее два класса, демонстрирующие особенности современного подхода к ИБ.

Класс «Приватность» содержит 4 семейства функциональных требований.

Анонимность. Позволяет выполнять действия без раскрытия идентификатора пользователя другим пользователям, субъектам и/или объектам. Анонимность может быть полной или выборочной. В последнем случае она может относиться не ко всем операциям и/или не ко всем пользователям (например, у уполномоченного пользователя может оставаться возможность выяснения идентификаторов пользователей).

Псевдонимность. Напоминает анонимность, но при применении псевдонима поддерживается ссылка на идентификатор пользователя для обеспечения подотчетности или для других целей.

Невозможность ассоциации. Семейство обеспечивает возможность неоднократного использования информационных сервисов, но не позволяет ассоциировать случаи использования между собой и приписать их одному лицу. Невозможность ассоциации защищает от построения профилей поведения пользователей (и, следовательно, от получения информации на основе подобных профилей).

Скрытность. Требования данного семейства направлены на то, чтобы можно было использовать информационный сервис с сокрытием факта использования. Для реализации скрытности может применяться, например, широковещательное распространение информации, без указания конкретного адресата. Годятся для реализации скрытности и методы стеганографии, когда скрывается не только содержание сообщения (как в криптографии), но и сам факт его отправки.

Еще один показательный (с нашей точки зрения) класс функциональных требований – «Использование ресурсов», содержащий требования доступности. Он включает три семейства.

Отказоустойчивость. Требования этого семейства направлены на сохранение доступности информационных сервисов даже в случае сбоя или отказа. В ОК различаются активная и пассивная отказоустойчивость. Активный механизм содержит специальные функции, которые активизируются в случае сбоя. Пассивная отказоустойчивость подразумевает наличие избыточности с возможностью нейтрализации ошибок.

Обслуживание по приоритетам. Выполнение этих требований позволяет управлять использованием ресурсов так, что низкоприоритетные операции не могут помешать высокоприоритетным.

Распределение ресурсов. Требования направлены на защиту (путем применения механизма квот) от несанкционированной монополизации ресурсов.

«Общие критерии» – очень продуманный и полный документ с точки зрения функциональных требований. В то же время, хотелось бы обратить внимание и на некоторые недостатки.

Первый – это отсутствие объектного подхода. Функциональные требования не сгруппированы в осмысленные наборы (объектные интерфейсы), к которым могло бы применяться наследование. Подобное положение, как известно из технологии программирования, чревато появлением слишком большого числа комбинаций функциональных компонентов, несопоставимых между собой.

В современном программировании ключевым является вопрос накопления и многократного использования знаний. Стандарты – одна из форм накопления знаний. Следование в ОК «библиотечному», а не объектному подходу сужает круг фиксируемых знаний, усложняет их корректное использование.

К сожалению, в «Общих критериях» отсутствуют архитектурные требования, что является естественным следствием избранного старомодного программистского подхода «снизу вверх». Технологичность средств безопасности, следование общепризнанным рекомендациям по протоколам и программным интерфейсам, а также апробированным архитектурным решениям, таким как менеджер/агент, – необходимые качества изделий информационных технологий, предназначенных для поддержки критически важных функций, к числу которых, безусловно, относятся функции безопасности. Без рассмотрения интерфейсных аспектов системы оказываются нерасширяемыми и изолированными. Очевидно, с практической точки зрения это недопустимо. В то же время, обеспечение безопасности интерфейсов – важная задача, которую желательно решать единообразно.

**Требования доверия безопасности**

Установление доверия безопасности, согласно «Общим критериям», основывается на активном исследовании объекта оценки.

Форма представления требований доверия, в принципе, та же, что и для функциональных требований. Специфика состоит в том, что каждый элемент требований доверия принадлежит одному из трех типов:

- действия разработчиков;
- представление и содержание свидетельств;
- действия оценщиков.

Всего в ОК 10 классов, 44 семейства, 93 компонента требований доверия безопасности. Перечислим классы:

- разработка (требования для поэтапной детализации функций безопасности от краткой спецификации до реализации);
- поддержка жизненного цикла (требования к модели жизненного цикла, включая порядок устранения недостатков и защиту среды разработки);
- тестирование;
- оценка уязвимостей (включая оценку стойкости функций безопасности);

- поставка и эксплуатация;
- управление конфигурацией;
- руководства (требования к эксплуатационной документации);
- поддержка доверия (для поддержки этапов жизненного цикла после сертификации);
- оценка профиля защиты;
- оценка задания по безопасности.

Применительно к требованиям доверия в "Общих критериях" сделана весьма полезная вещь, не реализованная, к сожалению, для функциональных требований. А именно, введены так называемые оценочные уровни доверия (их семь), содержащие осмысленные комбинации компонентов.

Оценочный уровень доверия 1 (начальный) предусматривает анализ функциональной спецификации, спецификации интерфейсов, эксплуатационной документации, а также независимое тестирование. Уровень применим, когда угрозы не рассматриваются как серьезные.

Оценочный уровень доверия 2, в дополнение к первому уровню, предусматривает наличие проекта верхнего уровня объекта оценки, выборочное независимое тестирование, анализ стойкости функций безопасности, поиск разработчиком явных уязвимых мест.

На уровне 3 ведется контроль среды разработки и управление конфигурацией объекта оценки.

На уровне 4 добавляются полная спецификация интерфейсов, проекты нижнего уровня, анализ подмножества реализации, применение неформальной модели политики безопасности, независимый анализ уязвимых мест, автоматизация управления конфигурацией. Вероятно, это самый высокий уровень, которого можно достичь при существующей технологии программирования и приемлемых затратах.

Уровень 5, в дополнение к предыдущим, предусматривает применение формальной модели политики безопасности, полуформальной функциональной спецификации и проекта верхнего уровня с демонстрацией соответствия между ними. Необходимо проведение анализа скрытых каналов разработчиками и оценщиками.

На уровне 6 реализация должна быть представлена в структурированном виде. Анализ соответствия распространяется на проект нижнего уровня.

Оценочный уровень 7 (самый высокий) предусматривает формальную верификацию проекта объекта оценки. Он применим к ситуациям чрезвычайно высокого риска.

## 6. Основные этапы построения защищенной информационной системы

Цель мероприятий в области информационной безопасности – защитить интересы субъектов информационных отношений. Интересы эти многообразны, но все они концентрируются вокруг трех основных аспектов: доступность, целостность, конфиденциальность.

Важность проблематики информационной безопасности (ИБ) объясняется двумя основными причинами:

- ценностью накопленных информационных ресурсов;
- критической зависимостью от информационных технологий.

Разрушение важной информации, кража конфиденциальных данных, перерыв в работе вследствие отказа – все это выливается в крупные материальные потери, наносит ущерб репутации организации. Проблемы с системами управления или медицинскими системами угрожают здоровью и жизни людей.

Современные информационные системы сложны и, значит, опасны уже сами по себе, даже без учета активности злоумышленников. Постоянно обнаруживаются новые уязвимые места в программном обеспечении. Приходится принимать во внимание чрезвычайно широкий спектр аппаратного и программного обеспечения, многочисленные связи между компонентами.

Меняются принципы построения корпоративных информационных систем (ИС). Используются многочисленные внешние информационные сервисы; предоставляются вовне собственные.

Подтверждением сложности проблематики ИБ является параллельный (и довольно быстрый) рост затрат на защитные мероприятия и количества нарушений ИБ в сочетании с ростом среднего ущерба от каждого нарушения.

Успех в области информационной безопасности может принести только комплексный подход, сочетающий меры четырех уровней [10 – 12]:

- законодательного;
- административного;
- процедурного;
- программно-технического.

Бурное развитие глобальных сетей, привлекает все больше внимания к сети Internet со стороны частных лиц и различных организаций. Многие организации интегрируют свои сети в глобальную сеть, а также устанавливают свои серверы услуг (www-, FTP-) в глобальных сетях. Использование глобальных сетей в коммерческих целях, при передаче информации, содержащую коммерческую или государственную тайну, влечет за собой необходимость построения квалифицированной системы защиты информации.

При создании информационной инфраструктуры корпоративной автоматизированной системы на базе современных компьютерных сетей неизбежно возникает вопрос о защищенности этой структуры от угроз безопасности информации. Насколько адекватны реализованные в сети механизмы безопасности существующим рискам? Можно ли доверять этой системе обработку (хранение, передачу) конфиденциальной информации? И т.д. этот список велик.

Такими вопросами рано или поздно задаются все специалисты отделов защиты информации и других подразделений, отвечающих за эксплуатацию и сопровождение сетей. Ответы на эти вопросы далеко неочевидны. Анализ защищенности сети от угроз безопасности информации – работа сложная. Умение оценивать и управлять рисками, знание типовых угроз и уязвимостей, критериев и подходов к анализу защищенности, владение методами анализа, знание различных программно-аппаратных платформ, используемых в современных компьютерных сетях – все это далеко не полный перечень качеств, которыми должны обладать специалисты, проводящие работы по анализу защищенности сети. Анализ защищенности является фундаментом на базе, которого проводятся работы по построению защищенной информационной сети и аудиту (или проверке) безопасности этой сети в дальнейшем.

В первом разделе работы приведено достаточно подробное описание каждого уровня (законодательного, административного, процедурного, программно-технического) защиты информационных активов организации в отдельности. Раздел заканчивается примером построения автоматизированной сети предприятия на базе компьютерного оборудования, а также приводится возможная политика безопасности предприятия и список необходимых правил и инструкций для персонала организации.

Во втором разделе приводится классификация видов аудита безопасности и некоторые практические рекомендации по планированию и реализации авторизованного аудита, а также примеры активного аудита безопасности информационных активов организации.

Средства защиты информации делятся на формальные и неформальные. К первым относятся средства, выполняющие защитные функции строго по заранее предусмотренной процедуре и без непосредственного участия человека. К неформальным средствам отнесены такие, которые либо определяются целенаправленной деятельностью людей, либо регламентируют (непосредственно или косвенно) эту деятельность, рисунок 6.1.

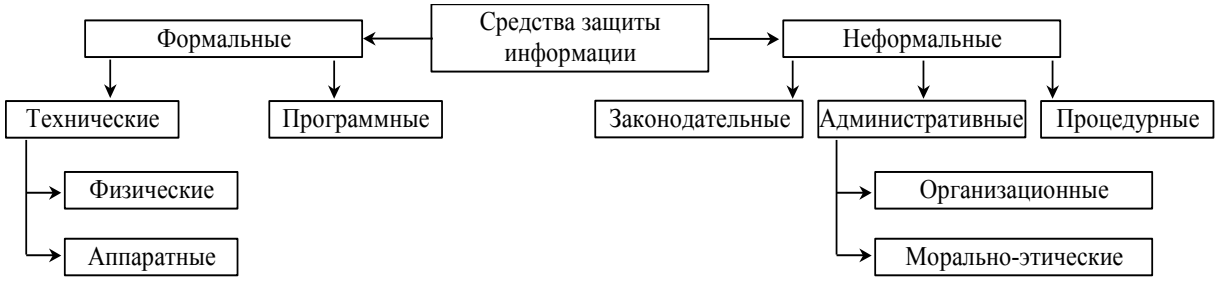



Рис. 6.1. Средства защиты информации

## 6.1. Законодательный уровень

### 6.1.1. Закон РФ «Об информации, информатизации и защите информации»

Федеральный закон от 20 февраля 1995 года № 24-ФЗ «Об информации, информатизации и защите информации» (далее «Закон об информации») является одним из основных базовых законов в области защиты информации, который регламентирует отношения, возникающие при формировании и использовании информационных ресурсов Российской Федерации на основе сбора, накопления, хранения, распространения и предоставления потребителям документированной информации, а также при создании и использовании информационных технологий, при защите информации и прав субъектов, участвующих в информационных процессах и информатизации.

Основными задачами системы защиты информации, нашедшими отражение в «Законе об информации», являются:

- предотвращение утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования, блокирования информации и т.п., вмешательства в информацию и информационные системы;

- сохранение полноты, достоверности, целостности информации, ее массивов и программ обработки данных, установленных собственником или уполномоченным им лицом;

- сохранение возможности управления процессом обработки, пользования информацией в соответствии с условиями, установленными собственником или владельцем информации;

- обеспечение конституционных прав граждан на сохранение личной тайны и конфиденциальности персональной информации, накапливаемой в банках данных;

сохранение секретности или конфиденциальности информации в соответствии с правилами, установленными действующим законодательством и другими законодательными или нормативными актами;

- соблюдение прав авторов программно-информационной продукции, используемой в информационных системах.

В частности статья 19 Закона устанавливает обязательность сертификации средств обработки и защиты документированной информации с ограниченным доступом, предназначенных для обслуживания граждан и организаций, а также обязательность получения лицензий для организаций, осуществляющих проектирование и производство средств защиты информации.

Статья 20 определяет основные цели защиты информации. В соответствии с этой статьей таковыми, в частности, являются:

- предотвращение утечки, хищения, утраты, искажения и подделки информации;
- предотвращение угроз безопасности личности, общества и государства;
- предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;
- защита конституционных прав на сохранение личной тайны и конфиденциальности персональных сведений;
- сохранение государственной тайны и конфиденциальности информации.

Пункт 3 статьи 21 возлагает контроль за соблюдением требований к защите информации, за эксплуатацией специальных средств защиты информации, а также обеспечение организационных мер защиты информационных систем, обрабатывающих информацию с ограниченным доступом в негосударственных структурах, на органы государственной власти. Это означает, что контроль состояния защиты должен охватывать все три составляющие информации с ограниченным доступом, входящей в государственные информационные ресурсы:

- информацию, составляющую государственную тайну;
- конфиденциальную информацию;
- персональные данные о гражданах.

Очень важна статья 22, которая определяет права и обязанности субъектов в области защиты информации. В частности, пункты 2 и 5 обязывают владельца информационной системы обеспечивать необходимый уровень защиты конфиденциальной информации и оповещать собственников информационных ресурсов о фактов нарушения режима защиты информации. Пунктом 3 риск, связанный с использованием не сертифицированных информационных систем и средств их обеспечения и защиты, возлагается на собственника (владельца) систем и средств. Риск, связанный с использованием информации, полученной из таких систем, относится на потребителя информации. Пункт 4 устанавливает право собственника документов или информационной системы обращаться в организации, осуществляющие сертификацию средств защиты таких систем, для проведения анализа достаточности мер защиты его ресурсов и систем и получения консультаций.

Статья 23 Закона посвящена защите прав субъектов в сфере информационных процессов и информатизации. Статья устанавливает, что защита прав субъектов в данной сфере осуществляется судом, арбитражным судом и третейскими судами, которые могут создаваться на постоянной или временной основе.

### 6.1.2. Закон РФ «О лицензировании отдельных видов деятельности»

Закон «О лицензировании отдельных видов деятельности» от 8 августа 2001 года номер 128-ФЗ (Принят Государственной Думой 13 июля 2001 года). Начнем с основных определений.

Статья 17 Закона устанавливает перечень видов деятельности, на осуществление которых требуются лицензии. Рассмотрим следующие виды:

- распространение шифровальных (криптографических) средств;
- техническое обслуживание шифровальных (криптографических) средств;
- предоставление услуг в области шифрования информации;
- разработка и производство шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных систем, телекоммуникационных систем;
- выдача сертификатов ключей электронных цифровых подписей, регистрация владельцев электронных цифровых подписей, оказание услуг, связанных с использованием электронных цифровых подписей и подтверждением подлинности электронных цифровых подписей;
- выявление электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
- разработка и (или) производство средств защиты конфиденциальной информации;
- техническая защита конфиденциальной информации;
- разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации, индивидуальными предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность.

Необходимо учитывать, что, согласно статье 1, действие данного Закона не распространяется на следующие виды деятельности:

- деятельность, связанная с защитой государственной тайны;
- деятельность в области связи;
- образовательная деятельность.

Основными лицензирующими органами в области защиты информации являются Федеральное агентство правительственной связи и информации (ФАПСИ) и Гостехкомиссия России. ФАПСИ ведает всем, что связано с криптографией, Гостехкомиссия лицензирует деятельность по защите конфиденциальной информации. Кроме того, ввоз и вывоз средств криптографической защиты информации (шифровальной техники) и нормативно-технической документации к ней может осуществляться исключительно на основании лицензии Министерства внешних экономических связей Российской Федерации, выдаваемой на основании решения ФАПСИ. Все эти вопросы регламентированы соответствующими указами Президента и постановлениями Правительства РФ.

### 6.1.3. Пакет руководящих документов Государственной технической комиссии при Президенте Российской Федерации

В 1992 году Государственная техническая комиссия при Президенте РФ опубликовала пять «Руководящих документов», посвященных проблеме защиты от несанкционированного доступа (НСД) к информации, обрабатываемой средствами вычислительной техники (СВТ) и автоматизированными системами (АС) [2]:

«Руководящий документ. Концепция защиты средств вычислительной техники (СВТ) и автоматизированных систем (АС) от несанкционированного доступа (НСД) к информации».- Гостехкомиссия России, 30 марта 1992 года.

«Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации».- Гостехкомиссия России, 30 марта 1992 года.

«Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».- Гостехкомиссия России, 30 марта 1992 года.

«Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД в автоматизированных системах и средствах вычислительной техники».- Гостехкомиссия России, 30 марта 1992 года.

«Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения».- Гостехкомиссия России, 30 марта 1992 года.

В 1997 году к этим документам добавился еще один [9]:

«Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации».

АС от НСД к информации

Центральным элементом (идейной основой) набора руководящих документов Гостехкомиссии является «Руководящий документ. Концепция защиты СВТ и АС от НСД к информации» [9]. В этом документе излагается система взглядов и основных принципов, которые закладываются в основу проблемы защиты информации от НСД, являющейся частью общей проблемы безопасности информации.

В «Концепции» различаются два понятия, соответствующие двум группам критериев безопасности:

- показатели защищенности средств вычислительной техники,
- критерии защищенности автоматизированных систем.

«Концепция» предусматривает существование двух относительно самостоятельных и имеющих отличие направлений в проблеме защиты информации от НСД. Это - направление, связанное с СВТ, и направление, связанное с АС. Отличие двух направлений порождено тем, что СВТ разрабатываются и поставляются на рынок лишь как элементы, из которых в дальнейшем строятся функционально ориентированные АС, и поэтому, не решая прикладных задач, СВТ не содержат пользовательской информации.

Помимо пользовательской информации при создании АС появляются такие отсутствующие при разработке СВТ характеристики АС, как полномочия пользователей, модель нарушителя, технология обработки информации.

Существуют различные способы покушения на информационную безопасность: радиотехнические, акустические, программные и т.п. Среди них НСД выделяется как доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых СВТ или АС. Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения СВТ или АС.

В разделе 3 «Концепции» формулируются основные принципы защиты от НСД к информации:

3.1. Защита СВТ и АС основывается на положениях и требованиях существующих законов, стандартов и нормативно-методических документов по защите от НСД к информации.

3.2. Защита СВТ обеспечивается комплексом программно-технических средств.

3.3. Защита АС обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер.

3.4. Защита АС должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.

3.5. Программно-технические средства защиты не должны существенно ухудшать основные функциональные характеристики АС (надежность, быстродействие, возможность изменения конфигурации АС).

3.6. Неотъемлемой частью работ по защите является оценка эффективности средств защиты, осуществляемая по методике, учитывающей всю совокупность технических характеристик оцениваемого объекта, включая технические решения и практическую реализацию средств защиты.

3.7. Защита АС должна предусматривать контроль эффективности средств защиты от НСД. Этот контроль может быть либо периодическим, либо инициироваться по мере необходимости пользователем АС или контролирующими органами.

В качестве главного средства защиты от НСД к информации в разделе 6 «Концепции» рассматривается система разграничения доступа (СРД) субъектов к объектам доступа:

6.1. Обеспечение защиты СВТ и АС осуществляется:

- СРД субъектов к объектам доступа;
- обеспечивающими средствами для СРД.

6.2. Основными функциями СРД являются:

- реализация правил разграничения доступа (ПРД) субъектов и их процессов к данным;
- реализация ПРД субъектов и их процессов к устройствам создания твердых копий;
- изоляция программ процесса, выполняемого в интересах субъекта, от других субъектов;
- управление потоками данных с целью предотвращения записи данных на носители несоответствующего грифа;
- реализация правил обмена данными между субъектами для АС и СВТ, построенных по сетевым принципам.

6.3. Обеспечивающие средства для СРД выполняют следующие функции:

- идентификацию и опознание (аутентификацию) субъектов и поддержание привязки субъекта к процессу, выполняемому для субъекта;
- регистрацию действий субъекта и его процесса; предоставление возможностей исключения и включения новых субъектов и объектов доступа, а также изменение полномочий субъектов;
- реакцию на попытки НСД, например, сигнализацию, блокировку, восстановление после НСД;
- тестирование;
- очистку оперативной памяти и рабочих областей на магнитных носителях после завершения работы пользователя с защищаемыми данными;
- учет выходных печатных и графических форм и твердых копий в АС;

- контроль целостности программной и информационной части как СРД, так и обеспечивающих ее средств.

6.4. Ресурсы, связанные как с СРД, так и с обеспечивающими ее средствами, включаются в объекты доступа.

6.5. Способы реализации СРД зависят от конкретных особенностей СВТ и АС. Возможно применение следующих способов защиты и любых их сочетаний:

- распределенная СРД и СРД, локализованная в программно-техническом комплексе (ядро защиты);

- СРД в рамках операционной системы, СУБД или прикладных программ;

- СРД в средствах реализации сетевых взаимодействий или на уровне приложений;

- использование криптографических преобразований или методов непосредственного контроля доступа;

- программная и (или) техническая реализация СРД.

В целом разработка Руководящих документов Гостехкомиссии России явилась следствием бурно развивающегося процесса внедрения новых информационных технологий. Документы достаточно оперативно заполнили правовой вакуум в области стандартов информационной безопасности в стране и на определенном этапе позволили решать актуальную задачу обеспечения безопасности информации. Поскольку разработка документов такого рода для России представляет достаточно новую область деятельности, можно рассматривать их как первую стадию формирования отечественных стандартов в области информационной безопасности.

На разработку этих документов большое влияние оказала «Оранжевая книга» Министерства обороны США, которое выразилось в ориентации на системы военного и специального применения, в использовании единой универсальной шкалы степени защищенности и в игнорировании вопросов ценности и времени жизни информации.

К недостаткам документов, помимо отсутствия требований к защите от угроз работоспособности, относится ориентация только на противодействие НСД и отсутствие требований к адекватности реализации политики безопасности. Собственно «политика безопасности» трактуется в этих документах исключительно как поддержание режима секретности и отсутствие НСД. Из-за этого средства защиты ориентируются на противодействие только внешним угрозам, а к структуре самой системы и ее функционированию не предъявляется никаких требований.

С точки зрения разработчиков данных руководящих документов основная и едва ли не единственная задача средств обеспечения безопасности – это обеспечение защиты от несанкционированного доступа к информации. Если средствам контроля и обеспечения целостности информации в них еще уделяется некоторое внимание, то поддержка

работоспособности систем обработки информации (как мера защиты от угроз работоспособности) вообще не упоминается. Определенный уклон в сторону поддержания секретности объясняется тем, что эти документы были разработаны в расчете на применение в существующих информационных системах Министерства обороны и спецслужб России, а также недостаточно высоким уровнем технологий этих систем.

**Документы Гостехкомиссии России о модели нарушителя в АС**

Модель нарушителя определяется в 4-м разделе основного Руководящего документа Гостехкомиссии России «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации» [2].

В качестве *нарушителя* в этом документе рассматривается субъект, имеющий доступ к работе с штатными средствами АС и СВТ как части АС.

Нарушители классифицируются по уровню возможностей, предоставляемых им штатными средствами АС и СВТ. Выделяется четыре уровня этих возможностей. Классификация является иерархической, т.е. каждый следующий уровень включает в себя функциональные возможности предыдущего.

*Первый уровень* определяет самый низкий уровень возможностей ведения диалога в АС – запуск задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации.

*Второй уровень* определяется возможностью создания и запуска собственных программ с новыми функциями по обработке информации.

*Третий уровень* определяется возможностью управления функционированием АС, т.е. воздействием на базовое программное обеспечение системы и на состав и конфигурацию ее оборудования.

*Четвертый уровень* определяется всем объемом возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств АС, вплоть до включения в состав СВТ собственных технических средств с новыми функциями по обработке информации.

Подчеркивается, что в своем уровне нарушитель является специалистом высшей квалификации, знает все о АС и, в частности, о системе и средствах ее защиты.

**Классификация защищенности СВТ. Классификация защищенности АС**

Руководящие документы Гостехкомиссии России «Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации» [2] и «Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» [2] определяют основные показатели защищенности по классам средств

вычислительной техники (Таблица 6.1) и требования к классам защищенности автоматизированных систем (Таблица 6.2).

Таблица 6.1 – Распределение показателей защищенности по классам средств вычислительной техники

| Наименование показателя | Класс защищенности | | | | | |
|---|---|---|---|---|---|---|
| | 6 | 5 | 4 | 3 | 2 | 1 |
| Дискреционный принцип контроля доступа | + | + | + | = | + | = |
| Мандатный принцип контроля доступа | - | - | + | = | = | = |
| Очистка памяти | - | + | + | + | = | = |
| Изоляция модулей | - | - | + | = | + | = |
| Маркировка документов | - | - | + | = | = | = |
| Защита ввода и вывода на отчужденный носитель информации | - | - | + | = | = | = |
| Сопоставление пользователя с устройством | - | - | + | = | = | = |
| Идентификация и аутентификация | + | = | + | = | = | = |
| Гарантии проектирования | - | + | + | + | + | + |
| Регистрация | - | + | + | + | = | = |
| Взаимодействие пользователя с КСЗ | - | - | - | + | = | = |
| Надежное восстановление | - | - | - | + | = | = |
| Целостность КСЗ | - | + | + | + | = | = |
| Контроль модификации | - | - | - | - | + | = |
| Контроль дистрибуции | - | - | - | - | + | = |
| Гарантии архитектуры | - | - | - | - | - | + |
| Тестирование | + | + | + | + | + | = |
| Руководство пользователя | + | = | = | = | = | = |
| Руководство по КСЗ | + | + | = | + | + | = |
| Тестовая документация | + | + | + | + | + | = |
| Конструкторская (проектная) документация | + | + | + | + | + | + |

Обозначения:

« - » - нет требований к данному классу

« + » - новые или дополнительные требования

« = » - требования совпадают с требованиями к СВТ предыдущего класса

Седьмой класс присваивается средствам вычислительной техники, к которым предъявлялись требования по защите от несанкционированного доступа к информации, но при оценке защищенность средства оказалась ниже уровня требований шестого класса.

Таблица 6.2 – Требования к классам защищенности автоматизированных систем

| Подсистемы и требования | Классы | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | Б | А | Б | А | Д | Г | В | Б | А |
| I. Подсистема управления доступом | | | | | | | | | |
| Идентификация, проверка подлинности и контроль доступа субъектов: | | | | | | | | | |
| В систему | | | | | | | | | |
| к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ | | | | | | | | | |
| к программам | | | | | | | | | |
| к томам, каталогам, файлам, записям, полям записей | | | | | | | | | |
| Управление потоками информации | | | | | | | | | |
| II. Подсистема регистрации и учета | | | | | | | | | |
| Регистрация и учет | | | | | | | | | |
| входа/выхода субъектов доступа в/из системы (узла сети) | | | | | | | | | |
| выдачи печатных (графических) выходных документов | | | | | | | | | |
| запуска/завершения программ и процессов (заданий, задач) | | | | | | | | | |
| доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям | | | | | | | | | |

| Подсистемы и требования | Классы | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | Б | А | Б | А | Д | Г | В | Б | А |
| и каналам связи | | | | | | | | | |
| доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей | | | | | | | | | |
| изменения полномочий субъектов доступа | | | | | | | | | |
| создаваемых защищаемых объектов доступа | | | | | | | | | |
| Учет носителей информации | | | | | | | | | |
| Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей | | | | | | | | | |
| Сигнализация попыток нарушения защиты | | | | | | | | | |
| III. Криптографическая подсистема | | | | | | | | | |
| Шифрование конфиденциальной информации | | | | | | | | | |
| Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах | | | | | | | | | |
| Использование аттестованных (сертифицированных) криптографических средств | | | | | | | | | |
| IV. Подсистема обеспечения целостности | | | | | | | | | |
| Обеспечение целостности программных средств и обрабатываемой информации | | | | | | | | | |
| Физическая охрана средств | | | | | | | | | |

| Подсистемы и требования | Классы | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | Б | А | Б | А | Д | Г | В | Б | А |
| вычислительной техники и носителей информации | | | | | | | | | |
| Наличие администратора (службы) защиты информации в АС | | | | | | | | | |
| Периодическое тестирование СЗИ НСД | | | | | | | | | |
| Наличие средств восстановления СЗИ НСД | | | | | | | | | |
| Использование сертифицированных средств защиты | | | | | | | | | |

Обозначения:

« + » - требование к данному классу присутствует.

**Показатели защищенности МЭ**

В руководящем документе Гостехкомиссии России [9]: «Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» устанавливается классификация межсетевых экранов (МЭ) по уровня защищенности от НСД к информации на базе перечня показателей защищенности и совокупности описывающих их требований.

Под сетями ЭВМ, распределенными АС, в данном документе понимаются соединенные каналами связи системы обработки данных, ориентированные на конкретного пользователя.

МЭ представляет собой локальное (однокомпонентное) или функционально - распределенное средство (комплекс), реализующее контроль за информацией, поступающей в АС и/или выходящей из АС, и обеспечивает защиту АС посредством фильтрации информации, т.е. ее анализа по совокупности критериев и принятия решения о ее распространении в (из) АС.

Руководящий документ разработан в дополнение к Руководящим документам Гостехкомиссии России «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» и «Автоматизированные системы. Защита от

несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».

Документ предназначен для заказчиков и разработчиков МЭ, а также сетей ЭВМ, распределенных автоматизированных систем с целью использования при формулировании и реализации требований по их защите от НСД к информации.

**Общие положения**

Данные показатели содержат требования к средствам защиты, обеспечивающим безопасное взаимодействие сетей ЭВМ, АС посредством управления межсетевыми потоками информации и реализованных в виде МЭ.

Показатели защищенности применяются к МЭ для определения уровня защищенности, который они обеспечивают при межсетевом взаимодействии.

Конкретные перечни показателей определяют классы защищенности МЭ.

Деление МЭ на соответствующие классы по уровням контроля межсетевых информационных потоков с точки зрения защиты информации необходимо в целях разработки и применения обоснованных и экономически оправданных мер по достижению требуемого уровня защиты информации при взаимодействии ЭВМ, АС. Дифференциация подхода к выбору функций защиты в МЭ определяется АС, для защиты которой применяется данный экран.

Устанавливается пять классов защищенности МЭ. Каждый класс характеризуется определенной минимальной совокупностью требований по защите информации.

Самый низкий класс защищенности – пятый, применяемый для безопасного взаимодействия АС класса 1Д с внешней средой, четвертый – для 1Г, третий – 1В, второй – 1Б, самый высокий – первый, применяемый для безопасного взаимодействия АС класса 1А с внешней средой

Требования, предъявляемые к МЭ, не исключают требований, не исключают требований, предъявляемых к СВТ и АС в соответствии с руководящими документами Гостехкомиссии России «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» и «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».

При включении МЭ в АС определенного класса защищенности, класс защищенности совокупной АС, полученной из исходной путем добавления в нее МЭ, не должен понижаться. Для АС класса 3Б, 2Б должны применяться МЭ не ниже 5 класса. Для АС класса 3А, 2А в зависимости от важности обрабатываемой информации должны применяться МЭ следующих классов:

- при обработке информации с грифом «секретно» - не ниже 3 класса;

- при обработке информации с грифом «совершенно секретно» - не ниже 2 класса;

- при обработке информации с грифом «особой важности» - не ниже 1 класса.

Таким образом, фактически, обмен информацией, составляющей государственную тайну, между автоматизированными системами классов 1Д – 1А или при наличии такой системы только на одном конце, данным документом не предусмотрен.

**Перечень показателей по классам защищенности МЭ**

Таблица 6.3.

| Показатели защищенности | Классы защищенности | | | | |
|---|---|---|---|---|---|
| | 5 | 4 | 3 | 2 | 1 |
| Управление доступом (фильтрация данных и трансляция адресов) | + | + | + | + | = |
| Идентификация и аутентификация | - | - | + | = | + |
| Регистрация | - | + | + | + | = |
| Администрирование: идентификация и аутентификация | + | = | + | + | + |
| Администрирование: регистрация | + | + | + | = | = |
| Администрирование: простота использования | - | - | + | = | + |
| Целостность | + | = | + | + | + |
| Восстановление | + | = | = | + | = |
| Тестирование | + | + | + | + | + |
| Руководство администратора защиты | + | = | = | = | = |
| Тестовая документация | + | + | + | + | + |
| Конструкторская (проектная) документация | + | = | + | = | + |

Обозначения:

« - » - нет требований к данному классу;

« + » - новые или дополнительные требования;

« = » - требования совпадают с требованиями к МЭ предыдущего класса

### 6.2. Административный уровень

К *административному уровню* информационной безопасности относятся действия общего характера, предпринимаемые руководством организации. Административный уровень является основой практического построения интегрированной

системы, определяющей генеральное направление работ по обеспечению безопасности информации (ОБИ).

Целью административного уровня является разработка программы работ в области информационной безопасности и обеспечение ее выполнения. Программа представляет официальную политику безопасности, отражающую собственный концептуальный подход организации к ОБИ. Конкретизация политики безопасности выражается в планах по информационной защите АС.

Практические мероприятия по созданию системы ОБИ, включают следующие этапы:

- Разработка политики безопасности.
- Проведение анализа рисков.
- Планирование обеспечения информационной безопасности.
- Планирование действий в чрезвычайных ситуациях.
- Подбор механизмов и средств обеспечения информационной безопасности.
- Собственно первые два этапа обычно трактуются как выработка политики безопасности и составляют административный уровень системы ОБИ предприятия.
- Третий и четвертый этапы заключаются в разработке процедур безопасности, на этих этапах формируется уровень планирования системы ОБИ, этот уровень так же можно назвать *процедурным*.

На последнем этапе практических мероприятий определяется *программно-технический* уровень системы ОБИ.

### 6.2.1. Политика безопасности

В «Оранжевой книге» *политика безопасности* трактуется как набор норм, правил и практических приемов, которые регулируют управление, защиту и распределение ценной информации. На практике политика безопасности (ПБ) трактуется несколько шире — как совокупность документированных административных решений, направленных на обеспечение безопасности информационного ресурса. Результатом политики является высокоуровневый документ, представляющий систематизированное изложение целей, задач, принципов и способов достижения информационной безопасности.

Данный документ представляет методологическую основу практических мер (процедур) по реализации ОБИ и содержит следующие группы сведений.

- Основные положения информационной безопасности.
- Область применения.
- Цели и задачи обеспечения информационной безопасности.
- Распределение ролей и ответственности.
- Общие обязанности.

Основные положения определяют важность ОБИ, общие проблемы безопасности, направления их решения, роль сотрудников, нормативно-правовые основы.

Областью применения политики безопасности являются основные активы и подсистемы АС, подлежащие защите. Типовыми активами являются программно-аппаратное и информационное обеспечение АС, персонал, в отдельных случаях информационная инфраструктура предприятия.

Цели, задачи, критерии ОБИ вытекают из функционального назначения предприятия. Например, для режимных организаций на первое место ставится соблюдение конфиденциальности. Для сервисных информационных служб реального времени важным является обеспечение доступности (оперативной готовности) подсистем. Для информационных хранилищ актуальным может быть обеспечение целостности данных и т.д. Здесь указываются законы и правила организации, которые следует учитывать при проведении работ по ОБИ.

Типовыми целями могут быть следующие:

- обеспечение уровня безопасности, соответствующего нормативным документам предприятия;
- следование экономической целесообразности в выборе защитных мер;
- обеспечение соответствующего уровня безопасности в конкретных функциональных областях АС;
- обеспечение подотчетности всех действий пользователей с информационными ресурсами и анализа регистрационной информации и др.

Если предприятие не является изолированным, цели и задачи рассматриваются в более широком контексте: должны быть оговорены вопросы безопасного взаимного влияния локальных и удаленных подсистем.

В рассматриваемом документе могут быть конкретизированы некоторые стратегические принципы безопасности (вытекающие из целей и задач ОБИ). Таковыми являются стратегии действий в случае нарушения политики безопасности предприятия и сторонних организаций, взаимодействия с внешними организациями, правоохранительными органами, прессой и др. В качестве примера можно привести две стратегии ответных действий на нарушение безопасности:

- «выследить и осудить», когда злоумышленнику позволяют продолжить действия с целью его компрометации и наказания (данную стратегию одобряют правоохранительные органы!);
- «защититься и продолжить», когда организация опасается за уязвимость информационных ресурсов и оказывает максимальное противодействие нарушению.

Политика безопасности затрагивает всех пользователей компьютеров в организации. Поэтому важно решить так называемые политические вопросы наделения всех категорий пользователей соответствующими правами, привилегиями и обязанностями.

Для этого определяется круг лиц, имеющий доступ к подсистемам и сервисам АС. Для каждой категории пользователей описываются правильные и неправильные способы использования ресурсов — что запрещено и разрешено. Здесь специфицируются уровни и регламентация доступа различных групп пользователей. Следует указать какое из правил умолчания на использование ресурсов принято в организации, а именно:

- что явно не запрещено, то разрешено или
- что явно не разрешено, то запрещено.

Одним из самых уязвимых мест в ОБИ является распределение прав доступа. В политике безопасности должна быть утверждена схема управления распределением прав доступа к сервисам — централизованная или децентрализованная, или иная. Должно быть четко определено, кто распоряжается правами доступа к сервисам и какими именно правами. Целесообразно детально описать практические процедуры наделения пользователей правами. Здесь следует указать должностных лиц, имеющих административные привилегии и пароли для определенных сервисов.

Права и обязанности пользователей определяются применительно к безопасному использованию подсистем и сервисов АС. При определении прав и обязанностей администраторов следует стремиться к некоторому балансу между правом пользователей на тайну и обязанностью администратора контролировать нарушения безопасности.

Важным элементом политики является распределение ответственности. Политика не может предусмотреть всего, однако она должна для каждого вида проблем найти ответственного.

Обычно выделяется несколько уровней ответственности. На первом уровне каждый пользователь обязан работать в соответствии с политикой безопасности (защищать свой счет), подчиняться распоряжениям лиц, отвечающих за отдельные аспекты безопасности, ставить в известность руководство обо всех подозрительных ситуациях. Системные администраторы отвечают за защиту соответствующих информационно-вычислительных подсистем. Администраторы сетей должны обеспечивать реализацию организационно-технических мер, необходимых для проведения в жизнь политики безопасности АС. Более высокий уровень - руководители подразделений отвечают за доведение и контроль положений политики безопасности.

С практической точки зрения, политику безопасности целесообразно разделить на несколько уровней (как правило, выделяют два-три уровня).

*Верхний уровень* носит общий характер и определяет политику организации в целом. Здесь основное вниманию уделяется: порядку создания и пересмотра политики безопасности; целям, преследуемым организацией в области информационной безопасности; вопросам выделения и распределения ресурсов; принципам технической политики в области выбора методов и средств защиты информации; координированию мер безопасности; стратегическому планированию и контролю; внешним взаимодействиям и другим вопросам, имеющим общеорганизационный характер.

На указанном уровне формулируются главные цели в области информационной безопасности (определяемые сферой деятельности предприятия): обеспечение конфиденциальности, целостности и/или доступности [2].Вообще говоря, на верхний уровень следует выносить минимум вопросов. Подобное вынесение целесообразно, когда оно сулит значительную экономию средств или когда иначе поступить просто невозможно.

*Средний уровень* политики безопасности выделяют в случае структурной сложности организации либо при необходимости обозначить специфичные подсистемы организации. Это касается отношения к перспективным, еще не достаточно апробированным технологиям. Например, использование новых сервисов Internet, организация связи и обработка информации на домашних и портативных компьютерах, степень соблюдения положений компьютерного права и др. Кроме того, на среднем уровне политики безопасности могут быть выделены особо значимые контуры АС организации, например, обрабатывающие секретную или критично важную информацию. Т.е. к среднему уровню можно отнести вопросы, касающиеся отдельных аспектов информационной безопасности, но важные для различных эксплуатируемых организацией систем.

Политика среднего уровня должна для каждого аспекта освещать следующие темы:

*Описание аспекта*. Например, если рассмотреть применение пользователями неофициального программного обеспечения (ПО), последнее можно определить как ПО, которое не было одобрено и/или закуплено на уровне организации.

*Область применения*. Следует определить, где, когда, как, по отношению к кому и чему применяется данная политика безопасности.

*Позиция организации по данному аспекту*. Продолжая пример с неофициальным ПО, можно представить себе позиции полного запрета, выработки процедуры приемки подобного ПО и т.п. Позиция может быть сформулирована и в гораздо более общем виде, как набор целей, которые преследует организация в данном аспекте.

*Роли и обязанности.* В «политический» документ необходимо включить информацию о должностных лицах, ответственных за реализацию политики безопасности. Например, если для использования неофициального ПО сотрудникам требуется разрешение

руководства, должно быть известно, у кого и как его можно получить. Если неофициальное ПО использовать нельзя, следует знать, кто следит за выполнением данного правила.

*Законопослушность*. Политика должна содержать общее описание запрещенных действий и наказаний за них.

*Точки контакта.* Должно быть известно, куда следует обращаться за разъяснениями, помощью и дополнительной информацией. Обычно «точкой контакта» служит определенное должностное лицо, а не конкретный человек, занимающий в данный момент данный пост.

За разработку и реализацию политики безопасности верхнего и среднего уровней отвечают руководитель службы безопасности, администраторы безопасности АС, администратор корпоративной сети.

*Нижний уровень* политики безопасности относится к конкретным службам или подразделениям организации и детализирует верхние уровни политики безопасности. Данный уровень необходим, когда вопросы безопасности конкретных подсистем требуют решения на управленческом, а не только на техническом уровне.

Понятно, что на данном уровне определяются конкретные цели, частные критерии и показатели информационной безопасности, определяются права конкретных групп пользователей, формулируются соответствующие условия доступа к информации и т.п. Здесь из конкретных целей выводятся (обычно формальные) *правила безопасности*, описывающие, кто, что и при каких условиях может делать или не может. Более детальные и формальные правила упростят внедрения системы и настройку средств ОБИ.

На этом уровне описываются механизмы защиты информации и используемые программно-технические средства для их реализации (в рамках, конечно, управленческого уровня, но не технического).

За политику безопасности нижнего уровня отвечают системные администраторы.

Британский стандарт BS 7799:1995 рекомендует включать в документ, характеризующий политику безопасности организации, следующие разделы:

- вводный раздел, подтверждающий озабоченность высшего руководства проблемами информационной безопасности;

- организационный раздел, содержащий описание подразделений, комиссий, групп и т.д., отвечающих за работы в области информационной безопасности;

- классификационный, описывающий имеющиеся в организации материальные и информационные ресурсы и необходимый уровень их защиты;

- штатный, характеризующий меры безопасности, применяемые к персоналу (описание должностей с точки зрения информационной безопасности, организация обучения и

переподготовки персонала, порядок реагирования на нарушения режима безопасности и т.п.);

- раздел, освещающий вопросы физической защиты;

управляющий раздел, описывающий подход к управлению компьютерами и компьютерными сетями;

- раздел, описывающий правила разграничения доступа к производственной информации;

- раздел, характеризующий порядок разработки и сопровождения систем;

- раздел, описывающий меры, направленные на обеспечение непрерывной работы организации;

- юридический раздел, подтверждающий соответствие политики безопасности действующему законодательству.

В рамках разработки политики безопасности проводится анализ рисков. Это делается с целью минимизации затрат на ОБИ. Основной принцип безопасности: затраты на средства защиты не должны превышать стоимости защищаемых объектов. При этом если ПБ оформляется в виде высокоуровневого документа, описывающего общую стратегию, то анализ рисков (как приложение) оформляется в виде списка активов, нуждающихся в защите.

### 6.2.2. Анализ рисков

*Управление рисками* (или их анализ) рассматривается на административном уровне ИБ, поскольку только руководство организации способно выделить необходимые ресурсы, инициировать и контролировать выполнение соответствующих программ.

Управление рисками и выработка собственной ПБ, актуально только для тех организаций, информационные системы которых и/или обрабатываемые данные можно считать нестандартными. Обычную организацию вполне устроит типовой набор защитных мер, выбранный на основе представления о типичных рисках или вообще без всякого анализа рисков (особенно это верно с формальной точки зрения, в свете проанализированного нами ранее российского законодательства в области ИБ). Можно провести аналогию между индивидуальным строительством и получением квартиры в районе массовой застройки. В первом случае необходимо принять множество решений, оформить большое количество бумаг, во втором достаточно определиться лишь с несколькими параметрами.

Использование информационных систем связано с определенной совокупностью рисков. Когда возможный ущерб неприемлемо велик, необходимо принять экономически оправданные меры защиты. Периодическая *оценка рисков* необходима для контроля эффективности деятельности в области безопасности и для учета изменений обстановки.

С количественной точки зрения уровень риска является функцией вероятности реализации определенной угрозы (использующей некоторые уязвимые места), а также величины возможного ущерба.

Таким образом, суть мероприятий по управлению рисками состоит в том, чтобы оценить их размер, выработать эффективные и экономичные меры снижения рисков, а затем убедиться, что риски заключены в приемлемые рамки (и остаются таковыми). Следовательно, управление рисками включает в себя два вида деятельности, которые чередуются циклически:

- оценка рисков;
- выбор эффективных и экономичных защитных средств (нейтрализация рисков).

По отношению к выявленным рискам возможны следующие действия:

- ликвидация риска;
- уменьшение риска (за счет использования дополнительных защитных средств);
- принятие риска (и выработка плана действия в соответствующих условиях);
- переадресация риска (например, путем заключения страхового соглашения).

Процесс управления рисками можно разделить на несколько этапов, рисунок 6.2.

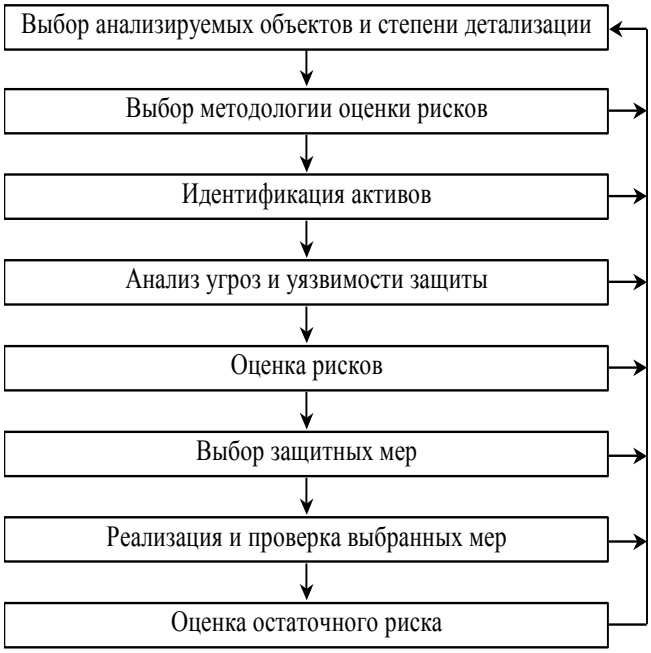



Рис. 6.2. Алгоритм анализа рисков

Два последних этапа (реализация и проверка выбранных мер, оценка остаточного риска) относятся к выбору защитных средств (нейтрализации рисков), остальные – к оценке рисков. Уже перечисление этапов показывает, что управление рисками – процесс циклический. По существу, последний этап – это оператор конца цикла, предписывающий вернуться к началу. Риски нужно контролировать постоянно, периодически проводя их

переоценку. Отметим, что добросовестно выполненная и тщательно документированная первая оценка может существенно упростить последующую деятельность.

**Предварительный этап анализа риска**

На начальном этапе методом экспертной оценки решаются общие вопросы проведения анализа риска. Первым делом выбираются компоненты АС и степень детальности их рассмотрения. Всеобъемлющий анализ требует рассмотрения всей информационной инфраструктуры. Но на практике из принципа разумной достаточности могут быть выделены и подвергнуты большей детализации отдельные наиболее важные компоненты и службы, в первую очередь, где риски велики или неизвестны. Более тщательному анализу подвергаются новые и модифицированные компоненты АС, а также компоненты, где имели место новые инциденты и нарушения безопасности.

Далее выбираются методологии оценки рисков как процесса получения количественной или качественной оценки ущерба, который может произойти в случае реализации угроз безопасности АС. Методологии носят частный характер, присущий организации и АС, и зависят от конкретного множества дестабилизирующих факторов и условий функционирования АС, возможности их количественной оценки, степени их неточности, неполноты, нечеткости и т.д. На практике, с учетом допустимой приближенной оценки рисков, часто используют простые наглядные методы, основанные на элементах теории вероятности и математической статистики.

**Идентификация активов**

Основу процесса анализа риска составляет определение: что надо защищать, от кого и как. Для этого выявляются активы (компоненты АС), нуждающиеся в защите. Ниже представлены основные категории активов АС предприятия.

Аппаратное обеспечение (компьютеры, периферийные устройства, коммуникационные линии, сетевое оборудование и их составные части).

Программное обеспечение (исходные, объектные и загрузочные модули операционных систем, вспомогательных системных и коммуникационных программ, инструментальных средств разработки, прикладных программных пакетов).

Информационное обеспечение (вводимые и обрабатываемые, хранимые, передаваемые и резервные (сохранные копии) данные и метаданные).

Персонал (обслуживающий персонал и пользователи).

Документация (конструкторская, техническая, пользовательская и иная документация).

Расходные материалы (бумага, магнитные носители, картриджи и т.д.).

В некоторых специфичных АС активы, уникальные для организации, могут быть выделены в отдельные группы, например: коммуникационное, алгоритмическое или

лингвистическое обеспечение. Кроме того, могут подлежать защите части инфраструктуры, в частности подсистемы электроснабжения и др.

Главным результатом процесса идентификации активов является получение детальной информационной структуры организации и способов использования информации. Дальнейшие этапы анализа риска основываются именно на данной, зафиксированной на некоторый момент времени, информации.

**Анализ угроз**

После идентификации активов АС следует рассмотреть все возможные угрозы указанным активам, оценить риски и ранжировать их по степени возможного ущерба.

Под *угрозой* обычно понимают любое событие (действие), которое потенциально может нанести ущерб АС путем нарушения нарушению конфиденциальности, целостности или доступности информации. Угрозы могут быть преднамеренными, являющимися следствием умышленных (злонамеренных) действий людей, и непреднамеренные, вызванные ошибками человека или сбоями и отказами работы технических и программных средств, или стихийными действиями. В настоящее время существует огромное количество угроз, способных привести к нарушению конфиденциальности, целостности и доступности информации.

При анализе угроз необходимо выявить их источники и условия реализации. Это поможет в выборе дополнительных средств защиты. Часто одни угрозы могут быть следствием или условием проявления ряда других угроз. Например, несанкционированный доступ (в различных формах его проявления) к ресурсам облегчает реализацию практически любой угрозы: от порчи магнитного носителя до комплексной удаленной атаки.

**Оценка рисков**

После идентификации угрозы необходимо оценить риск проявления угрозы. В большинстве случаев возможно получить количественную оценку риска. Она может быть получена на базе экспертного опроса, оценена статистически или рассчитана по некоторой математической зависимости (адекватной конкретной угрозе конкретному активу).

Кроме вероятности осуществления угрозы, важен размер ожидаемых потерь. В общем случае ожидаемые потери рассчитываются по следующей формуле:

$$E = P \cdot V, \qquad (6.1)$$

где P – вероятностная оценка риска проявления угрозы,

V – ущерб при реализации угрозы.

Однако, как вероятности угрозы, так и ожидаемые потери не всегда можно оценить количественно. Например, рассчитать замену компьютера достаточно просто, но трудно оценить потенциальный ущерб в случае задержки выдачи данных, искажения информации, разглашения отдельных сведений и т.д. Некоторые инциденты могут нанести

ущерб репутации фирмы, вызвать социальную напряженность в коллективе, повлечь юридическое преследование предприятия со стороны пользователей и т.д.

Существует несколько простых способов оценки вероятностей проявления угроз и возможных потерь:

- Экспертная оценка событий. Методы экспертных оценок применяются при оценке трудно предсказуемых угроз, например стихийных бедствий, и являются самыми неточными.

- Методика определения приемлемости уровня риска по трехбалльной шкале. Согласно методике, оцениваемым рискам и ущербам ставятся оценки по трехбалльной шкале: 1, 2, 3. Полученные два множества оценок рисков и ущербов перемножаются. Множество возможных значений будет следующим: 1, 2, 3, 4, 6, 9. Полагается, что первые два значения характеризуют низкий уровень риска, третий и четвертый – средний, два последних – высокий.

Методика определения приемлемости уровня риска с учетом видимости угроз и их последствий. Здесь вводится понятие видимости угрозы для внешнего мира – мера информации о системе, доступной злоумышленнику (и вызывающей нездоровый интерес). Согласно указанной методике, оцениваемым рискам, видимости, физическим ущербам и моральным ущербам ставятся оценки по трехбалльной шкале 1, 2, 3. Значения рисков умножаются на значения для видимости, а значения для физического ущерба умножаются на значения для морального ущерба. Затем полученные два числа складываются. Считается, что уровень риска низкий, если итоговое число меньше 7, высокий, если итоговое число больше 11, иначе – средний.

Статистическая оценка событий и использование статистических моделей (отражающих законы распределения конкретных типов угроз). Данный метод позволяет получить приемлемые результаты для оценки часто проявляемых регистрируемых угроз, например: сбоев и отказов вычислительного процесса.

Использование аналитических моделей (возможно в виде таблиц) потенциального ущерба в зависимости от заранее определенных коэффициентов.

Следует оговориться, что методы анализа риска обычно не отличаются высокой точностью. Дело в том, что основная задача анализа риска (как инструмента планирования) оценить уровень возможных потерь и уровень затрат на защиту. Для практики, когда разнородные исходные данные имеют приближенный или субъективный характер оценки, высокая точность расчета и не требуется. Иногда вообще невозможно оценить точность результата.

**Выбор и проверка защитных мер**

Для уменьшения размера ущерба необходим выбор соответствующих мер защиты: организационных, физических, программно-технических и др. Каждая угроза может быть предотвращена различными способами. Поэтому на данном этапе решается задача анализа и синтеза мер, методов и средств защиты по критерию эффективность/стоимость с учетом, конечно, технической политики организации и других жизненно важных характеристик АС.

После выбора способов защиты АС производится проверка их эффективности. Если остаточные риски стали опять-таки неприемлемы, весьма разумно повторить этапы анализа риска.

Завершая подраздел, следует отметить, что разработка политики безопасности и проведение анализа риска являются кропотливыми научно-техническими задачами. Поэтому важно правильно подобрать коллектив разработчиков. Обычно этим профессионально занимается группа информационной безопасности предприятия. Однако возможно привлечение администраторов и разработчиков систем и сетей, специалистов по аудиту и управлению, психологов, представителей службы режима.

### 6.3. Процедурный уровень

#### 6.3.1. Основные классы мер процедурного уровня

Эти меры безопасности ориентированы на людей. Именно люди формируют режим информационной безопасности, и они же оказываются главной угрозой, поэтому «человеческий фактор» заслуживает особого внимания.

В российских компаниях накоплен богатый опыт регламентирования и реализации процедурных (организационных) мер, однако дело в том, что они пришли из «докомпьютерного» прошлого, поэтому требуют переоценки.

Следует осознать ту степень зависимости от компьютерной обработки данных, в которую попало современное общество. Без всякого преувеличения можно сказать, что необходима информационная гражданская оборона. Спокойно, без нагнетания страстей, нужно разъяснять обществу не только преимущества, но и опасности, связанные с использованием информационных технологий. Акцент следует делать не на военной или криминальной стороне дела, а на гражданских аспектах, связанных с поддержанием нормального функционирования аппаратного и программного обеспечения, то есть концентрироваться на вопросах доступности и целостности данных.

На процедурном уровне можно выделить следующие классы мер:

- управление персоналом;
- физическая защита;
- поддержание работоспособности;
- реагирование на нарушения режима безопасности;

- планирование восстановительных работ.

**Управление персоналом**

Управление персоналом начинается с приема нового сотрудника на работу и даже раньше – с составления описания должности. Уже на данном этапе желательно подключить к работе специалиста по информационной безопасности для определения компьютерных привилегий, ассоциируемых с должностью. Существует два общих принципа, которые следует иметь в виду:

- разделение обязанностей;
- минимизация привилегий.

*Принцип разделения обязанностей* предписывает так распределять роли и ответственность, чтобы один человек не мог нарушить критически важный для организации процесс. Например, нежелательна ситуация, когда крупные платежи от имени организации выполняет один человек. Надежнее поручить одному сотруднику оформление заявок на подобные платежи, а другому – заверять эти заявки. Другой пример – процедурные ограничения действий суперпользователя. Можно искусственно «расщепить» пароль суперпользователя, сообщив первую его часть одному сотруднику, а вторую – другому. Тогда критически важные действия по администрированию ИС они смогут выполнить только вдвоем, что снижает вероятность ошибок и злоупотреблений.

*Принцип минимизации привилегий* предписывает выделять пользователям только те права доступа, которые необходимы им для выполнения служебных обязанностей. Назначение этого принципа очевидно – уменьшить ущерб от случайных или умышленных некорректных действий.

Предварительное составление описания должности позволяет оценить ее критичность и спланировать процедуру проверки и отбора кандидатов. Чем ответственнее должность, тем тщательнее нужно проверять кандидатов: навести о них справки, быть может, побеседовать с бывшими сослуживцами и т.д. Подобная процедура может быть длительной и дорогой, поэтому нет смысла дополнительно усложнять ее. В то же время, неразумно и совсем отказываться от предварительной проверки, чтобы случайно не принять на работу человека с уголовным прошлым или психическим заболеванием. Когда кандидат определен, он, вероятно, должен пройти обучение; по крайней мере, его следует подробно ознакомить со служебными обязанностями, а также с нормами и процедурами информационной безопасности. Желательно, чтобы меры безопасности были им усвоены до вступления в должность и до заведения его системного счета с входным именем, паролем и привилегиями.

С момента заведения системного счета начинается его администрирование, а также протоколирование и анализ действий пользователя. Постепенно изменяется

окружение, в котором работает пользователь, его служебные обязанности и т.п. Все это требует соответствующего изменения привилегий. Техническую сложность представляют временные перемещения пользователя, выполнение им обязанностей взамен сотрудника, ушедшего в отпуск, и иные обстоятельства, когда полномочия нужно сначала предоставить, а через некоторое время взять обратно. В такие периоды профиль активности пользователя резко меняется, что создает трудности при выявлении подозрительных ситуаций. Определенную аккуратность следует соблюдать и при выдаче новых постоянных полномочий, не забывая ликвидировать старые права доступа.

Ликвидация системного счета пользователя, особенно в случае конфликта между сотрудником и организацией, должна производиться максимально оперативно (в идеале – одновременно с извещением о наказании или увольнении). Возможно и физическое ограничение доступа к рабочему месту. Разумеется, если сотрудник увольняется, у него нужно принять все его компьютерное хозяйство и, в частности, криптографические ключи, если использовались средства шифрования.

К управлению сотрудниками примыкает администрирование лиц, работающих по контракту (например, специалистов фирмы-поставщика, помогающих запустить новую систему). В соответствии с принципом минимизации привилегий, им нужно выделить ровно столько прав, сколько необходимо, и изъять эти права сразу по окончании контракта. Проблема, однако, состоит в том, что на начальном этапе внедрения «внешние» сотрудники будут администрировать «местных», а не наоборот. Здесь на первый план выходит квалификация персонала организации, его способность быстро обучаться, а также оперативное проведение учебных курсов. Важны и принципы выбора деловых партнеров.

Иногда внешние организации принимают на обслуживание и администрирование ответственные компоненты компьютерной системы, например, сетевое оборудование. Нередко администрирование выполняется в удаленном режиме. Вообще говоря, это создает в системе дополнительные уязвимые места, которые необходимо компенсировать усиленным контролем средств удаленного доступа или, опять-таки, обучением собственных сотрудников.

**Физическая защита**

Безопасность информационной системы зависит от окружения, в котором она функционирует. Необходимо принять меры для защиты зданий и прилегающей территории, поддерживающей инфраструктуры, вычислительной техники, носителей данных.

Основной принцип физической защиты, соблюдение которого следует постоянно контролировать, формулируется как “непрерывность защиты в пространстве и времени”. Ранее мы рассматривали понятие окна опасности. Для физической защиты таких окон быть не должно. Направления физической защиты:

- физическое управление доступом;
- противопожарные меры;
- защита поддерживающей инфраструктуры;
- защита от перехвата данных;
- защита мобильных систем.

Меры физического управления доступом позволяют контролировать и при необходимости ограничивать вход и выход сотрудников и посетителей. Контролироваться может все здание организации, а также отдельные помещения, например, те, где расположены серверы, коммуникационная аппаратура и т.п.

При проектировании и реализации мер физического управления доступом целесообразно применять *объектный подход*. Во-первых, определяется периметр безопасности, ограничивающий контролируемую территорию. На этом уровне детализации важно продумать внешний интерфейс организации – порядок входа/выхода штатных сотрудников и посетителей, вноса/выноса техники. Все, что не входит во внешний интерфейс, должно быть инкапсулировано, то есть, защищено от нелегальных проникновений.

Во-вторых, производится декомпозиция контролируемой территории, выделяются (под) объекты и связи (проходы) между ними. При такой, более глубокой детализации следует выделить среди подобъектов наиболее критичные с точки зрения безопасности и обеспечить им повышенное внимание. Декомпозиция должна быть семантически оправданной, обеспечивающей разграничение разнородных сущностей, таких как оборудование разных владельцев или персонал, работающий с данными разной степени критичности.

Необходимо, чтобы посетители, по возможности, не имели непосредственного доступа к компьютерам или, в крайнем случае, позаботиться о том, чтобы от окон и дверей не просматривались экраны мониторов и принтеры. Необходимо, чтобы посетителей по внешнему виду можно было отличить от сотрудников.

Средства физического управления доступом – это охрана, двери с замками, перегородки, телекамеры, датчики движения и многое другое. Для выбора оптимального (по критерию стоимость/эффективность) средства целесообразно провести анализ рисков (к этому мы еще вернемся). Кроме того, есть смысл периодически отслеживать появление технических новинок в данной области, стараясь максимально автоматизировать физическую защиту.

Отметим необходимость установки противопожарной сигнализации и автоматических средств пожаротушения. К поддерживающей инфраструктуре можно отнести системы электро-, водо- и теплоснабжения, кондиционеры и средства

коммуникаций. При размещении компьютеров необходимо принять во внимание расположение водопроводных и канализационных труб и постараться держаться от них подальше. Сотрудники должны знать, куда следует обращаться при обнаружении протечек.

Перехват данных может осуществляться самыми разными способами. Злоумышленник может подсматривать за экраном монитора, читать пакеты, передаваемые по сети, производить анализ побочных электромагнитных излучений и наводок (ПЭМИН) и т.д. Остается уповать на повсеместное использование криптографии (что, впрочем, сопряжено у нас в стране со множеством технических и законодательных проблем), стараться максимально расширить контролируемую территорию, разместившись в тихом особнячке, поодаль от других домов, пытаться держать под контролем линии связи (например, заключать их в надувную оболочку с обнаружением прокалывания), но самое разумное, вероятно, – постараться осознать, что для коммерческих систем обеспечение конфиденциальности является все-таки не главной задачей.

Мобильные и портативные компьютеры – заманчивый объект кражи. Их часто оставляют без присмотра, в автомобиле или на работе, и похитить такой компьютер совсем несложно. То и дело средства массовой информации сообщают о том, что какой-нибудь офицер английской разведки или американский военный лишился таким образом движимого имущества. Мы настоятельно рекомендуем шифровать данные на жестких дисках таких компьютеров.

Вообще говоря, при выборе средств физической защиты следует производить анализ рисков. Так, принимая решение о закупке источника бесперебойного питания, необходимо учесть качество электропитания в здании, занимаемом организацией (впрочем, почти наверняка оно окажется плохим). Характер и длительность сбоев электропитания, стоимость доступных источников и возможные потери от аварий (поломка техники, приостановка работы организации и т.п.).

В то же время, во многих случаях решения очевидны. Меры противопожарной безопасности обязательны для всех организаций. Стоимость реализации многих мер (например, установка обычного замка на дверь серверной комнаты) либо мала, либо хоть и заметна, но все же явно меньше, чем возможный ущерб. В частности, имеет смысл регулярно копировать большие базы данных.

**Поддержание работоспособности**

Далее рассмотрим ряд мероприятий, направленных на поддержание работоспособности информационных систем. Именно здесь таится наибольшая опасность. Нечаянные ошибки системных администраторов и пользователей грозят повреждением аппаратуры, разрушением программ и данных; в лучшем случае они создают бреши в защите, которые делают возможной реализацию угроз.

Недооценка факторов безопасности в повседневной работе – ахиллесова пята многих организаций. Дорогие средства безопасности теряют смысл, если они плохо документированы, конфликтуют с другим программным обеспечением, а пароль системного администратора не менялся с момента установки.

Можно выделить следующие направления повседневной деятельности:

- поддержка пользователей;
- поддержка программного обеспечения;
- конфигурационное управление;
- резервное копирование;
- управление носителями;
- документирование;
- регламентные работы.

*Поддержка пользователей* подразумевает прежде всего консультирование и оказание помощи при решении разного рода проблем. Иногда в организациях создают для этой цели специальный «справочный стол», но чаще от пользователей отбивается системный администратор. Очень важно в потоке вопросов уметь выявлять проблемы, связанные с информационной безопасностью. Так, многие трудности пользователей, работающих на персональных компьютерах, могут быть следствием заражения вирусами. Целесообразно фиксировать вопросы пользователей, чтобы выявлять их типичные ошибки и выпускать памятки с рекомендациями для распространенных ситуаций.

*Поддержка программного обеспечения* – одно из важнейших средств обеспечения целостности информации. Прежде всего, необходимо следить за тем, какое программное обеспечение установлено на компьютерах. Если пользователи будут устанавливать программы по своему усмотрению, это может привести к заражению вирусами, а также появлению утилит, действующих в обход защитных средств. Вполне вероятно также, что «самодеятельность» пользователей постепенно приведет к хаосу на их компьютерах, а исправлять ситуацию придется системному администратору.

Второй аспект поддержки программного обеспечения – контроль за отсутствием неавторизованного изменения программ и прав доступа к ним. Сюда же можно отнести поддержку эталонных копий программных систем. Обычно контроль достигается комбинированием средств физического и логического управления доступом, а также использованием утилит проверки и обеспечения целостности.

*Конфигурационное управление* позволяет контролировать и фиксировать изменения, вносимые в программную конфигурацию. Прежде всего, необходимо застраховаться от случайных или непродуманных модификаций, уметь как минимум

возвращаться к прошлой, работающей, версии. Фиксация изменений позволит легко восстановить текущую версию после аварии.

Лучший способ уменьшить количество ошибок в рутинной работе – максимально автоматизировать ее. Автоматизация и безопасность зависят друг от друга; тот, кто заботится в первую очередь об облегчении своей задачи, на самом деле оптимальным образом формирует режим информационной безопасности.

*Резервное копирование* необходимо для восстановления программ и данных после аварий. И здесь целесообразно автоматизировать работу, как минимум, сформировав компьютерное расписание создания полных и инкрементальных копий, а как максимум – воспользовавшись соответствующими программными продуктами. Нужно также наладить размещение копий в безопасном месте, защищенном от несанкционированного доступа, пожаров, протечек, то есть от всего, что может привести к краже или повреждению носителей. Целесообразно иметь несколько экземпляров резервных копий и часть из них хранить вне территории организации, защищаясь таким образом от крупных аварий и аналогичных инцидентов. Время от времени в тестовых целях следует проверять возможность восстановления информации с копий.

*Управлять носителями* необходимо для обеспечения физической защиты и учета дискет, лент, печатных выдач и т.п. Управление носителями должно обеспечивать конфиденциальность, целостность и доступность информации, хранящейся вне компьютерных систем. Под физической защитой здесь понимается не только отражение попыток несанкционированного доступа, но и предохранение от вредных влияний окружающей среды (жары, холода, влаги, магнетизма). Управление носителями должно охватывать весь жизненный цикл – от закупки до выведения из эксплуатации.

*Документирование* – неотъемлемая часть информационной безопасности. В виде документов оформляется почти все – от политики безопасности до журнала учета носителей. Важно, чтобы документация была актуальной, отражала именно текущее состояние дел, причем в непротиворечивом виде.

К хранению одних документов (содержащих, например, анализ уязвимых мест системы и угроз) применимы требования обеспечения конфиденциальности, к другим, таким как план восстановления после аварий – требования целостности и доступности (в критической ситуации план необходимо найти и прочитать).

*Регламентные работы* – очень серьезная угроза безопасности. Сотрудник, осуществляющий регламентные работы, получает исключительный доступ к системе, и на практике очень трудно проконтролировать, какие именно действия он совершает. Здесь на первый план выходит степень доверия к тем, кто выполняет работу.

**Реагирование на нарушения режима безопасности**

Программа безопасности, принятая организацией, должна предусматривать набор оперативных мероприятий, направленных на обнаружение и нейтрализацию нарушений режима информационной безопасности. Важно, чтобы в подобных случаях последовательность действий была спланирована заранее, поскольку меры нужно принимать срочные и скоординированные.

Реакция на нарушения режима безопасности преследует три главные цели:

- локализация инцидента и уменьшение наносимого вреда;
- выявление нарушителя;
- предупреждение повторных нарушений.

В организации должен быть человек, доступный 24 часа в сутки (лично, по телефону, пейджеру или электронной почте), который отвечает за реакцию на нарушения. Все должны знать координаты этого человека и обращаться к нему при первых признаках опасности. В общем, как при пожаре, нужно знать, куда звонить, и что делать до приезда пожарной команды.

Нередко требование локализации инцидента и уменьшения наносимого вреда вступает в конфликт с желанием выявить нарушителя. В ПБ организации приоритеты действий, совершаемых во время инцидента, должны быть расставлены заранее. Шкала приоритетов может выглядеть следующим образом:

- защита жизни и здоровья людей;
- защита секретных и/или критически важных данных;
- защита прочих данных, включая частную, научную и управленческую информацию;
- предотвращение повреждения систем;
- минимизация урона, нанесенного вычислительным ресурсам.

Идентификации инцидента сопутствует выяснение его масштабов и возможных последствий, а для эффективного противодействия важно правильно определить его границы. Кроме того, оценка возможных последствий позволит установить приоритеты при выделении ресурсов для принятия ответных мер.

Чтобы найти нарушителя, нужно заранее выяснить контактные координаты поставщика сетевых услуг и договориться с ним о самой возможности и порядке выполнения соответствующих действий. Чтобы предотвратить повторные нарушения, необходимо анализировать каждый инцидент, выявлять причины, накапливать статистику. Каковы источники вредоносного ПО? Какие пользователи имеют обыкновение выбирать слабые пароли? На подобные вопросы и должны дать ответ результаты анализа.

Необходимо отслеживать появление новых уязвимых мест и как можно быстрее ликвидировать ассоциированные с ними окна опасности. Кто-то в организации должен

курировать этот процесс, принимать краткосрочные меры и корректировать программу безопасности для принятия долгосрочных мер.

Враждебные акции, будь то нападение внешних злоумышленников или месть обиженного сотрудника, необходимо предусмотреть заранее. Ничто не может заменить предварительно составленного плана восстановительных работ. В разделах политики безопасности, касающихся реакции на инциденты, должны быть освещены следующие темы:

- обзор (цели, преследуемые ПБ в плане реакции на инциденты);
- оценка (насколько серьезно произошедшее событие);
- извещение (кого следует известить о нем);
- ответные меры (что следует предпринять в ответ);
- правовой аспект (каковы правовые последствия случившегося);
- регистрационная документация (что следует фиксировать до, во время и после инцидента).

Когда есть уверенность, что нарушение режима безопасности действительно имеет место, следует известить соответствующий персонал. Чтобы удержать события под контролем и с технической, и с эмоциональной точек зрения, очень важно, кто и как будет извещен.

Любое сообщение об инциденте должно быть внятным, любая фраза - ясной, точной и полной. Попытки скрыть отдельные моменты, сообщая ложную или неполную информацию, способны не только помешать принятию эффективных ответных мер, но и привести к ухудшению ситуации.

Меры, предпринимаемые для борьбы с нарушением, можно подразделить на основные категории:

сдерживание;

ликвидация;

восстановление;

анализ.

Цель сдерживания - ограничить атакуемую область. Например, как можно быстрее приостановить распространение червя в сети.

Когда задача сдерживания решена, можно приступать к ликвидации. В этом поможет программный инструментарий (в частности, антивирусные пакеты).

После ликвидации атаки наступает время восстановления, т. е. приведения системы в нормальное состояние. Следует предпринять по крайней мере следующие действия:

произвести переучет системных активов, т. е. тщательно проверить состояние систем;

отразить уроки, извлеченные из инцидента, в пересмотренной программе обеспечения безопасности, чтобы не допустить повторения аналогичного нарушения;

произвести новый анализ риска с учетом полученной информации;

начать следствие против виновников инцидента, если это признано необходимым.

Устранить все уязвимые места, сделавшие возможным нарушение режима безопасности, непросто, но необходимо. Ключевым моментом здесь является понимание механизма вторжения.

При восстановлении, возможно, придется вернуться к начальному состоянию системы с последующей ее настройкой. Чтобы облегчить действия даже в таком, наихудшем, случае, целесообразно хранить записи о начальных установках и обо всех внесенных изменениях.

Анализ – одна из самых важных стадий реакции на инциденты, о которой, тем не менее, почти всегда забывают. Она важна потому, что позволяет всем причастным лицам извлечь поучительные уроки, чтобы в будущем в аналогичных ситуациях действовать эффективнее.

Требуется получить ответы по крайней мере на следующие вопросы:

Что именно и когда произошло?

Насколько хорошо сработал персонал?

Какая срочная информация понадобилась в первую очередь, и что способствовало ее скорейшему получению?

Что в следующий раз нужно делать по-другому?

После восстановления системы в ней нередко остаются уязвимости или даже ловушки. На фазе анализа система должна быть тщательно обследована, чтобы выявить проблемы, упущенные при восстановлении. В качестве отправной точки разумно воспользоваться программными средствами контроля защищенности.

Целесообразно документировать все детали, связанные с инцидентом: способы его обнаружения, процедуры исправления ситуации, процедуры мониторинга и усвоенные уроки. Детальное документирование в конечном итоге ведет к экономии времени, позволяет оценить размер нанесенного ущерба.

**Планирование восстановительных работ**

Ни одна организация не застрахована от серьезных аварий, вызванных естественными причинами, действиями злоумышленника, халатностью или некомпетентностью. В то же время, у каждой организации есть функции, которые руководство считает критически важными, они должны выполняться несмотря ни на что. Планирование восстановительных работ позволяет подготовиться к авариям, уменьшить ущерб от них и сохранить способность к функционированию хотя бы в минимальном объеме.

Отметим, что меры информационной безопасности можно разделить на три группы, в зависимости от того, направлены ли они на предупреждение, обнаружение или ликвидацию последствий атак. Большинство мер носит предупредительный характер. Оперативный анализ регистрационной информации и некоторые аспекты реагирования на нарушения (так

называемый активный аудит) служат для обнаружения и отражения атак. Планирование восстановительных работ, очевидно, можно отнести к последней из трех перечисленных групп.

Процесс планирования восстановительных работ можно разделить на следующие этапы:

выявление критически важных функций организации, установление приоритетов;

идентификация ресурсов, необходимых для выполнения критически важных функций;

определение перечня возможных аварий;

разработка стратегии восстановительных работ;

подготовка к реализации выбранной стратегии;

проверка стратегии.

Планируя восстановительные работы, следует отдавать себе отчет в том, что полностью сохранить функционирование организации не всегда возможно. Необходимо выявить критически важные функции, без которых организация теряет свое лицо, и даже среди критичных функций расставить приоритеты, чтобы как можно быстрее и с минимальными затратами возобновить работу после аварии.

*Идентифицируя ресурсы*, необходимые для выполнения критически важных функций, следует помнить, что многие из них имеют некомпьютерный характер. На данном этапе желательно подключать к работе специалистов разного профиля, способных в совокупности охватить все аспекты проблемы. Критичные ресурсы обычно относятся к одной из следующих категорий:

персонал;

информационная инфраструктура;

физическая инфраструктура.

Составляя списки ответственных специалистов, следует учитывать, что некоторые из них могут непосредственно пострадать от аварии (например, от пожара), кто-то может находиться в состоянии стресса, часть сотрудников, возможно, будет лишена возможности попасть на работу (например, в случае массовых беспорядков). Желательно иметь некоторый резерв специалистов или заранее определить каналы, по которым можно на время привлечь дополнительный персонал.

Информационная инфраструктура включает в себя элементы, описанные в пункте «идентификация активов».

Нужно подготовиться к тому, что на «запасном аэродроме», куда организация будет эвакуирована после аварии, аппаратная платформа может отличаться от исходной. Соответственно, следует продумать меры поддержания совместимости по программам и данным.

Среди внешних информационных сервисов для коммерческих организаций, вероятно, важнее всего получить оперативную информацию и связь с государственными службами, курирующими данный сектор экономики.

Документация важна хотя бы потому, что не вся информация, с которой работает организация, представлена в электронном виде. Скорее всего, план восстановительных работ напечатан на бумаге.

К физической инфраструктуре относятся здания, инженерные коммуникации, средства связи, оргтехника и многое другое. Компьютерная техника не может работать в плохих условиях, без стабильного электропитания и т.п.

Анализируя критичные ресурсы, целесообразно учесть временной профиль их использования. Большинство ресурсов требуются постоянно, но в некоторых нужда может возникать только в определенные периоды (например, в конце месяца или года при составлении отчета).

При определении перечня возможных аварий нужно попытаться разработать их сценарии. Как будут развиваться события? Каковы могут оказаться масштабы бедствия? Что произойдет с критичными ресурсами? Например, смогут ли сотрудники попасть на работу? Будут ли выведены из строя компьютеры? Возможны ли случаи саботажа? Будет ли работать связь? Пострадает ли здание организации? Можно ли будет найти и прочитать необходимые бумаги?

Стратегия восстановительных работ должна базироваться на наличных ресурсах и быть не слишком накладной для организации. При разработке стратегии целесообразно провести анализ рисков, которым подвергаются критичные функции, и попытаться выбрать наиболее экономичное решение.

Стратегия должна предусматривать не только работу по временной схеме, но и возвращение к нормальному функционированию.

Подготовка к реализации выбранной стратегии состоит в выработке плана действий в экстренных ситуациях и по их окончании, а также в обеспечении некоторой избыточности критичных ресурсов. Последнее возможно и без большого расхода средств, если заключить с одной или несколькими организациями соглашения о взаимной поддержке в случае аварий – те, кто не пострадал, предоставляют часть своих ресурсов во временное пользование менее удачливым партнерам.

Избыточность обеспечивается также мерами резервного копирования, хранением копий в нескольких местах, представлением информации в разных видах (на бумаге и в файлах) и т.д. Имеет смысл заключить соглашение с поставщиками информационных услуг о первоочередном обслуживании в критических ситуациях или заключать соглашения с несколькими поставщиками. Правда, эти меры могут потребовать определенных расходов.

Проверка стратегии производится путем анализа подготовленного плана, принятых и намеченных мер.

### 6.4. Программно-технический уровень

В предыдущих разделах по практические мероприятиям построения интегрированной системы информационной были освещены законодательный, административный и процедурный уровни системы ОБИ. Последний уровень формирования защищенной информационной системы отвечает за выработку программно-технических мер и, соответственно, носит название *программно-технического уровня*.

Работа на данном уровне заключаются в выборе механизмов (подсистем) и средств ОБИ, рисунок 6.3.

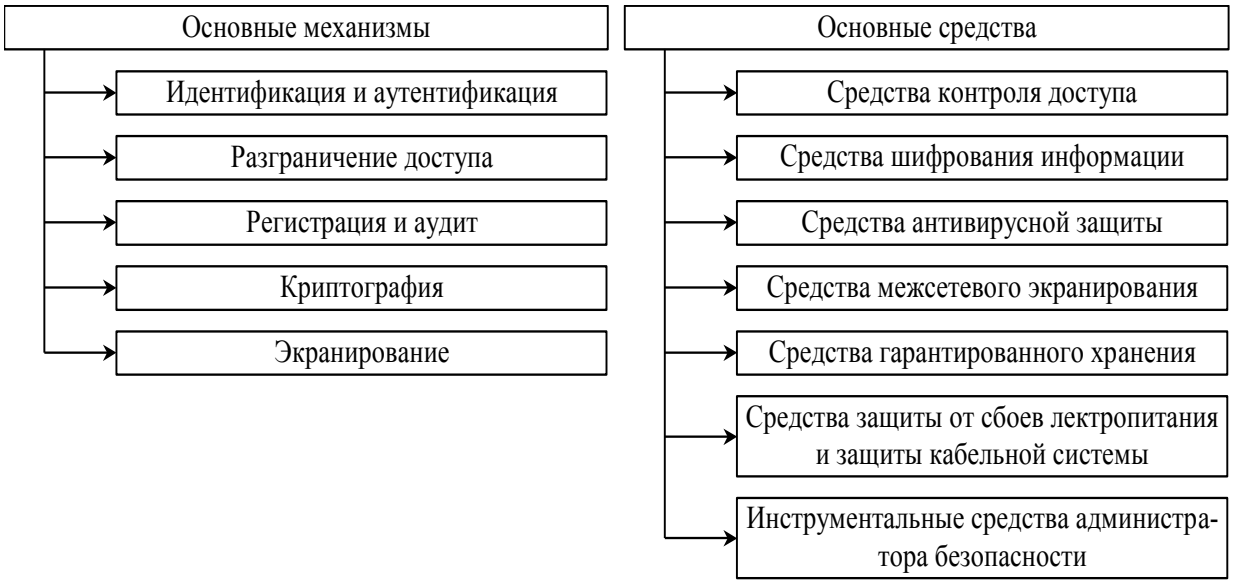



Рис. 6.3. Основные механизмы и средства интегрированной системы информационной безопасности предприятия

Далее рассмотрим более подробно представленные механизмы и средства.

#### 6.4.1. Идентификация и аутентификация

Основой систем ОБИ являются идентификация и аутентификация, так как все механизмы защиты информации рассчитаны на работу с поименованными субъектами и объектами АС. В качестве *субъектов* АС могут выступать как пользователи, так и процессы, а в качестве *объектов* АС – информация и другие информационные ресурсы системы.

Присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным перечнем называется *идентификацией. Идентификатор пользователя* – некоторое уникальное количество информации, позволяющее различать индивидуальных пользователей парольной системы (проводить их идентификацию). Часто идентификатор

также называют *именем* пользователя или *именем учетной записи* пользователя. Идентификация обеспечивает выполнение следующих функций ОБИ [2]:

установление подлинности и определение полномочий субъекта при его допуске в систему,

контролирование установленных полномочий в процессе сеанса работы;

регистрация действий и др.

*Аутентификацией* (*установлением подлинности)* называется проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности. Другими словами, аутентификация заключается в проверке: является ли подключающийся субъект тем, за кого он себя выдает.

**Процедура аутентификации**

Общая процедура идентификации и аутентификации пользователя при его доступе в АС представлена на рисунке 6.4. Если в процессе аутентификации подлинность субъекта установлена, то система защиты информации должна определить его полномочия (совокупность прав). Это необходимо для последующего контроля и разграничения доступа к ресурсам.

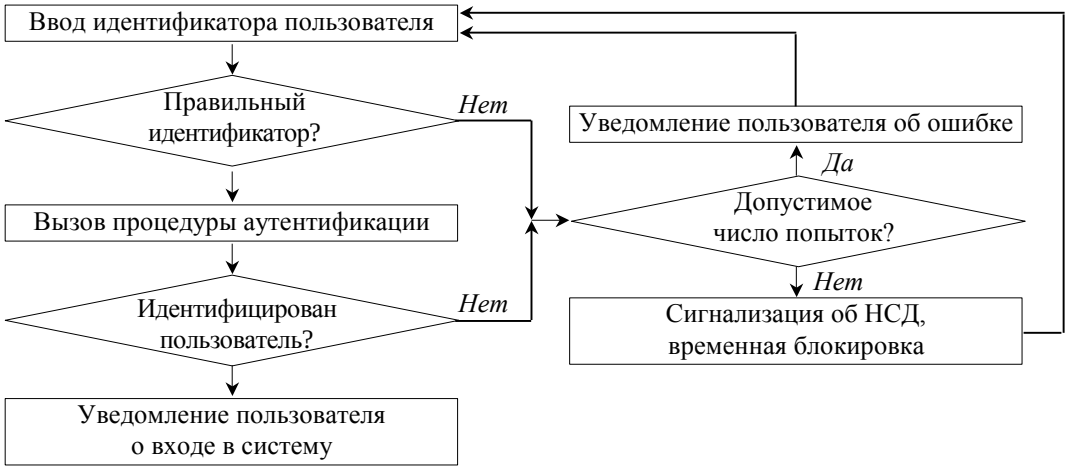



Рис. 6.4. Классическая процедура идентификации и аутентификации

**Классификация систем аутентификации**

Классифицировать системы аутентификации можно по различным признакам,

рисунок 6.5.

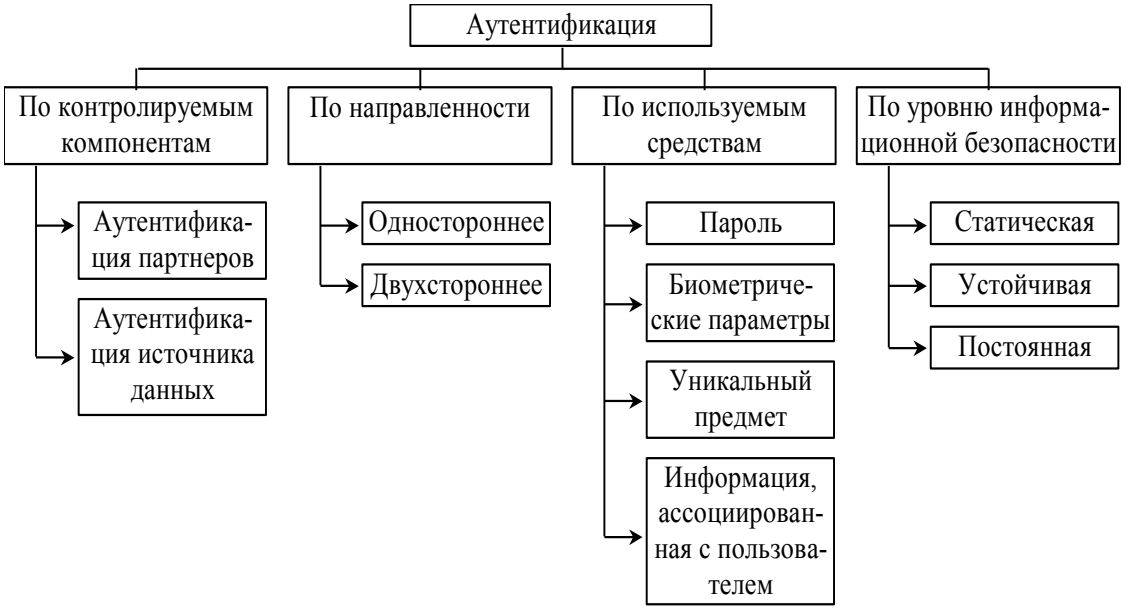



Рис. 6.5. Классифицировать системы аутентификации

По *контролируемому компоненту* системы способы аутентификации можно разделить на аутентификацию партнеров по общению и аутентификацию источника данных. *Аутентификация партнеров* по общению используется при установлении (и периодической проверке) соединения во время сеанса. Она служит для предотвращения таких угроз, как маскарад и повтор предыдущего сеанса связи. *Аутентификация источника данных* – это подтверждение подлинности источника отдельной порции данных.

По *направленности* аутентификация может быть *односторонней* (пользователь доказывает свою подлинность системе, например при входе в систему) и *двусторонней* (взаимной).

Обычно методы аутентификации классифицируют по *используемым средствам*. В этом случае указанные методы делят на четыре группы:

Основанные на знании лицом, имеющим право на доступ к ресурсам системы, некоторой *секретной информации – пароля*.

Основанные на использовании *уникального предмета*: жетона, электронной карточки и др.

Основанные на измерении *биометрических параметров человека* – физиологических или поведенческих атрибутах живого организма.

Основанные на *информации, ассоциированной с пользователем*, например с его координатами.

Рассмотрим эти группы подробнее.

1. Наиболее распространенными простыми и привычными являются методы аутентификации, основанные на *паролях* — секретных идентификаторах субъектов. Здесь

при вводе субъектом своего пароля подсистема аутентификации сравнивает его с паролем, хранящимся в базе эталонных данных в зашифрованном виде. В случае совпадения паролей подсистема аутентификации разрешает доступ к ресурсам АС.

Парольные методы следует классифицировать по степени изменяемости паролей:

методы, использующие постоянные (многократно используемые) пароли,

методы, использующие одноразовые (динамично изменяющиеся) пароли.

В большинстве АС используются многоразовые пароли. В этом случае пароль пользователя не изменяется от сеанса к сеансу в течение установленного администратором системы времени его действительности. Это упрощает процедуры администрирования, но повышает угрозу рассекречивания пароля. Известны множество способов вскрытия пароля: от подсмотра через плечо до перехвата сеанса связи. Вероятность вскрытия злоумышленником пароля повышается, если пароль несет смысловую нагрузку (год рождения, имя девушки), небольшой длины, набран на одном регистре, не имеет ограничений на период существования и т.д. Важно, разрешено ли вводить пароль только в диалоговом режиме или есть возможность обращаться из программы. В последнем случае, возможно запустить программу по подбору паролей. Более надежный способ – использование одноразовых или динамически меняющихся паролей. Известны следующие методы парольной защиты, основанные на одноразовых паролях:

методы модификации схемы простых паролей;

методы «запрос-ответ»;

функциональные методы.

В первом случае пользователю выдается список паролей. При аутентификации система запрашивает у пользователя пароль, номер в списке которого определен по случайному закону. Длина и порядковый номер начального символа пароля тоже могут задаваться случайным образом.

При использовании метода «запрос-ответ» система задает пользователю некоторые вопросы общего характера, правильные ответы на которые известны только конкретному пользователю.

Функциональные методы основаны на использовании специальной функции парольного преобразования F(X). Это позволяет обеспечить возможность изменения (по некоторой формуле) паролей пользователя во времени. Указанная функция должна удовлетворять следующим требованиям:

для заданного пароля X легко вычислить новый пароль Y = F(X);

зная X и Y, сложно или невозможно определить функцию F(X).

Наиболее известными примерами функциональных методов являются: метод функционального преобразования и метод “рукопожатия”.

Идея метода функционального преобразования состоит в периодическом изменении самой функции F(X). Последнее достигается наличием в функциональном выражении динамически меняющихся параметров, например функции от некоторой даты и времени. Пользователю сообщается исходный пароль, собственно функция и периодичность смены пароля. Нетрудно видеть, что паролями пользователя на заданных n-периодах времени будут следующие: X, F(X), F(F(X)), ... $F(X)^{n-1}$.

Метод “рукопожатия” состоит в следующем. Функция парольного преобразования известна только пользователю и системе защиты. При входе в АС подсистема аутентификации генерирует случайную последовательность X, которая передается пользователю. Пользователь вычисляет результат функции Y= F(X) и возвращает его в систему. Система сравнивает собственный вычисленный результат с полученным от пользователя. При совпадении указанных результатов подлинность пользователя считается доказанной.

Достоинством метода является то, что передача какой-либо информации, которой может воспользоваться злоумышленник, здесь сведена к минимуму.

В ряде случаев пользователю может оказаться необходимым проверить подлинность другого удаленного пользователя или некоторой АС, к которой он собирается осуществить доступ. Наиболее подходящим здесь является метод «рукопожатия», так как никто из участников информационного обмена не получит никакой конфиденциальной информации.

Отметим, что методы аутентификации, основанные на одноразовых паролях, также не обеспечивают абсолютной защиты. Например, если злоумышленник имеет возможность подключения к сети и перехватывать передаваемые пакеты, то он может посылать последние как собственные.

2. В последнее время получили распространение комбинированные методы идентификации, требующие, помимо знания пароля, наличие *карточки* (token) – специального устройства, подтверждающего подлинность субъекта.

Карточки разделяют на два типа:

пассивные (карточки с памятью);

активные (интеллектуальные карточки).

Самыми распространенными являются пассивные карточки с магнитной полосой, которые считываются специальным устройством, имеющим клавиатуру и процессор. При использовании указанной карточки пользователь вводит свой идентификационный номер. В случае его совпадения с электронным вариантом, закодированным в карточке, пользователь получает доступ в систему. Это позволяет достоверно установить лицо, получившее доступ к системе и исключить несанкционированное использование карточки злоумышленником

(например, при ее утере). Такой способ часто называют двухкомпонентной аутентификацией.

Иногда (обычно для физического контроля доступа) карточки применяют сами по себе, без запроса личного идентификационного номера.

К *достоинству* использования карточек относят то, что обработка аутентификационной информации выполняется устройством чтения, без передачи в память компьютера. Это исключает возможность электронного перехвата по каналам связи.

*Недостатки* пассивных карточек следующие: они существенно дороже паролей, требуют специальные устройства чтения, их использование подразумевает специальные процедуры безопасного учета и распределения. Их также необходимо оберегать от злоумышленников, в первую очередь, естественно, не оставлять в устройствах. Известны случаи подделки пассивных карточек.

Интеллектуальные карточки кроме памяти имеют собственный микропроцессор. Это позволяет реализовать различные варианты парольных методов защиты, как-то: многоразовые пароли, динамически меняющиеся пароли, обычно “запрос – ответные” методы. Все карточки обеспечивают двухкомпонентную аутентификацию.

К указанным достоинствам интеллектуальных карточек следует добавить их многофункциональность. Их можно применять не только для целей безопасности, но и, например, для финансовых операций. Сопутствующим недостатком карточек является их высокая стоимость.

3. Методы аутентификации, основанные на измерении *биометрических параметров* человека, обеспечивают почти 100%-ую идентификацию, решая проблемы утери или утраты паролей и личных идентификаторов. Однако методы нельзя использовать при идентификации процессов или данных (объектов данных), они только начинают развиваться (имеются проблемы со стандартизацией и распространением), требуют пока сложного и дорогостоящего оборудования. Это обусловливает их использование пока только на особо важных объектах и системах, главным образом в МО РФ.

Примерами внедрения указанных методов являются системы идентификации пользователя по рисунку радужной оболочки глаза, отпечаткам ладони, формам ушей, инфракрасной картине капиллярных сосудов, по почерку, по запаху, по тембру голоса и даже по ДНК рисунок 6.6.

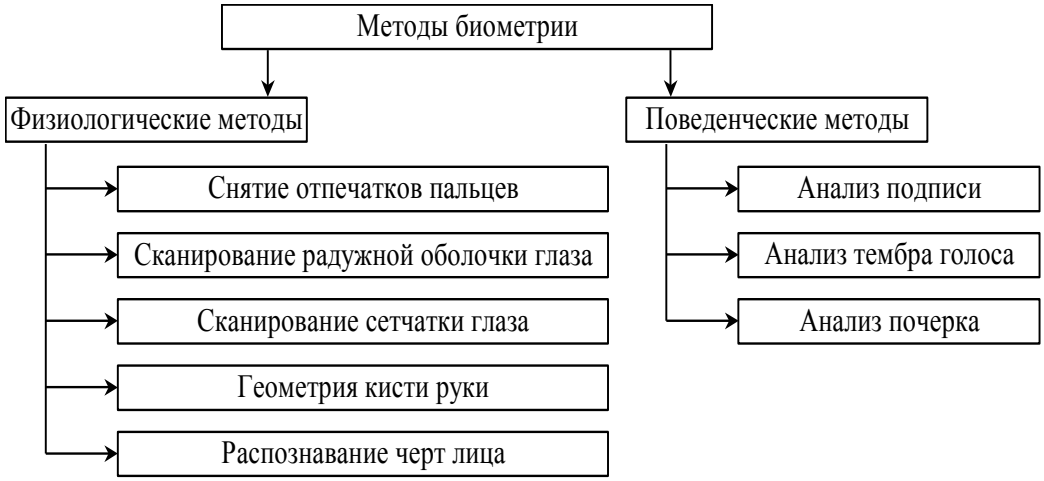



Рис. 6.6. Примеры распространенных методов биометрии

Новым направлением является использование биометрических характеристик в интеллектуальных расчетных карточках, жетонах-пропусках и элементах сотовой связи. Например, при расчете в магазине предъявитель карточки кладет палец на сканер в подтверждение, что карточка действительно его.

Назовем наиболее используемые биометрические атрибуты и соответствующие системы.

*Отпечатки пальцев*. Такие сканеры имеют небольшой размер, универсальны, относительно недороги. Биологическая повторяемость отпечатка пальца составляет $10^{-5}$%. В настоящее время пропагандируются правоохранительными органами из-за крупных ассигнований в электронные архивы отпечатков пальцев.

*Геометрия руки*. Соответствующие устройства используются, когда из-за грязи или травм трудно применять сканеры пальцев. Биологическая повторяемость геометрии руки около 2-х %.

*Радужная оболочка глаза*. Данные устройства обладают наивысшей точностью. Теоретическая вероятность совпадения двух радужных оболочек составляет 1 из $10^{78}$.

*Термический образ лица*. Системы позволяют идентифицировать человека на расстоянии до десятков метров. В комбинации с поиском данных по базе данных такие системы используются для опознания авторизованных сотрудников и отсеивания посторонних. Однако при изменении освещенности сканеры лица имеют относительно высокий процент ошибок.

*Голос*. Проверка голоса удобна для использования в телекоммуникационных приложениях. Необходимые для этого 16-разрядная звуковая плата и конденсаторный микрофон стоят менее 25 $. Вероятность ошибки составляет 2-5%. Данная технология подходит для верификации по голосу по телефонным каналам связи, она более надежна по сравнению с частотным набором личного номера. Сейчас развиваются направления

идентификации личности и его состояния по голосу — возбужден, болен, говорит правду, не в себе и т.д.

*Ввод с клавиатуры*. Здесь при вводе, например, пароля отслеживаются скорость и интервалы между нажатиями.

*Подпись*. Для контроля рукописной подписи используются дигитайзеры.

4. Новейшим направлением аутентификации является доказательство подлинности удаленного пользователя по его местонахождению. Данный защитный механизм основан на использовании системы космической навигации, типа GPS (Global Positioning System). Пользователь, имеющий аппаратуру GPS, многократно посылает координаты заданных спутников, находящихся в зоне прямой видимости. Подсистема аутентификации, зная орбиты спутников, может с точностью до метра определить месторасположение пользователя. Высокая надежность аутентификации определяется тем, что орбиты спутников подвержены колебаниям, предсказать которые достаточно трудно. Кроме того, координаты постоянно меняются, что сводит на нет их перехват. В данном случае, есть мнение, что изящная территориально-распределенная атака на компьютерные системы под силу лишь программистам Ракетно-Космических Сил.

Аппаратура GPS проста и надежна в использовании и сравнительно недорога. Это позволяет ее использовать в случаях, когда авторизованный удаленный пользователь должен находиться в нужном месте.

Суммируя возможности средств аутентификации, ее можно классифицировать по уровню информационной безопасности на три категории:

Статическая аутентификация;

Устойчивая аутентификация;

Постоянная аутентификация.

Первая категория обеспечивает защиту только от НСД в системах, где нарушитель не может во время сеанса работы прочитать аутентификационную информацию. Примером средства статической аутентификации являются традиционные постоянные пароли. Их эффективность преимущественно зависит от сложности угадывания паролей и, собственно, от того, насколько хорошо они защищены.

Для компрометации статической аутентификации нарушитель может подсмотреть, подобрать, угадать или перехватить аутентификационные данные и т.д.

Устойчивая аутентификация использует динамические данные аутентификации, меняющиеся с каждым сеансом работы. Реализациями устойчивой аутентификации являются системы, использующие одноразовые пароли и электронные подписи. Усиленная аутентификация обеспечивает защиту от атак, где злоумышленник может перехватить аутентификационную информацию и силиться использовать ее в следующих сеансах работы.

Однако устойчивая аутентификация не обеспечивает защиту от активных атак, в ходе которых маскирующийся злоумышленник может оперативно (в течение сеанса аутентификации) перехватить, модифицировать и вставить информацию в поток передаваемых данных.

Постоянная аутентификация обеспечивает идентификацию каждого блока передаваемых данных, что предохраняет их от несанкционированной модификации или вставки. Примером реализации указанной категории аутентификации является использование алгоритмов генерации электронных подписей для каждого бита пересылаемой информации.

### 6.4.2. Разграничение доступа

После выполнения идентификации и аутентификации необходимо установить полномочия (совокупность прав) субъекта для последующего контроля санкционированного использования вычислительных ресурсов, доступных в АС. Такой процесс называется *разграничением (логическим управлением) доступа*.

Обычно полномочия субъекта представляются: списком ресурсов, доступным пользователю, и правами по доступу к каждому ресурсу из списка. В качестве вычислительных ресурсов могут быть программы, информация, логические устройства, объем памяти, время процессора, приоритет и т.д.

Можно выделить следующие методы разграничения доступа:

разграничение доступа по спискам,

использование матрицы установления полномочий,

разграничения доступа по уровням секретности и категориям,

парольное разграничение доступа.

Рассмотрим подробнее приведенные методы разграничения доступа.

1. При *разграничении доступа по спискам* задаются соответствия:

каждому пользователю — список ресурсов и прав доступа к ним;

каждому ресурсу — список пользователей и их прав доступа к данному ресурсу.

Списки позволяют установить права с точностью до пользователя. Здесь нетрудно добавить права или явным образом запретить доступ. Списки используются в большинстве ОС и СУБД.

2. *Использование матрицы установления* полномочий подразумевает применение *матрицы доступа* (таблицы полномочий). В указанной матрице строками являются идентификаторы субъектов, имеющих доступ в АС, а столбцами — объекты (информационные ресурсы) АС. Каждый элемент матрицы может содержать имя и размер предоставляемого ресурса, право доступа (чтение, запись и др.), ссылку на другую информационную структуру, уточняющую права доступа, ссылку на программу, управляющую правами доступа и др.

Данный метод предоставляет более унифицированный и удобный подход, т.к. вся информация о полномочиях хранится в виде единой таблицы, а не в виде разнотипных списков. Недостатками матрицы являются ее возможная громоздкость и неоптимальность (большинство клеток - пустые).

3. *Разграничения доступа по уровням секретности и категориям* состоят в том, что ресурсы АС разделяются в соответствии с уровнями секретности или категорий.

При разграничении по уровню секретности выделяют несколько уровней, например: общий доступ, конфиденциально, секретно, совершенно секретно. Полномочия каждого пользователя задаются в соответствии с максимальным уровнем секретности, к которому он допущен. Пользователь имеет доступ ко всем данным, имеющим уровень (гриф) секретности не выше, чем он имеет.

При разграничении по категориям задается и контролируется ранг категории, соответствующей пользователю. Соответственно, все ресурсы АС декомпозируют по уровню важности, причем определенному уровню соответствует некоторый ранг персонала (типа: руководитель, администратор, пользователь).

4. *Парольное разграничение*, очевидно, представляет использование методов доступа субъектов к объектам по паролю. При этом используются все методы парольной защиты. Очевидно, что постоянное использование паролей создает неудобства пользователям и временные задержки. Поэтому указанные методы используют в исключительных ситуациях.

На практике обычно сочетают различные методы разграничения доступа. Например, первые три метода усиливают парольной защитой.

В ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации» и в документах Гостехкомиссии определены два вида (принципа) разграничения доступа:

дискретное управление доступом,

мандатное управление доступом.

*Дискретное управление доступом* представляет собой разграничение доступа между поименованными субъектами и поименованными объектами. Субъект с определенным правом доступа может передать это право любому другому субъекту. Данный вид организуется на базе методов разграничения по спискам или с помощью матрицы.

*Мандатное управление доступом* — разграничение доступа субъектов к объектам, основанное на характеризуемой меткой конфиденциальности информации, содержащейся в объектах, и официальном разрешении (допуске) субъектов обращаться к информации такого уровня конфиденциальности. Иначе, для реализации мандатного управления доступом каждому субъекту и каждому объекту присваивают классификационные метки, отражающие их место в соответствующей иерархии. С помощью этих меток субъектам и объектам

должны быть назначены классификационные уровни, являющиеся комбинациями уровня иерархической классификации и иерархических категорий. Данные метки должны служить основой мандатного принципа разграничения доступа. Ясно, что методы разграничения доступа по уровням секретности и категориям являются примерами мандатного управления доступом.

**Ролевое управление доступом**

При большом количестве пользователей традиционные подсистемы управления доступом становятся крайне сложными для администрирования. Число связей в них пропорционально произведению количества пользователей на количество объектов. Необходимы решения в объектно-ориентированном стиле, способные эту сложность понизить.

Таким решением является *ролевое управление доступом* (РУД). Суть его в том, что между пользователями и их привилегиями появляются промежуточные сущности – *роли*. Для каждого пользователя одновременно могут быть активными несколько ролей, каждая из которых дает ему определенные права (рисунок 6.7).

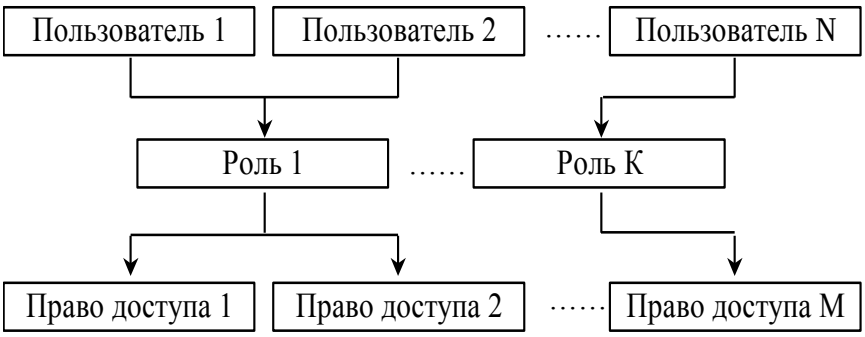



Рис. 6.7. Пользователи, объекты и роли.

Ролевой доступ нейтрален по отношению к конкретным видам прав и способам их проверки; его можно рассматривать как объектно-ориентированный каркас, облегчающий администрирование, поскольку он позволяет сделать подсистему разграничения доступа управляемой при сколь угодно большом числе пользователей, прежде всего за счет установления между ролями связей, аналогичных наследованию в объектно-ориентированных системах. Кроме того, ролей должно быть значительно меньше, чем пользователей. В результате число администрируемых связей становится пропорциональным сумме (а не произведению) количества пользователей и объектов, что по порядку величины уменьшить уже невозможно.

Ролевой доступ развивается более 10 лет (сама идея ролей, разумеется, значительно старше) как на уровне операционных систем, так и в рамках СУБД и других

информационных сервисов. В частности, существуют реализации ролевого доступа для Web-серверов.

В 2001 году Национальный институт стандартов и технологий США предложил проект стандарта ролевого управления доступом, основные положения которого приведены ниже.

Ролевое управление доступом оперирует следующими основными понятиями:

пользователь (человек, интеллектуальный автономный агент и т.п.);

сеанс работы пользователя;

роль (обычно определяется в соответствии с организационной структурой);

объект (сущность, доступ к которой разграничивается; например, файл ОС или таблица СУБД);

операция (зависит от объекта: для файлов ОС – чтение, запись, выполнение и т.п.; для таблиц СУБД – вставка, удаление и т.п.);

право доступа (разрешение выполнять определенные операции над определенными объектами).

*Ролям приписываются пользователи и права доступа,* можно считать, что они (роли) именуют отношения “многие ко многим” между пользователями и правами. Роли могут быть приписаны многие пользователи; один пользователь может быть приписан нескольким ролям. Во время сеанса работы пользователя активизируется подмножество ролей, которым он приписан, в результате чего он становится обладателем объединения прав, приписанных активным ролям. Одновременно пользователь может открыть несколько сеансов.

Между ролями может быть определено отношение частичного порядка, называемое *наследованием*. Если роль r2 является наследницей r1, то все права r1 приписываются r2, а все пользователи r2 приписываются r1. *Наследование ролей* соответствует наследованию классов в объектно-ориентированном программировании, только правам доступа соответствуют методы классов, а пользователям – объекты (экземпляры) классов.

Отношение наследования является иерархическим, причем права доступа и пользователи распространяются по уровням иерархии навстречу друг другу. В общем случае наследование является множественным, то есть у одной роли может быть несколько предшественниц (и, естественно, несколько наследниц, которых мы будем называть также преемницами).

Можно представить себе формирование *иерархии ролей,* начиная с минимума прав (и максимума пользователей), приписываемых роли «сотрудник», с постепенным уточнением состава пользователей и добавлением прав (роли «системный администратор», «бухгалтер» и т.п.), вплоть до роли «руководитель» (что, впрочем, не значит, что руководителю предоставляются неограниченные права, как и другим ролям, в соответствии с принципом *минимизации привилегий*, этой роли целесообразно разрешить только то, что необходимо для выполнения служебных обязанностей).

Существует масса принципов информационной безопасности, в частности *разделение обязанностей*, причем в двух видах: статическом и динамическом.

*Статическое разделение обязанностей* налагает ограничения на приписывание пользователей ролям. В простейшем случае членство в некоторой роли запрещает приписывание пользователя определенному множеству других ролей. В общем случае данное ограничение задается как пара «множество ролей – число» (где множество состоит, по крайней мере, из двух ролей, а число должно быть больше 1), так что никакой пользователь не может быть приписан указанному (или большему) числу ролей из заданного множества. Например, может существовать пять бухгалтерских ролей, но политика безопасности допускает членство не более чем в двух таких ролях (здесь 3).

При наличии наследования ролей ограничение приобретает несколько более сложный вид, но суть остается простой: при проверке членства в ролях нужно учитывать приписывание пользователей ролям-наследницам.

*Динамическое разделение обязанностей* отличается от статического только тем, что рассматриваются роли, одновременно активные (быть может, в разных сеансах) для данного пользователя, а не те, которым пользователь статически приписан. Например, один пользователь может играть роль и кассира, и контролера, но не одновременно; чтобы стать контролером, он должен сначала закрыть кассу. Тем самым реализуется так называемое *временное ограничение доверия*, являющееся аспектом минимизации привилегий.

Рассматриваемый проект стандарта содержит спецификации трех категорий функций, необходимых для администрирования РУД:

*Административные функции* (создание и сопровождение ролей и других атрибутов ролевого доступа): создать/удалить роль/пользователя, приписать пользователя/право роли или ликвидировать существующую ассоциацию, создать/удалить отношение наследования между существующими ролями, создать новую роль и сделать ее наследницей/предшественницей существующей роли, создать/удалить ограничения для статического/динамического разделения обязанностей.

*Вспомогательные функции* (обслуживание сеансов работы пользователей): открыть сеанс работы пользователя с активацией подразумеваемого набора ролей; активировать новую роль, деактивировать роль; проверить правомерность доступа.

*Информационные функции* (получение сведений о текущей конфигурации с учетом отношения наследования). Здесь проводится разделение на обязательные и необязательные функции. К числу первых принадлежат получение списка пользователей, приписанных роли, и списка ролей, которым приписан пользователь.

Все остальные функции отнесены к разряду необязательных. Это получение информации о правах, приписанных роли, о правах заданного пользователя (которыми он обладает как

член множества ролей), об активных в данный момент сеанса ролях и правах, об операциях, которые роль/пользователь правомочны совершить над заданным объектом, о статическом/динамическом разделении обязанностей.

### 6.4.3. Регистрация и аудит

*Регистрация* (или протоколирование) представляет собой механизм подотчетности системы ОБИ, фиксирующий все события, касающиеся безопасности, такие как: вход и выход субъектов доступа, запуск и завершение программ, выдача печатных документов, попытки доступа к защищаемым ресурсам, изменение полномочий субъектов доступа и статуса объектов доступа и т.д.

Эффективность системы ОБИ принципиально повышается в случае дополнения регистрации *аудитом* — анализом протоколируемой информации. Это позволяет оперативно выявлять нарушения, определять слабые места в системе защите, анализировать закономерности системы, оценивать работу пользователей и т.д.

Реализация механизма регистрации и аудита преследует следующие цели:

обеспечение подотчетности пользователей и администраторов;

обеспечение возможности реконструкции последовательности событий;

обнаружение попыток нарушений информационной безопасности;

предоставление информации для выявления и анализа проблем.

Кроме того, механизм регистрации и аудита является психологическим средством, напоминающим потенциальным нарушителям о неотвратимости возмездия за проступки и оплошности.

Практическими средствами регистрации и аудита могут быть следующие:

различные системные утилиты и прикладные программы,

регистрационный (системный или контрольный) журнал.

Первое средство является обычно дополнением к мониторингу, осуществляемого администратором системы. Комплексный подход к протоколированию и аудиту обеспечивается при использовании регистрационного журнала.

*Регистрационный журнал* — это хронологически упорядоченная совокупность записей результатов деятельности субъектов системы, достаточная для восстановления, просмотра и анализа последовательности действий, окружающих или приводящих к выполнению операций, процедур или совершению событий при транзакции с целью контроля конечного результата. Типовая запись регистрационного журнала включает в себя:

тип записи,

дата,

время,

терминал,

пользователь,

событие,

результат.

Процесс ведения регистрационного журнала состоит из четырех этапов:

Сбор и хранение;

Защита;

Интеграция;

Анализ.

На первом этапе определяются данные, подлежащие сбору и хранению, период чистки и архивации журнала, степень централизации управления, место и средства хранения журнала, возможность регистрации шифрованной информации и др.

Регистрируемые данные должны быть защищены, в первую очередь от несанкционированной модификации и, возможно, раскрытия. Дополнительные требования по безопасности определяются концентрацией информации обо всей АС, множеством сегментов АС с различными уровнями доступа, разницей зон административной ответственности и др.

Этап интеграции необходим для объединения и согласования форматов регистрируемых данных из различных систем. Некоторые системы не имеют механизмов контроля и регистрации данных. Возможно, здесь придется разработать программы дополнительного контроля данных и программы трансформации данных в единый формат.

Самым важным этапом является анализ регистрационной информации. Известны несколько методов анализа информации с целью выявления НСД.

*Статистические методы*. Здесь накапливается среднестатистические параметры функционирования подсистем (исторический профиль трафика) и сравниваются с текущими. Наличие определенных отклонений может сигнализировать о возможности появления некоторых угроз. Например, так выявляются: сбои в работе сервера из-за лавинного потока запросов, быстро распространяемый компьютерный вирус, нарушитель, маскирующиеся под легального пользователя, но ведущий себя иначе («маскарад») и др.

*Эвристические методы*. В данном случае в логических правилах системы поддержки принятия решений закодированы известные сценарии НСД, характеристики наблюдаемой системы, сигнализирующие о нарушениях, или модели действий, по совокупности приводящие к НСД. Понятно, что данные методы идентифицируют только известные угрозы, определенные в базе знаний системы поддержки принятия решений.

Аудиту информационной безопасности посвящен второй раздел работы (см. ниже).

### 6.4.4. Криптография

В этом пункте будут рассмотрены криптографические сервисы безопасности, точнее, элементарные сведения, помогающие составить общее представление о компьютерной криптографии и ее месте в общей архитектуре информационных систем.

Криптография необходима для реализации, по крайней мере, трех сервисов безопасности:

шифрование;

контроль целостности;

аутентификация (этот сервис был рассмотрен ранее).

**Шифрование**

*Шифрование* – наиболее мощное средство обеспечения конфиденциальности. Во многих отношениях оно занимает центральное место среди программно-технических регуляторов безопасности, являясь основой реализации многих из них, и в то же время последним (а подчас и единственным) защитным рубежом. Например, для портативных компьютеров только шифрование позволяет обеспечить конфиденциальность данных даже в случае кражи.

В большинстве случаев и шифрование, и контроль целостности играют глубоко инфраструктурную роль, оставаясь прозрачными и для приложений, и для пользователей. Типичное место этих сервисов безопасности – на сетевом и транспортном уровнях реализации стека сетевых протоколов.

Различают два основных метода шифрования:

симметричный,

асимметричный.

При *симметричном* шифровании один и тот же ключ (хранящийся в секрете) используется и для зашифрования, и для расшифрования данных. Разработаны весьма эффективные (быстрые и надежные) методы симметричного шифрования. Национальный стандарт на подобные методы – ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».

Основным недостатком симметричного шифрования является то, что секретный ключ должен быть известен и отправителю, и получателю. С одной стороны, это создает новую проблему распространения ключей. С другой стороны, получатель на основании наличия зашифрованного и расшифрованного сообщения не может доказать, что он получил это сообщение от конкретного отправителя, поскольку такое же сообщение он мог сгенерировать самостоятельно.

В *асимметричных* методах используются два ключа. Один из них, несекретный (он может публиковаться вместе с другими открытыми сведениями о пользователе), применяется для шифрования, другой (секретный, известный только получателю) – для расшифрования. Самым популярным из асимметричных является метод RSA (Райвест,

Шамир, Адлеман), основанный на операциях с большими (скажем, 100-значными) простыми числами и их произведениями.

Существенным недостатком асимметричных методов шифрования является их низкое быстродействие, поэтому данные методы приходится сочетать с симметричными (асимметричные методы на 3 – 4 порядка медленнее). Так, для решения задачи эффективного шифрования с передачей секретного ключа, использованного отправителем, сообщение сначала симметрично зашифровывают случайным ключом, затем этот ключ зашифровывают открытым асимметричным ключом получателя, после чего сообщение и ключ отправляются по сети [3].

**Контроль целостности**

Криптографические методы позволяют надежно контролировать целостность как отдельных порций данных, так и их наборов (таких как поток сообщений); определять подлинность источника данных; гарантировать невозможность отказаться от совершенных действий – «неотказуемость».

В основе криптографического контроля целостности лежат два понятия:

хэш-функция;

электронная цифровая подпись (ЭЦП).

*Хэш-функция* – это трудно обратимое преобразование данных (односторонняя функция), реализуемое, как правило, средствами симметричного шифрования со связыванием блоков. Результат шифрования последнего блока (зависящий от всех предыдущих) и служит результатом хэш-функции.

Пусть имеются данные, целостность которых нужно проверить, хэш-функция и ранее вычисленный результат ее применения к исходным данным (так называемый дайджест). Обозначим хэш-функцию через h, исходные данные – через T, проверяемые данные – через T'. Контроль целостности данных сводится к проверке равенства h(T') = h(T). Если оно выполнено, считается, что T' = T. Совпадение дайджестов для различных данных называется коллизией. В принципе, коллизии, конечно, возможны, поскольку мощность множества дайджестов меньше, чем мощность множества хэшируемых данных, однако то, что h есть функция односторонняя, означает, что за приемлемое время специально организовать коллизию невозможно.

Два российских стандарта, ГОСТ Р 34.10-94 «Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма» и ГОСТ Р 34.11-94 «Функция хэширования», объединенные общим заголовком «Информационная технология. Криптографическая защита информации», регламентируют вычисление дайджеста и реализацию ЭЦП. В сентябре 2001 года был утвержден, а 1 июля

2002 года вступил в силу новый стандарт ЭЦП – ГОСТ Р 34.10-2001, разработанный специалистами ФАПСИ.

### 6.4.5. Экранирование

Механизмом обеспечения целостности данных в информационно-вычислительных сетях является *экранирование*, выполняющее функции разграничения информационных потоков на границе защищаемой сети. С одной стороны, это повышает безопасность объектов внутренней сети за счет игнорирования неавторизованных запросов из внешней среды. Указанное уменьшает уязвимость внутренних объектов потому, что сторонний нарушитель должен преодолеть некоторый защитный барьер — *межсетевой экран*, в котором механизмы ОБИ сконфигурированы особо тщательно и жестко. С другой стороны, экранирование позволяет контролировать информационные потоки, исходящие во внешнюю среду, что повышает режим конфиденциальности АС. Кроме функций разграничения доступа, экранирование обеспечивает регистрацию информационных обменов.

Функции экранирования выполняет *межсетевой экран* или *брандмауэр* (firewall), под которым понимают программную или программно-аппаратную систему, которая выполняет контроль информационных потоков, поступающих в АС и/или выходящих из АС, и обеспечивает защиту АС посредством фильтрации информации. Фильтрация информации состоит в анализе информации по совокупности критериев и принятии решения о ее распространении в/из АС.

В общем случае межсетевой экран выполняет свои функции, контролируя все информационные потоки между двумя сегментами сети или сетями.

Межсетевые экраны классифицируют следующим образом:

на внешние и внутренние, обеспечивающие защиту соответственно от внешней сети или защиту между сегментами сети,

по уровню фильтрации, соответствующему эталонной модели OSI/ ISO.

Говоря о внешних и внутренних сетевых экранах, следует отметить следующее. *Внешние* обычно имеют дело только с протоколом TCP/IP сети Internet. Для *внутренних* сетевых экранов может иметь место многопротокольность.

Работа всех межсетевых экранов основана на использовании информации разных уровней модели OSI (таблица 6.4). Как правило, чем выше уровень модели OSI, на котором межсетевой экран фильтрует пакеты, тем выше обеспечиваемый им уровень защиты.

Межсетевые экраны разделяют на четыре типа:

межсетевые экраны с фильтрацией пакетов;

шлюзы сеансового уровня;

шлюзы прикладного уровня;

межсетевые экраны экспертного уровня.

Таблица 6.4. Типы межсетевых экранов и уровни модели ISO/OSI

| Уровень модели OSI | Протоколы Internet | Тип межсетевого экрана |
|---|---|---|
| Прикладной | Telnet, FTP, DNS, NFS, PING, SMTP, HTTP | Шлюз прикладного уровня<br>Межсетевой экран экспертного уровня |
| Представления данных | | |
| Сеансовый | TCP, UDP | Шлюз сеансового уровня |
| Транспортный | TCP, UDP | |
| Сетевой | IP, ICMP | Межсетевой экран с фильтрацией пакетов |
| Канальный | | |
| Физический | | |

1. *Межсетевые экраны с фильтрацией пакетов* (packet-filtering firewall) представляют собой маршрутизаторы или работающие на сервере программы, сконфигурированные таким образом, чтобы фильтровать входящие и исходящие пакеты. Поэтому такие экраны называют иногда пакетными фильтрами. Фильтрация осуществляется путем анализа IP-адреса источника и приемника, а также портов входящих TCP- и UDP-пакетов и сравнением их с сконфигурированной таблицей правил.

Данные системы просты в использовании, дешевы, оказывают минимальное влияние на производительность АС. Основным недостатком является их уязвимость для IP-спуфинга - замены адресов IP. Кроме того, они сложны при конфигурировании: для их установки требуется знание сетевых, транспортных и прикладных протоколов.

2. *Шлюзы сеансового уровня* (circuit-level gateway) контролируют допустимость *сеанса* связи. Они следят за подтверждением (квитированием) связи между авторизованным клиентом и внешним хостом (и наоборот), определяя, является ли запрашиваемый сеанс связи допустимым. При фильтрации пакетов шлюз сеансового уровня основывается на информации, содержащейся в заголовках пакетов сеансового уровня протокола TCP, т. е. функционирует на два уровня выше, чем межсетевой экран с фильтрацией пакетов. Кроме того, указанные системы обычно имеют функции трансляции сетевых адресов, которая скрывает внутренние IP-адреса, т.е. исключают IP-спуфинг. Однако, т.к. системы контролируют пакеты только на сеансовом уровне, то и отсутствует контроль содержимого пакетов, генерируемых различными службами. Для исключения указанного недостатка применяются шлюзы прикладного уровня.

3. *Шлюзы прикладного уровня* (application-level gateway) проверяют содержимое каждого проходящего через шлюз пакета и могут фильтровать отдельные виды команд или информации в протоколах прикладного уровня, которые им поручено обслуживать. Это более совершенный и надежный тип брандмауэра, использующий программы-посредники (proxies) прикладного уровня или агенты. Агенты составляются для конкретных служб Internet (HTTP, FTP, telnet и т.д.) и служат для проверки сетевых пакетов на наличие достоверных данных. Однако шлюзы прикладного уровня снижают уровень производительности системы из-за повторной обработки в программе-посреднике. Это незаметно при работе в Internet из-за узости каналов связи, но существенно при работе во внутренней сети - Intranet. К недостаткам можно добавить необходимость (а значит и дополнительные временные и экономические затраты) в разработке новых программ-посредников при внедрении новой службы Internet.

4. *Межсетевые экраны экспертного уровня* (stateful inspection firewall) сочетают в себе элементы всех трех описанных выше категорий. Как и межсетевые экраны с фильтрацией пакетов, они работают на сетевом уровне модели OSI, фильтруя входящие и исходящие пакеты на основе проверки IP-адресов и номеров портов. Межсетевые экраны экспертного уровня также выполняют функции шлюза сеансового уровня, определяя, относятся ли пакеты к соответствующему сеансу. И наконец, брандмауэры экспертного уровня берут на себя функции шлюза прикладного уровня, оценивая содержимое каждого пакета в соответствии с политикой безопасности, выработанной в конкретной организации.

Специфика указанных межсетевых экранов состоит в том, что для обеспечения защиты они перехватывают и анализируют каждый пакет на прикладном уровне модели OSI. Вместо применения связанных с приложениями программ-посредников, брандмауэры экспертного уровня используют *специальные алгоритмы распознавания и обработки данных* на уровне приложений. С помощью этих алгоритмов пакеты сравниваются с известными шаблонами данных, что, теоретически, должно обеспечить более эффективную фильтрацию пакетов.

Поскольку брандмауэры экспертного уровня допускают прямое соединение между авторизованным клиентом и внешним хостом, то они оказывают меньшее влияние на производительность, чем шлюзы прикладного уровня. Спорным остаются вопрос: обеспечивают они меньшую безопасность АС по сравнению со шлюзами прикладного уровня или нет [2].

### 6.4.6. Антивирусная защита

Известно, что нельзя добиться 100 %-ой защиты ПК от компьютерных вирусов отдельными программными средствами. Поэтому для уменьшения потенциальной опасности внедрения компьютерных вирусов и их распространения по корпоративной сети необходим комплексный подход, сочетающий различные административные меры, программно-

технические средства антивирусной защиты, а также средства резервирования и восстановления. Делая акцент на программно-технических средствах, можно выделить три основных уровня антивирусной защиты:

Поиск и уничтожение известных вирусов.

Поиск и уничтожение неизвестных вирусов.

Блокировка проявления вирусов.

Поиск и уничтожение известных вирусов

При поиске и уничтожении известных вирусов наиболее распространенным является *метод сканирования*. Указанный метод заключается в выявлении компьютерных вирусов по их уникальному фрагменту программного кода (сигнатуре, программному штамму). Для этого создается некоторая *база данных сканирования* с фрагментами кодов известных компьютерных вирусов. Обнаружение вирусов осуществляется путем сравнения данных памяти компьютера с фиксированными кодами базы данных сканирования. В случае выявления и идентификации кода нового вируса, его сигнатура может быть введена в базу данных сканирования. В виду того, что сигнатура известна, то существует возможность корректного восстановления (обеззараживания) зараженных файлов и областей. Следует добавить, что некоторые системы хранят не сами сигнатуры, а, например, контрольные суммы или имитоприставки сигнатур.

Антивирусные программы, выявляющие известные компьютерные вирусы, называются *сканерами* или *детекторами*. Программы, включающие функции восстановления зараженных файлов, называют *полифагами* (фагами), докторами или дезинфекторами. Примером сканера-полифага является знакомая программа Aidstest.

Принято разделять сканеры на следующие:

*транзитные*, периодически запускаемые для выявления и ликвидации вирусов,

*резидентные* (постоянно находящиеся в оперативной памяти), проверяющие заданные области памяти системы при возникновении связанных с ними событий (например, проверка файла при его копировании или переименовании).

К недостаткам сканеров следует отнести то, что они позволяют обнаружить вирусы, которые уже проникали в вычислительные системы, изучены и для них определена сигнатура. Для эффективной работы сканеров необходимо оперативно пополнять базу данных сканирования. Однако с увеличением объема базы данных сканирования и числа различных типов искомых вирусов снижается скорость антивирусной проверки. Само собой, если время сканирования будет приближаться ко времени восстановления, то необходимость в антивирусном контроле может стать не столь актуальной.

Некоторые вирусы (мутанты и полиморфные) кодируют или видоизменяют свой программный код. Это затрудняет или делает невозможным выделить сигнатуру, а следовательно, обнаружить вирусы методом сканирования.

Для выявления указанных маскирующихся вирусов используются специальные методы. К ним можно отнести метод эмуляции процессора. Метод заключается в имитации выполнения процессором программы и подсовывания вирусу фиктивных управляющих ресурсов. Обманутый таким образом вирус, находящийся под контролем антивирусной программы, расшифровывает свой код. После этого, сканер сравнивает расшифрованный код с кодами из своей базы данных сканирования.

**Поиск и уничтожение неизвестных вирусов**

Выявление и ликвидация неизвестных вирусов необходимы для защиты от вирусов, пропущенных на первом уровне антивирусной защиты. Наиболее эффективным методом является контроль целостности системы (обнаружение изменений). Данный метод заключаются в проверке и сравнении текущих параметров вычислительной системы с эталонными, соответствующими ее незараженному состоянию. Понятно, что контроль целостности не являются прерогативой исключительно системы антивирусной защиты. Он обеспечивает защищенность информационного ресурса от несанкционированных модификации и удаления в результате различного рода нелегитимных воздействий, сбоев и отказов системы и среды.

Для реализации указанных функций используются программы, называемые *ревизорами*. Работа ревизора состоит из двух этапов: фиксирование эталонных характеристик вычислительной системы (в основном диска) и периодическое сравнение их с текущими характеристиками. Обычно контролируемыми характеристиками являются контрольная сумма, длина, время, атрибут “только для чтения” файлов, дерево каталогов, сбойные кластеры, загрузочные сектора дисков. В сетевых системах могут накапливаться среднестатистические параметры функционирования подсистем (в частности исторический профиль сетевого трафика), которые сравниваются с текущими.

Ревизоры, как и сканеры, делятся на транзитные и резидентные.

К недостаткам ревизоров, в первую очередь резидентных, относят создаваемые ими всякие неудобства и трудности в работе пользователя. Например, многие изменения параметров системы вызваны не вирусами, а работой системных программ или действиями пользователя-программиста. По этой же причине ревизоры не используют для контроля зараженности текстовых файлов, которые постоянно меняются. Таким образом, необходимо соблюдение некоторого баланса между удобством работы и контролем целостности системы.

Ревизоры обеспечивают высокий уровень выявления неизвестных компьютерных вирусов, однако они не всегда обеспечивают корректное лечение зараженных файлов. Для

лечения зараженных файлов неизвестными вирусами обычно используются эталонные характеристики файлов и предполагаемые способы их заражения.

Кроме этого ревизоры не определяют зараженные файлы, создаваемые или копируемые в систему.

Разновидностью контроля целостности системы является метод программного самоконтроля, именуемые вакцинацией. Идея методов состоит в присоединении к защищаемой программе модуля (*вакцины*), контролирующего характеристики программы, обычно ее контрольную сумму.

Помимо статистических методов контроля целостности, для выявления неизвестных и маскирующихся вирусов используются эвристические методы. Они позволяет выявить по известным признакам (определенным в базе знаний системы) некоторые маскирующиеся или новые модифицированные вирусы известных типов. В качестве примера признака вируса можно привести код, устанавливающий резидентный модуль в памяти, меняющий параметры таблицы прерываний и др. Программный модуль, реализующий эвристический метод обнаружения вирусов, называют *эвристическим анализатором*.

К недостаткам эвристических анализаторов можно отнести ошибки 1-го и 2-го рода: ложные срабатывания и пропуск вирусов. Соотношение указанных ошибок зависит от уровня эвристики.

Понято, что если для обнаруженного эвристическим анализатором компьютерного вируса сигнатура отсутствует в базе данных сканирования, то лечение зараженных данных может быть некорректным.

**Блокировка проявления вирусов**

Блокировка проявления вирусов предназначена для защиты от деструктивных действий и размножения компьютерных вирусов, которым удалось преодолеть первые два уровня защиты. Методы основаны на перехвате характерных для вирусов функций. Известны два вида указанных антивирусных средства:

программы-фильтры,

аппаратные средства контроля.

*Программы-фильтры*, называемые также резидентными сторожами и мониторами, постоянно находятся в оперативной памяти и перехватывают заданные прерывания, с целью контроля подозрительной действий. При этом они могут блокировать “опасные” действия или выдавать запрос пользователю.

Действия, подлежащие контролю, могут быть следующими: модификация главной загрузочной записи (MBR) и загрузочных записей логических дисков и ГМД, запись по абсолютному адресу, низкоуровневое форматирование диска, оставление в оперативной

памяти резидентного модуля и др. Как и ревизоры, фильтры часто являются “навязчивыми” и создают определенные неудобства в работе пользователя.

Встроенные аппаратные средства ПК обеспечивают контроль модификации системного загрузчика и таблицы разделов жесткого диска, находящихся в главном загрузочном секторе диска (MBR). Включение указанных возможностей в ПК осуществляется с помощью программы Setup, расположенной в ПЗУ. Следует указать, что программу Setup можно обойти в случае замены загрузочных секторов путем непосредственного обращения к портам ввода-вывода контроллеров жесткого и гибкого дисков.

Наиболее полная защита от вирусов может быть обеспечена с помощью специальных контроллеров аппаратной защиты. Такой контроллер подключается к ISA-шине ПК и на аппаратном уровне контролирует *все* обращения к дисковой подсистеме компьютера. Это не позволяет вирусам маскировать себя. Контроллер может быть сконфигурирован так, чтобы контролировать отдельные файлы, логические разделы, “опасные” операции и т.д. Кроме того, контроллеры могут выполнять различные дополнительные функции защиты, например, обеспечивать разграничение доступа и шифрование.

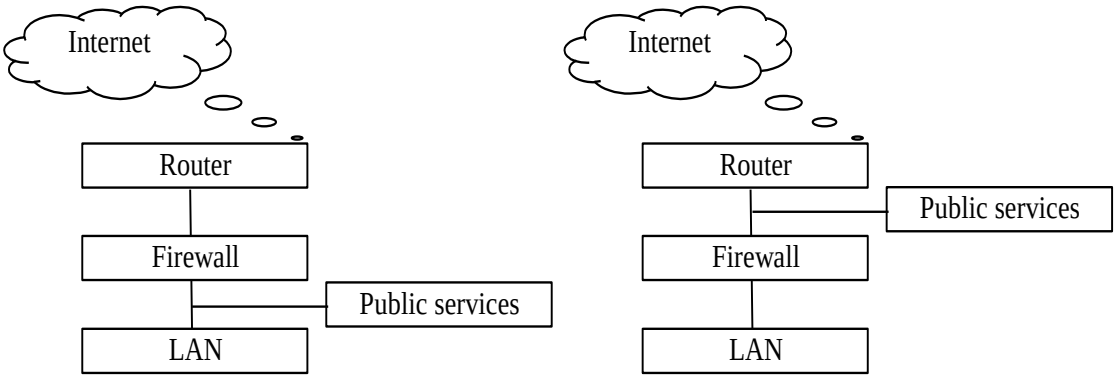
К недостаткам указанных контроллеров, как ISA-плат, относят отсутствие системы авто конфигурирования, и как следствие, возможность возникновения конфликтов с некоторыми системными программами, в том числе антивирусными [2].

### 6.5. Модель безопасности информационной сети предприятия

В данном разделе будет рассмотрен один из возможных вариантов построения защищенной информационной сети предприятия на базе компьютерного оборудования и программных средств.

Компьютерная сеть предприятия малого/среднего бизнеса включает в себя несколько локальных сетей объединенных в единую сеть организации и функционирующих как единое целое. Как правило, сеть включает в себя различного рода коммутационное оборудование, такое как маршрутизатор, хосты, коммутаторы, сетевые карты и т.д., а также всевозможные сервисы и программы.

Из предыдущего раздела известно, что в качестве первого рубежа защиты сети, от угроз из Internet, служит межсетевой экран. В общем случае существует два варианта постановки экрана в сеть, эти варианты приведены на рисунке 6.8.




а) Простое включение МЭ

б) Подключение МЭ с вынесением общедоступных серверов

Рис. 6.8. Варианты постановки МЭ в сеть

Наиболее простым является решение, при котором межсетевой экран просто экранирует локальную сеть от глобальной (6.8а). При этом публичные сервисы (Public services: WWW, FTP, e-mail) оказываются защищены межсетевым экраном. Требуется уделить много внимания на предотвращение проникновения на защищаемые станции локальной сети при помощи средств легкодоступных публичных серверов.

Для предотвращения доступа в локальную сеть, используя ресурсы публичных серверов, рекомендуется общедоступные серверы подключать перед межсетевым экраном, так как показано на рисунке 6.8б. Данный способ обладает более высокой защищенностью локальной сети, но низким уровнем защищенности общедоступных серверов.

Экскурс в технологию WWW. WWW представляет собой клиент-серверную технологию, основанную на прикладном протоколе HTTP. В нем имеется два вида сообщений: запросы от клиента к серверу и ответы сервера клиенту. Для передачи сообщений используется протокол TCP, стандартный порт HTTP-сервера – 80.

Очевидно, что не все информационные ресурсы WWW могут быть открыты для всеобщего просмотра. Для того чтобы ограничить доступ к какому-либо ресурсу, используется аутентификация клиента, т.е. клиент должен предоставить имя пользователя и пароль, прежде чем его пароль будет обслужен HTTP-сервером.

Почтовый сервис (e-mail) использует протоколы: SMPT (Simple Mail Transfer Protocol) и POP3 (Post Office Protocol).

Главной целью протокола SMTP служит надежная и эффективная доставка электронных почтовых сообщений. SMTP является довольно независимой системой и требует только надежного канала связи. Средой для SMTP может служить отдельная локальная сеть, система сетей или весь Internet.

SMTP базируется на следующей модели коммуникаций: в ответ на запрос пользователя почтовая программа-отправитель устанавливает двухстороннюю связь с программой-приемником (TCP, порт 25). Получателем может быть оконечный или промежуточный адресат. SMTP-команды генерируются отправителем и посылаются получателю. На каждую команду должен быть отправлен и получен отклик.

В некоторых небольших узлах Internet бывает непрактично поддерживать систему передачи сообщений MTS (Message Transport System). Рабочая станция может не иметь достаточных ресурсов для обеспечения непрерывной работы SMTP-сервера. Для “домашних ЭВМ” слишком дорого поддерживать связь с Internet круглые сутки.

POP3 обеспечивает доступ к электронной почте малых узлов и индивидуальных ЭВМ. Этот протокол обеспечивает доступ узла к базовому почтовому серверу. POP3 получает и стирает почтовые сообщения. Когда пользователь ЭВМ-клиента хочет послать сообщение, он устанавливает SMTP связь с почтовым сервером непосредственно и посылает все, что нужно через него. При этом ЭВМ POP3-сервер не обязательно является почтовым сервером. В исходный момент ЭВМ POP3-сервер прослушивает TCP-порт 110. Если ЭВМ-клиент хочет воспользоваться услугами POP3-сервера, то устанавливает с ним TCP связь. По установлении связи POP3-сервер посылает клиенту уведомление и сессия переходит в фазу авторизации. После этого может производиться обмен командами и откликами.

Преследуя своей целью защитить активы внутренней сети организации, а так же не загружать firewall – поставим экран после публичных сервисов.

Система защиты информации на уровне “периметра”, кроме межсетевого экрана, включает в себя такие защитные средства (Security services):

автоматизированное рабочее место администратора,

антивирусный шлюз,

сервер аудита безопасности системы,

средства адаптивного управления безопасностью ANS (Adaptive Network Security) и обнаружения атак IDS (Intrusion Detection System),

средства проверки почты,

и др.

В качестве внутреннего сервиса выступает сервис распределенных баз данных.

Разбивка сети на сегменты достигается за счет коммутатора (Switch), посредствам которого так же осуществляется доступ/запрет:

из одного локального сегмента в другой,

из внутренней сети к внутренним сервисам (например, к распределенной базе данных предприятия),

из внутренней сети к публичным сервисам,

из внутренней сети в Internet.

Благодаря коммутатору можно задавать любую политику безопасности.

Описанная структура информационной сети организации представлена на рисунке 6.9.

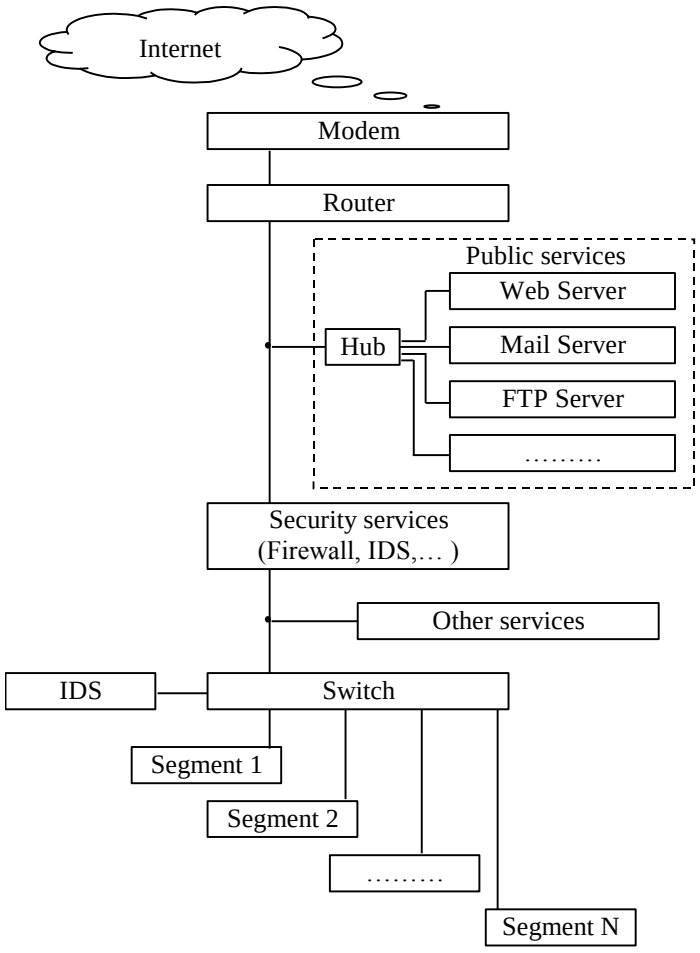



Рис. 6.9. Модель безопасности информационной сети предприятия

### 6.6.Типовая политика безопасности предприятия малого и среднего бизнеса – комплект документов и инструкций

Для модели безопасности информационной сети предприятия, представленной в предыдущем пункте (рисунок 6.9) необходимо предоставить:

Типовую политику безопасности.

Типовые документы и инструкции.

Основные средства, методы и элементы информационной защиты.

#### 6.6.1. Типовая политика безопасности

Типовая политика безопасности разработана для организации, имеющей выход в Internet и обладающая ресурсами, к которым необходим доступ из Internet.

**Сетевая безопасность**

Доступ из Internet в корпоративную сеть компании:

Доступ во внутреннюю сеть извне запрещен.

Доступ к межсетевому экрану извне запрещен.

Доступ к следующим сервисам: антивирусному шлюзу, серверу аудита безопасности системы, средствам адаптивного управления безопасностью и обнаружения атак, средствам проверки почты доступ извне запрещен.

Доступ к WWW, FTP, e-mail сервисам извне разрешен по следующим правилам.

Для WWW сервиса:

доступ извне разрешен всем только к 80 порту,

доступ администратора WWW-сервера разрешен только из сегмента административного управления при прохождении процедуры аутентификации/идентификации на firewall.

Для e-mail сервера:

разрешен доступ из внутренней сети компании к POP3-сервису через 110 порт,

разрешен доступ из внутренней сети компании к SMTP-сервису через 25 порт.

Межсетевой экран:

Firewall администрируется только локально с автоматизированного рабочего места администратора сети (процедура администрирования возможна при прохождении аутентификации/идентификации пользователем (администратором)). Регулярно ставятся и обновляются антивирусные программы и необходимые патчи, поддерживается максимально безопасная конфигурация операционной системы.

Средства адаптивного управления безопасностью:

Система анализа защищенности (Internet Scanner) администрируется локально с автоматизированного рабочего места администратора сети. Анализ всесторонних и/или выборочных тестов операционных систем, используемого прикладного ПО, маршрутизатора, межсетевого экрана, всех серверов и т.д., производится администратором безопасности регулярно (раз в неделю).

Система обнаружения атак IDS служащая для автоматической реконфигурации межсетевого экрана в случае обнаружения атак. Сервис контролирует весь входящий трафик из сети Internet.

Средства протоколирования:

Ведутся специальные файлы.

на межсетевом экране ведется запись в лог-файл обо всех обращениях и попытках связи (удачных и нет) из корпоративной сети и в корпоративную сеть,

система обнаружения атак запоминает все атаки и подозрительные активности (так же в лог-файле),

на Web-сервисе храниться информация обо всех посетителях (лог-файл),

администратор безопасности должен вести файл, содержащий информацию обо всех изменениях и попытках изменить информацию в лог-файлах предыдущих сервисов.

Коммутатор (Switch):

разрешен доступ из всех сегментов сети к Internet без ограничений,

доступ из сетей пользователей в сети администраторов (управления, безопасности) запрещен.

Локальная безопасность

Локальная безопасность направлена на защиту каждого компьютера сети.

Антивирусный контроль:

Антивирусный контроль на всех рабочих станциях.

Защита от НСД:

Необходимо поставить систему защиты от НСД, которая должна контролировать и разграничивать доступ к каждой рабочей станции и серверу. Система должна быть:

при загрузке идентификация простого пользователя должна производиться при помощи при помощи пароля,

блокировать доступ в setup всех рабочих станций и серверов всем пользователям кроме администратора,

блокировать компьютер, в случае если пользователь покинул свое место.

Криптографическая защита данных:

Сотрудники компании должны сохранять информацию начиная с уровня “строго конфиденциально» (см. п.6.2) на специальном криптодиске.

Защита персональным firewall:

Все рабочие станции должны быть защищены персональным firewall (реализованным программно).

Резервирование данных

Обязательным является резервирование пользователями важных данных на персональных компьютерах на внутреннем сервере данных компании.

Протоколирование доступа:

При локальном доступе пользователя к рабочей станции (администратора к серверам) ведется лог-файл его посещений (протоколируются все удачные и неудачные попытки входа в систему).

**Физическая безопасность**

Все сервисы безопасности и данных должны находится в отдельном помещении, доступ в которое разрешен только администраторам (у которых есть ключ или магнитная карта к этой комнате).

Необходимо введение отдельной должности администратора безопасности, все изменения в системах ИТ – администратор и администратор безопасности будут делать в паре (пароль разбит на две части: по одному сегменту на специалиста).

Помещение должно быть оборудовано принудительной вентиляцией и пожарной защитой (полуавтоматической или автоматической), возможно, видео наблюдением за действиями администраторов.

Необходимо контролировать поток служащих и посетителей компании (либо по специальным пропускам, либо по магнитным картам).

### 6.6.2. Типовые документы и инструкции

В соответствии с рекомендациями Британского стандарта BS 7799:1995 включим в документ, характеризующий политику безопасности организации, следующие разделы:

1 Вводный раздел.

2 Организационный раздел.

3 Классификационный.

4 Штатный раздел.

5 Раздел инструкций и требований по обеспечению внутренней информационной безопасности компании.

Соответствие четырех уровневой модели обеспечения безопасности информационной сети предприятия. Первые три раздела соответствуют административному уровню защиты информации, четвертый раздел – процедурному уровню, а программно-техническому уровню соответствует пятый раздел документов.

Ранее говорилось, что ПБ состоит из двух (трех) уровней, чем больше предприятие, тем сложнее структура политики. Для малого и среднего бизнеса достаточно привести двухуровневую структуру политики безопасности, назовем условно верхний уровень «административным», а нижний «техническим». Таким образом, в «административный» раздел войдут документы вводного, организационного, классификационного и штатного разделов. «Технический» раздел охватит свод правил, инструкций и требований по обеспечению информационной безопасности организации.

**Вводный раздел**

Позиция администрации предприятия по вопросу защиты информационных активов:

Надежное функционирование информационной компьютерной сети предприятия является частью производственного процесса. Защита информационных активов предприятия необходима.

Типовые цели предприятия в области защиты информации:

Приоритетной целью любого предприятия является обеспечение целостности, конфиденциальности, доступности информации. В качестве частных целей:

следование экономической целесообразности в выборе защитных мер,

обеспечение подотчетности всех действий пользователей с информационными ресурсами и анализа регистрационной информации,

и др.

**Организационный раздел**

Данный раздел включает описание всех групп пользователей имеющих отношение к работам в области информационной безопасности. В принципе данную формулировку можно трактовать по-разному, так как каждый пользователь сети так или иначе несет ответственность за некоторую часть производственной информации, с которой он работает. В таком контексте данный документ можно рассматривать как положение о категорировании пользователей автоматизированной системы.

Этот документ также может содержать положение о категорировании ресурсов.

Положение о категорировании пользователей АС:

В АС входят следующие группы пользователей:

Группа Администраторы. В нее входят администраторы информационных технологий и безопасности. Администраторы имеют полный доступ к ресурсам АС для ее администрирования.

Группа Топ-менеджеры. В группу входят: президент компании, генеральный директор, технический директор, заместители и т.д.

Группа Сотрудники. В группу входят все сотрудники компании (экономисты, бухгалтеры, сотрудники отдела кадров, …).

Каждая группа пользователей обладает различными правами доступа к информации различного уровня секретности. Уровень секретности определяется положением о категорировании ресурсов организации.

Положение о категорировании ресурсов:

В компании вводятся следующие уровни категорий секретности информации:

общедоступно,

конфиденциально,

строго конфиденциально,

секретно.

Сотрудникам компании строго запрещается разглашать кому-либо информацию, начиная с уровня «конфиденциально».

Общедоступной информацией является информация, уже опубликованная в средствах массовой информации, а также на Web-сайте компании. Решение о придании статуса «Общедоступно» принимает генеральный или технический директор.

Конфиденциальной информацией в компании является любая внутренняя информация компании (служебная, штатная,…).

Строго конфиденциальной информацией в компании является:

коммерческая информация (тексты договоров и соглашений с партнерами и клиентами),

техническая информация (тексты отчетов, ТЗ, значимые документы, продукты, ключи лицензирования и т.д.).

Решение о придание статуса «Строго конфиденциально» коммерческой информации принимает генеральный директор. Решение о придание статуса «Строго конфиденциально» технической информации принимает технический директор.

Порядок обращения с информацией, подлежащей защите

Должны быть четко описаны и классифицированы следующие действия с информацией:

1. копирование;

2. хранение;

3. передача почтой, факсом, е-мейлом;

4. передача голосом, включая мобильные телефоны, голосовую почту;

5. уничтожение.

1. Информация уровня «общедоступно». Доступ, копирование и любая передача информации данного уровня не ограничены. Уничтожение информации возможно только ее владельцем.

2. Информация уровня «конфиденциально». Подлежит защите от НСД средствами разграничения доступа.

Доступ к данной информации может осуществляться сотрудниками компании локально и удаленно. Удаленный доступ из корпоративной сети осуществляется без применения средств шифрования трафика. Удаленный доступ из Internet осуществляется с применением средств шифрования трафика.

Доступ к информации уровня «конфиденциально» осуществляется категориями пользователей: Администраторы, Топ-менеджеры, Сотрудники.

Копирование и любая передача информации данного уровня ограничены периметром компании. Уничтожение информации возможно только ее владельцем.

3. Информация уровня «строго конфиденциально». Подлежит защите от НСД средствами разграничения доступа и криптографической защите.

Удаленный доступ из корпоративной сети осуществляется с применением средств шифрования трафика. Удаленный доступ сотрудников из Internet осуществляется с применением средств шифрования трафика. Копирование и любая передача информации данного уровня возможно только в пределах компании и только авторизованным персонам. Уничтожение информации возможно только ее владельцем.

Право на удаление информации уровня “секретно” имеет только администратор безопасности вместе с ИТ – администратором (пароль разделен на две части между ними) с разрешения тех. Директора.

Доступ к информации уровня «строго конфиденциально» осуществляется категориями пользователей: Топ-менеджеры, Сотрудники (с разрешения тех. директора).

4. Информация уровня «секретно» подлежит защите от НСД, криптографической защите и обязательному протоколированию доступа.

Удаленный доступ из корпоративной сети осуществляется с применением средств шифрования трафика. Удаленный доступ из Internet запрещен. Копирование и любая передача информации данного уровня возможно только в пределах компании и только авторизованным персонам. Уничтожение информации возможно только ее владельцем.

Право на удаление информации уровня «секретно» имеет только администратор безопасности вместе с ИТ-администратором администратором (пароль разделен на две части между ними) с разрешения тех. директора.

Доступ к информации уровня «строго конфиденциально» осуществляется категориями пользователей: Топ-менеджеры.

**Классификационный раздел**

Данный раздел описывает имеющиеся в организации материальные, информационные ресурсы и необходимый уровень их защиты.

В качестве материальных ресурсов могут выступать элементы, описанные выше. В проекции на организацию с моделью безопасности информационной сети (рисунок 6.9) данный список может принять вид:

Аппаратное обеспечение:

компьютеры,

принтеры,

сканеры,

факсы и телефоны,

коммуникационные линии,

сетевое оборудование (сетевые карты) и их составные части.

Программное обеспечение:

операционные системы: Windows 2000, Server, NT, 98/95 (для рабочих станций),

прикладные программы: офисные приложения (MS Word, MS Excel, …), базы данных (1С, MS Access, Oracle, …), другое (…),

почтовые протоколы POP3, SMTP,

сетевые протоколы: стек TCP/IP,

система анализа защищенности (Internet Scanner),

система обнаружения атак IDS,

…

Информационное обеспечение (вводимые и обрабатываемые, хранимые, передаваемые и резервные (сохранные копии) данные и метаданные):

данные о сотрудниках (информация о личности (ФИО, …), занимаемой должности, правах доступа к информации, заработанной плате, …),

данные о клиентах/партнерах,

данные о соглашениях/контрактах с клиентами/партнерами,

промежуточные данные (при обработке какой бы то ни было информации),

данные о конфигурации системы, используемом оборудовании и программах,

….

Персонал:

обслуживающий персонал (ИТ – администраторы, администраторы безопасности),

пользователи (администрация организации, топ-менеджеры, экономисты, юристы, кладовщики, клиенты,…).

Документация (конструкторская, техническая, пользовательская, …).

Расходные материалы:

бумага,

магнитные носители,

картриджи,

др.

**Штатный раздел**

Данный раздел характеризует меры безопасности, применяемые к персоналу, иначе говоря, эти документы функционируют на процедурном уровне защиты информации. Типовые документы:

Описание должностей с точки зрения информационной безопасности,

Организация обучения и переподготовки персонала,

Порядок реагирования на нарушения режима безопасности и т.п.

Данный уровень был подробно рассмотрен ранее (см. п.3).

Раздел инструкций и требований по обеспечению внутренней

информационной безопасности компании

Приведу перечень всех типовых инструкций:

Правила парольной защиты

Правила защиты от вирусов и злонамеренного программного обеспечения

Требования по контролю за физического доступом

Требования по физической защите оборудования

Инструкция по безопасному уничтожению информации или оборудования

Инструкция по безопасности рабочего места (документов на рабочем столе и на экране монитора)

Правила осуществления удаленного доступа

Правила осуществления локального доступа

Требования резервного сохранения информации

Требования мониторинга и ведения диагностических лог файлов

Требование мониторинга доступа и использования систем и ведения лог файлов

Требования при обращении с носителями данных

Требования по неэлектронному информационному обмену

Требования при регистрации пользователей

Требования по проверке прав пользователей

Требования по контролю доступа в операционную систему

Требование к процедуре входа в систему (log on)

Правила использования системных утилит

Правила удаленной работы мобильных пользователей

Следующие требования должны быть предусмотрены:

Требование распределения ответственности при обеспечении безопасности

Правила безопасности при выборе персонала

Требования контроля оперативных изменений

Требования проверки входных данных

Требования к применению криптографических средств управления

Требования по контролю программ операционной системы

Требования по контролю доступа к исходным текстам программ и библиотек

Требования контроля вносимых изменений

Требование обеспечения непрерывности бизнеса

Требования соблюдения авторского права на программное обеспечение

Требования обеспечения сохранности улик (свидетельств, доказательств)

Требования по управлению системным аудитом

Инструкции

По приему на работу и допуску новых сотрудников к работе в АС и наделения их необходимыми полномочиями по доступу к ресурсам системы.

По увольнению работников и лишения их прав доступа в систему.

По действиям различных категорий персонала, включая сотрудников отдела безопасности информации, по ликвидации последствий кризисных (аварийных или нештатных) ситуаций, в случае их возникновения.

Действия персонала по ликвидации последствий кризисных (аварийных или нештатных) ситуаций в случае их возникновения.

Процедуры контроля в случае инцидентов.

## 7. Контроль безопасности информационной системы

### 7.1. Нормативная база аудита

#### 7.1.1. Законодательство в области аудита безопасности

Наиболее значимыми нормативными документами в области информационной безопасности, определяющими критерии для оценки защищенности АС, и требования, предъявляемые к механизмам защиты, являются:

Общие критерии оценки безопасности информационных технологий (The Common Criteria for Information Technology Security Evaluation/ISO 15408);

Практические правила управления информационной безопасностью (Code of practice for Information Security Management/ISO 17799);

Кроме этого, в нашей стране первостепенное значение имеют Руководящие документы (РД) Гостехкомиссии России. В других странах их место занимают соответствующие национальные стандарты (там, где они есть).

**ISO 15408: Common Criteria for Information Technology Security Evaluation**

Наиболее полно критерии для оценки механизмов безопасности программно-технического уровня представлены в международном стандарте ISO 15408: Common Criteria for Information Technology Security Evaluation (Общие критерии оценки безопасности информационных технологий), принятом в 1999 году.

Общие критерии оценки безопасности информационных технологий (далее «Общие Критерии») определяют функциональные требования безопасности (security functional requirements) и требования к адекватности реализации функций безопасности (security assurance requirements).

При проведении работ по анализу защищенности АС, а также СВТ «Общие критерии» целесообразно использовать в качестве основных критериев, позволяющих оценить уровень защищенности АС (СВТ) с точки зрения полноты реализованных в ней функций безопасности и надежности реализации этих функций.

Хотя применимость «Общих критериев» ограничивается механизмами безопасности программно-технического уровня, в них содержится определенный набор требований к механизмам безопасности организационного уровня и требований по физической защите, которые непосредственно связаны с описываемыми функциями безопасности.

Первая часть «Общих критериев» содержит определение общих понятий, концепции, описание модели и методики проведения оценки безопасности ИТ. В ней вводится понятийный аппарат, и определяются принципы формализации предметной области.

Требования к функциональности средств защиты приводятся во второй части «Общих критериев» и могут быть непосредственно использованы при анализе защищенности для оценки полноты реализованных в АС (СВТ) функций безопасности.

Третья часть «Общих критериев» содержит классы требований гарантированности оценки, включая класс требований по анализу уязвимостей средств и механизмов защиты под названием AVA: Vulnerability Assessment. Данный класс требований определяет методы, которые должны использоваться для предупреждения, выявления и ликвидации следующих типов уязвимостей:

Наличие побочных каналов утечки информации;

Ошибки в конфигурации либо неправильное использование системы, приводящее к переходу в небезопасное состояние;

Недостаточная надежность (стойкость) механизмов безопасности, реализующих соответствующие функции безопасности;

Наличие уязвимостей («дыр») в средствах защиты информации, дающих возможность пользователям получать НСД к информации в обход существующих механизмов защиты.

Соответствующие требования гарантированности оценки содержатся в следующих четырех семействах требований:

Семейство AVA_CCA: Covert Channel Analysis (Анализ каналов утечки информации);

Семейство AVA_MSU: Misuse (Ошибки в конфигурации либо неправильное использование системы, приводящее к переходу системы в небезопасное состояние);

Семейство AVA_SOF: Strength of TOE Security Functions (Стойкость функций безопасности, обеспечиваемая их реализацией);

Семейство AVA_VLA: Vulnerability Analysis (Анализ уязвимостей).

При проведении работ по аудиту безопасности перечисленные семейства требований могут использоваться в качестве руководства и критериев для анализа уязвимостей АС (СВТ).

**ISO 17799: Code of Practice for Information Security Management**

Наиболее полно критерии для оценки механизмов безопасности организационного уровня представлены в международном стандарте ISO 17799: Code of Practice for Information Security Management (Практические правила управления информационной безопасностью), принятом в 2000 году. ISO 17799 является ни чем иным, как международной версией британского стандарта BS 7799.

ISO 17799 содержит практические правила по управлению информационной безопасностью и может использоваться в качестве критериев для оценки механизмов безопасности организационного уровня, включая административные, процедурные и физические меры защиты (об этом упоминалось в первом разделе).

Практические правила разбиты на следующие 10 разделов:

Политика безопасности;

Организация защиты;

Классификация ресурсов и их контроль;

Безопасность персонала;

Физическая безопасность;

Администрирование компьютерных систем и вычислительных сетей;

Управление доступом;

Разработка и сопровождение информационных систем;

Планирование бесперебойной работы организации;

Контроль выполнения требований политики безопасности.

В этих разделах содержится описание механизмов безопасности организационного уровня, реализуемых в настоящее время в правительственных и коммерческих организациях во многих странах мира.

Десять средств контроля, предлагаемых в ISO 17799 (они обозначены как ключевые), считаются особенно важными. Под средствами контроля в данном контексте понимаются механизмы управления информационной безопасностью организации.

При использовании некоторых из средств контроля, например, шифрования данных, может потребоваться оценка рисков, чтобы определить нужны ли они и каким образом их следует реализовывать. Для обеспечения более высокого уровня защиты особенно ценных ресурсов или оказания противодействия особенно серьезным угрозам безопасности в ряде случаев могут потребоваться более сильные средства контроля, которые выходят за рамки ISO 17799.

Десять ключевых средств контроля, перечисленные ниже, представляют собой либо обязательные требования, например, требования действующего законодательства, либо считаются основными структурными элементами информационной безопасности, например, обучение правилам безопасности. Эти средства контроля актуальны для всех организаций и сред функционирования АС и составляют основу системы управления информационной безопасностью. Они служат в качестве основного руководства для организаций, приступающих к реализации средств управления информационной безопасностью.

Ключевыми являются следующие средства контроля:

Документ о политике информационной безопасности;

Распределение обязанностей по обеспечению информационной безопасности;

Обучение и подготовка персонала к поддержанию режима информационной безопасности;

Уведомление о случаях нарушения защиты;

Средства защиты от вирусов;

Планирование бесперебойной работы организации;

Контроль над копированием программного обеспечения, защищенного законом об авторском праве;

Защита документации организации;

Защита данных;

Контроль соответствия политике безопасности.

Процедура аудита безопасности АС включает в себя проверку наличия перечисленных ключевых средств контроля, оценку полноты и правильности их реализации, а также анализ их адекватности рискам, существующим в данной среде функционирования. Составной частью работ по аудиту безопасности АС также является анализ и управление рисками.

**РД Гостехкомиссии России**

В общем случае в нашей стране при решении задач защиты информации должно обеспечиваться соблюдение следующих указов Президента, федеральных законов, постановлений Правительства Российской Федерации, РД Гостехкомиссии России и других нормативных документов (см. также раздел 1):

Доктрина информационной безопасности Российской Федерации;

Указ Президента РФ от 6 марта 1997 г. №188 «Об утверждении перечня сведений конфиденциального характера»;

Закон Российской Федерации «Об информации, информатизации и защите информации» от 20.02.95 N 24-ФЗ;

Закон Российской Федерации «О связи» от 16.02.95 N 15-ФЗ;

Закон Российской Федерации «О правовой охране программ для электронных вычислительных машин и баз данных» от 23.09.92 N3523-1;

Закон Российской Федерации «Об участии в международном информационном обмене» от 04.07.96 N 85-ФЗ;

Постановление Правительства Российской Федерации «О лицензировании отдельных видов деятельности» от 16.09.98г;

Закон Российской Федерации «О государственной тайне» от 21 июля 1993 г;

ГОСТ Р 51583 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении».

Руководящий документ «Положение по аттестации объектов информатизации по требованиям безопасности информации» (Утверждено Председателем Гостехкомиссии России 25.11.1994 г.);

Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация АС и требования к защите информации» (Гостехкомиссия России, 1997);

«Положение о сертификации средств защиты информации по требованиям безопасности информации» (Постановление Правительства РФ 608, 1995 г.);

Руководящий документ «Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации» (Гостехкомиссия России, 1992 г.);

Руководящий документ «Концепция защиты средств вычислительной техники от НСД к информации» (Гостехкомиссия России, 1992 г.);

Руководящий документ «Защита от НСД к информации. Термины и определения» (Гостехкомиссия России, 1992 г.);

Руководящий документ «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД в АС и СВТ» (Гостехкомиссия России, 1992 г.);

Руководящий документ «Средства вычислительной техники. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации» (Гостехкомиссия России, 1997 г.);

Руководящий документ «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия не декларированных возможностей» (Гостехкомиссия России, 1999 г.);

Руководящий документ «Специальные требования и рекомендации по технической защите конфиденциальной информации» (Гостехкомиссия России, 2001г.).

РД Гостехкомиссии России составляют основу нормативной базы в области защиты от НСД к информации в нашей стране. Наиболее значимые из них, определяющие критерии для оценки защищенности АС (СВТ).

Критерии для оценки механизмов защиты программно-технического уровня, используемые при анализе защищенности АС и СВТ, выражены в РД Гостехкомиссии РФ:

«АС. Защита от НСД к информации. Классификация АС и требования по защите информации» и «СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации».

РД «СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации».

РД «СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации» устанавливает классификацию СВТ по уровню защищенности от НСД к информации на базе перечня показателей защищенности и совокупности описывающих их требований. (Основным источником при разработке этого документа послужила американская «Оранжевая книга»). Устанавливается семь классов защищенности СВТ от НСД к информации. Самый низкий класс седьмой, самый высокий - первый. Классы подразделяются на четыре группы, отличающиеся уровнем защиты:

Первая группа содержит только один седьмой класс, к которому относят все СВТ, не удовлетворяющие требованиям более высоких классов;

Вторая группа характеризуется дискреционной защитой и содержит шестой и пятый классы;

Третья группа характеризуется мандатной защитой и содержит четвертый, третий и второй классы;

Четвертая группа характеризуется верифицированной защитой содержит только первый класс.

РД «АС. Защита от НСД к информации. Классификация АС и требования по защите информации».

РД «АС. Защита от НСД к информации. Классификация АС и требования по защите информации» устанавливает классификацию автоматизированных систем, подлежащих защите от несанкционированного доступа к информации, и требования по защите информации в АС различных классов. К числу определяющих признаков, по которым производится группировка АС в различные классы, относятся:

наличие в АС информации различного уровня конфиденциальности;

уровень полномочий субъектов доступа АС на доступ к конфиденциальной

информации;

режим обработки данных в АС - коллективный или индивидуальный.

Устанавливается девять классов защищенности АС от НСД к информации. Каждый класс характеризуется определенной минимальной совокупностью требований по защите.

Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС. В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности и конфиденциальности информации и, следовательно, иерархия классов защищенности АС.

РД «СВТ. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации».

При анализе системы защиты внешнего периметра корпоративной сети в качестве основных критериев целесообразно использовать РД «СВТ. Межсетевые экраны. Защита от

НСД к информации. Показатели защищенности от НСД к информации». Данный документ определяет показатели защищенности МЭ. Каждый показатель защищенности представляет собой набор требований безопасности, характеризующих определенную область функционирования МЭ. Всего выделяется пять показателей защищенности:

Управление доступом;

Идентификация и аутентификация;

Регистрация событий и оповещение;

Контроль целостности;

Восстановление работоспособности.

На основании показателей защищенности определяются следующие пять классов защищенности МЭ:

Простейшие фильтрующие маршрутизаторы – 5 класс;

Пакетные фильтры сетевого уровня – 4 класс;

Простейшие МЭ прикладного уровня – 3 класс;

МЭ базового уровня – 2 класс;

Продвинутые МЭ – 1 класс.

МЭ первого класса защищенности могут использоваться в АС класса 1А, классах обрабатывающих информацию «особой важности». Второму классу защищенности МЭ соответствует класс защищенности АС 1Б, предназначенный для обработки «совершенно секретной» информации и т.п. [3].

### 7.1.2. Стандарты аудиторской деятельности

**Ассоциация аудита и контроля информационных систем**

Ассоциация аудита и контроля информационных систем – ISACA. Подход к проведению аудита ИС, как отдельной самостоятельной услуги, с течением времени упорядочился и стандартизировался. Крупные и средние аудиторские компании образовали ассоциации: союзы профессионалов в области аудита ИС, которые занимаются созданием и сопровождением стандартов аудиторской деятельности в сфере ИТ. Как правило, это закрытые стандарты.

Ассоциация ISACA занимается открытой стандартизацией аудита ИС.

Ассоциация ISACA основана в 1969 году и в настоящее время объединяет около 20 тысяч членов из более чем 100 стран, в том числе и России. Ассоциация координирует деятельность более чем 12000 аудиторов информационных систем.

Основная декларируемая цель ассоциации: это исследование, разработка, публикация и продвижение стандартизованного набора документов по управлению информационной технологией для ежедневного использования администраторами и аудиторами информационных систем.

В помощь профессиональным аудиторам, администраторам и заинтересованным пользователям ассоциацией ISACA и привлеченными специалистами из ведущих мировых консалтинговых компаний был разработан стандарт CoBiT.

**CoBiT**

CoBiT (Контрольные объекты информационной технологии) – открытый стандарт, первое издание, которое в 1996 году было продано в 98 странах по всему миру и облегчило работу профессиональных аудиторов в сфере информационных технологий. Стандарт связывает информационные технологии и действия аудиторов, объединяет и согласовывает многие другие стандарты в единый ресурс, позволяющий авторитетно, на современном уровне получить представление и управлять целями и задачами, решаемыми ИС. CoBiT учитывает все особенности информационных систем любого масштаба и сложности.

Основополагающее правило, положенное в основу CoBiT: ресурсы ИС должны управляться набором естественно сгруппированных процессов для обеспечения организации необходимой и надежной информацией (рисунок 7.1).

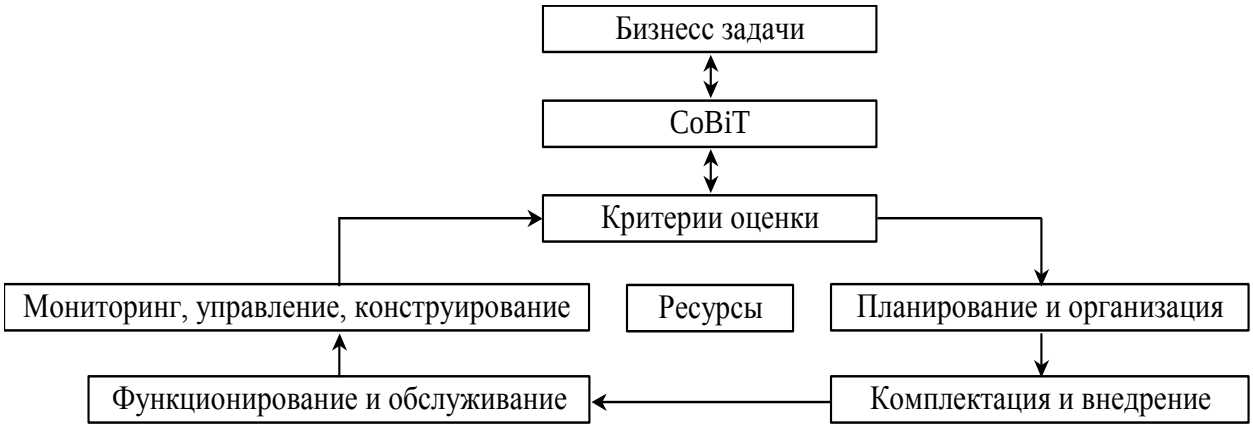



Рис. 7.1. Структура стандарта CoBiT

Каждый из приведенных элементов на блок схеме комплексный и включает в себя следующие компоненты.

*Ресурсы*: людские ресурсы, приложения, технологии, оборудование, данные. А теперь немного разъяснений по поводу того, какие ресурсы и критерии их оценки используются в стандарте CoBiT:

Трудовые ресурсы – под трудовыми ресурсами понимаются не только сотрудники организации, но также руководство организации и контрактный персонал. Рассматриваются навыки штата, понимание задач и производительность работы.

Приложения – прикладное программное обеспечение, используемое в работе организации.

Технологии – операционные системы, базы данных, системы управления и т.д.

Оборудование – все аппаратные средства ИС организации, с учетом их обслуживания.

Данные – данные в самом широком смысле — внешние и внутренние, структурированные и неструктурированные, графические, звуковые, мульти-медиа и т.д.

*Критерии оценки*: эффективность, технический уровень, безопасность, целостность, пригодность, согласованность, надежность.

Все эти ресурсы оцениваются CoBiT на каждом из этапов построения или аудита ИС по следующим критериям:

Эффективность – критерий, определяющий уместность и соответствие информации задачам бизнеса.

Технический уровень – критерий соответствия стандартам и инструкциям.

Безопасность – защита информации.

Целостность – точность и законченность информации.

Пригодность – доступность информации требуемым бизнес-процессам в настоящем и будущем. А также защита необходимых и сопутствующих ресурсов.

Согласованность – исполнение законов, инструкций и договоренностей, влияющих на бизнес-процесс, то есть внешние требования к бизнесу.

Надежность – соответствие информации, предоставляемой руководству организации, осуществление соответствующего управления финансированием и согласованность должностных обязанностей.

*Планирование и организация:*

P01 Стратегический план развития,

P02 Архитектура ИС,

P03 Технологическое направление,

P04 Внутренняя организационная структура и взаимоотношения,

P05 Управление инвестициями,

P06 Цели и задачи руководства,

P07 Пользователи и обслуживающий персонал,

P08 Законодательные и нормативные акты,

P09 Учет и анализ рисков,

P010 Управление проектами,

P011 Управление качеством.

Комплектация и внедрение:

A1 Технологическое решение,

A2 Прикладное ПО,

A3 Инфраструктура,

A4 Процедуры,

A5 Установка и аккредитация ИС,

A6 Оценка эффективности.

Функционирование и обслуживание:

DS1 Уровни обслуживания,

DS2 Услуги сторонних организаций,

DS3 Производительность и масштабируемость,

DS4 Непрерывность обслуживания,

DS5 Безопасность информации в ИС,

DS6 Определение и учет затрат,

DS7 Обучение пользователей,

DS8 Помощь и консультации обслуживающему персоналу,

DS9 Конфигурация элементов ИС,

DS10 Разрешение проблем и инцидентов,

DS11 Работа, передача, хранение и защита данных,

DS12 Безопасность работы,

DS13 Проведение и документирование работ.

Мониторинг, управление, контроль:

M1 Мониторинг происходящих процессов,

M2 Адекватность управления,

M3 Контроль независимого обслуживания,

M4 Проведение независимого аудита.

CoBiT базируется на стандартах аудита ISA и ISACF, но включает и другие международные стандарты, в том числе принимает во внимание утвержденные ранее стандарты и нормативные документы:

технические стандарты;

кодексы;

критерии ИС и описание процессов;

профессиональные стандарты;

требования и рекомендации;

требования к банковским услугам, системам электронной торговли и производству.

Стандарт разработан и проанализирован сотрудниками соответствующих подразделений ведущих консалтинговых компаний и используется в их работе наряду с собственными разработками.

Применение стандарта CoBiT возможно как для проведения аудита ИС организации, так и для изначального проектирования ИС. Обычный вариант прямой и обратной задач. Если в первом случае – это соответствие текущего состояния ИС лучшей практике аналогичных

организаций и предприятий, то в другом – изначально верный проект и, как следствие, по окончании проектирования – ИС, стремящаяся к идеалу.

Несмотря на малый размер разработчики старались, чтобы стандарт был прагматичным и отвечал потребностям бизнеса, при этом сохраняя независимость от конкретных производителей, технологий и платформ.

На базовой блок-схеме CoBiT отражена последовательность, состав и взаимосвязь базовых групп. *Бизнес-процессы* (в верхней части схемы) предъявляют свои требования к ресурсам ИС, которые анализируются с использованием критериев оценки CoBiT на всех этапах построения и проведения аудита.

Четыре базовые группы (домена) содержат в себе тридцать четыре подгруппы, которые, в свою очередь состоят из трехсот двух объектов контроля. Объекты контроля предоставляют аудитору всю достоверную и актуальную информацию о текущем состоянии ИС.

Отличительные черты CoBiT:

Большая зона охвата (все задачи от стратегического планирования и основополагающих документов до анализа работы отдельных элементов ИС).

Перекрестный аудит (перекрывающиеся зоны проверки критически важных элементов).

Адаптируемый, наращиваемый стандарт.

Стандарт легко масштабируется и наращивается. CoBiT позволяет использовать любые разработки производителей аппаратно-программного обеспечения и анализировать полученные данные не изменяя общие подходы и собственную структуру.

**Требования к представлению информации**

Ассоциация ISACA разработала и приняла требования к представлению информации при проведении аудита. Применение стандарта CoBiT гарантирует соблюдение этих требований.

Основное требование: полезность информации. Чтобы информация была полезной, она должна обладать определенными характеристиками, среди которых:

Понятность. Информация должна быть понятной для пользователя, который обладает определенным уровнем знаний, что не означает, однако, исключения сложной информации, если она необходима.

Уместность. Информация является уместной или относящейся к делу, если она влияет на решения пользователей и помогает им оценивать прошлые, настоящие, будущие события или подтверждать и исправлять прошлые оценки. На уместность информации влияет ее содержание и существенность. Информация является существенной, если ее отсутствие или неправильная оценка могут повлиять на решение пользователя. Еще одна характеристика уместности: это своевременность информации, которая означает, что вся значимая информация своевременно, без задержки включена в отчет и такой отчет предоставлен

вовремя. Неким аналогом принципа уместности в российской практике может служить требование полноты отражения операций за учетный период, хотя требование отражения всей информации не тождественно требованию отражения существенной информация.

Достоверность, надежность. Информация является достоверной, если она не содержит существенных ошибок или пристрастных оценок и правдиво отражает хозяйственную деятельность. Чтобы быть достоверной, информация должна удовлетворять следующим характеристикам:

правдивость;

нейтральность: информация не должна содержать однобоких оценок, то есть информация не должна предоставляться выборочно, с целью достижения определенного результата;

осмотрительность: готовность к учету потенциальных убытков, а не потенциальных прибылей и как следствие – создание резервов, такой подход уместен в состоянии неопределенности и не означает создание скрытых резервов или искажения информации;

достаточность информации: включает такую характеристику, как требование полноты информации, как с точки зрения ее существенности, так и затрат на ее подготовку.

**Стандарты в области оценки информационной безопасности**

**на базе «Общих критериев»**

Проект «Общие критерии» стал основой для «Общих критериев оценки безопасности информационных технологий», который носит не только технический, но и экономико-политический характер. Его цель состоит, в частности, в том, чтобы упростить, удешевить и ускорить путь сертифицированных изделий информационных технологий на мировой рынок.

Эта цель близка и понятна российским специалистам. В 2002 году был официально издан ГОСТ Р ИСО/МЭК 15408-2002 «Критерии оценки безопасности информационных технологий» с датой введения в действие первого января 2004 г. Таким образом, и Россия фактически живет по «Общим критериям» со всеми вытекающими из данного факта последствиями.

Согласно подходу, принятому в «Общих критериях», на основании предположений безопасности, при учете угроз и положений политики безопасности формулируются цели безопасности для объекта оценки. Для их достижения к объекту и его среде предъявляются требования безопасности.

«Общие критерии» в главной своей части являются каталогом (библиотекой) требований безопасности. Спектр стандартизованных требований чрезвычайно широк, что способствует универсальности “ОК”. Высокий уровень детализации делает их конкретными, допускающими однозначную проверку, способствует повторяемости результатов оценки. Требования параметризованы, что обеспечивает их гибкость.

«Общие критерии» содержат два основных вида требований безопасности:

*функциональные*, соответствующие активному аспекту защиты, предъявляемые к функциям безопасности объекта оценки и реализующим их механизмам;

*требования доверия*, соответствующие пассивному аспекту, предъявляемые к технологии и процессу разработки и эксплуатации объекта оценки.

Библиотека функциональных требований составляет вторую часть «Общих критериев», а каталог требований доверия – третью часть (первая содержит изложение основных концепций ОК).

Кроме того, выделяются общие требования к сервисам безопасности. К числу важнейших видов функциональных требований принадлежат: анализ аудита безопасности (FAU_SAA).

Из существенных для активного аудита компонентов класса FAU «Аудит безопасности» в «Общих критериях» отсутствуют анализ на соответствие политике безопасности (пороговый, статистический и сигнатурный анализы в семействе FAU_SAA предусмотрены), хранилища для описаний контролируемых объектов и для анализируемой информации, а также все интерфейсные компоненты.

В семейство FAU_GEN (генерация данных аудита безопасности) предлагается включить два новых компонента:

FAU_GEN.3 – ассоциирование объекта, операция с которым вызвала событие, с включением в регистрационные записи имени (идентификатора) этого объекта. На минимальном уровне должны протоколироваться открытие/закрытие объекта (установление/разрыв соединения и т.п.), на базовом - все промежуточные операции. На детальном уровне в регистрационные записи должны входить все операнды операции с объектом. Компонент FAU_GEN.3 добавлен по двум причинам. Во-первых, должна соблюдаться симметрия между субъектами и объектами. Во-вторых, статистические профили целесообразно строить не для субъектов, а для объектов, но для этого нужно располагать соответствующей информацией.

FAU_GEN.4 – предназначен для обеспечения неотказуемости сервиса, пользующегося услугами семейства FAU_GEN, от регистрации события.

Стандартный компонент FAU_SAR.3 дает возможность осуществлять поиск и сортировку регистрационной информации, задавая в качестве критериев логические выражения.

Подобные выражения полезны также для задания фильтров, управляющих работой сенсоров.

Автоматический анализ регистрационной информации с целью выявления подозрительной активности представлен в «Общих критериях» четырьмя компонентами семейства FAU_SAA.

FAU_SAA.1 ориентирован на обнаружение превышения порогов, заданных фиксированным набором правил.

FAU_SAA.2 служит для выявления нетипичной активности путем анализа профилей поведения. В «Общих критериях» предлагаются профили для субъектов, хотя профили объектов могут оказаться предпочтительными. «Общие критерии» допускают анализ, как в реальном времени, так и постфактум. Поддержку анализа в реальном времени следует рассматривать как важнейшую отличительную особенность средств активного аудита.

FAU_SAA.3 направлен на выявление простых атак путем проведения сигнатурного анализа.

FAU_SAA.4 позволяет выявлять сложные, многоэтапные атаки, осуществляемые группой злоумышленников. Предусматривается возможность настройки всех четырех компонентов путем добавления, модификации или удаления правил, отслеживаемых субъектов и сигнатур.

Вводится еще один компонент, FAU_SAA.5, позволяющий выявлять нарушения политики безопасности. Задавать политики предлагается с помощью предикатов первого порядка.

В плане автоматического реагирования на подозрительную активность «Общие критерии» по сути ограничились констатацией подобной возможности. Решающий элемент, который, получив рекомендации от компонентов анализа, определяет, действительно ли имеет место подозрительная активность, и, при необходимости, надлежащим образом реагирует (выбирая форму реакции в зависимости от серьезности выявленных нарушений).

Это значит, что решатель (решающий элемент) должен уметь:

ранжировать подозрительную активность;

реагировать в соответствии с рангом нарушения.

Оба аспекта должны управляться администратором безопасности.

В качестве отдельной возможности, присущей системам высокого класса, фигурирует проведение корреляционного анализа информации.

Описание контролируемых объектов и хранение соответствующей информации - важнейшая составная часть средств активного аудита, придающая им свойства расширяемости и настраиваемости. К этому компоненту предъявляются в первую очередь технологические требования.

Мониторы, как организующие оболочки для менеджеров средств активного аудита, должны обладать двумя группами свойств:

обеспечивать защиту процессов, составляющих менеджер, от злоумышленных воздействий;

обеспечивать высокую доступность этих процессов.

Первая группа обслуживается семейством FPT_SEP (разделение доменов).

Вторая группа свойств может обеспечиваться такими техническими решениями, как программное обеспечение промежуточного слоя, кластерные конфигурации и т.д.

В плане безопасности целесообразно следовать требованиям FPT_FLS.1 (невозможность перехода в небезопасное состояние в случае сбоя или отказа), а также FPT_RCV.2, FPT_RCV.3, FPT_RCV.4 (надежное восстановление в автоматическом режиме, без потери данных, с точностью до функции безопасности).

Безопасность интерфейсов монитора (с другими мониторами, сенсорами, администратором безопасности) может обеспечиваться компонентами FPT_ITI.1, FPT_ITI.2 (обнаружение и исправление модификации экспортируемых данных), FPT_ITC.1 (конфиденциальность экспортируемых данных), FPT_ITA.1 (доступность экспортируемых данных).

На рабочем месте администратора безопасности должны быть обеспечены стандартные для средств управления возможности: графический интерфейс, возможность настройки способа визуализации и уровня детализации, отбора отображаемых событий. Специфичной для средств активного аудита является возможность получения объяснений от анализаторов и решателей по поводу обнаруженной подозрительной активности. Такие объяснения помогают выбрать адекватный способ реагирования.

Функциональный пакет (ФП) – это неоднократно используемая совокупность функциональных компонентов, объединенных для достижения определенных целей безопасности.

Профили защиты (ПЗ), соответствующие классам защищенности, строятся на основе базового ПЗ и соответствующих комбинаций ФП. Можно зафиксировать профили для следующих разновидностей средств активного аудита:

класс 5 - защита одного информационного сервиса с отслеживанием фиксированного набора характеристик и пороговым анализом (базовый ПЗ);

класс 4 - защита однохостовой конфигурации с произвольным набором информационных сервисов, отслеживанием сетевого трафика, системных и прикладных событий, пороговым и простым сигнатурным анализом в реальном масштабе времени;

класс 3 - защита сегмента локальной сети от многоэтапных атак при сохранении остальных предположений класса 4;

класс 2 - защита произвольной конфигурации с выявлением нетипичного поведения при сохранении остальных предположений класса 3;

класс 1 - наложение всех требований с возможностью обеспечения заданного соотношения между ошибками первого и второго рода.

### 7.2. Методы и средства аудита безопасности информационных систем

#### 7.2.1. Основные понятия и определения

**Активный аудит и его место среди других сервисов безопасности**

Формула «защищать, обнаруживать, реагировать» является классической. Только эшелонированная, активная оборона, содержащая разнообразные элементы, дает шанс на успешное отражение угроз.

*Назначение активного аудита* – обнаруживать и реагировать. Обнаружению подлежит подозрительная активность компонентов ИС – от пользователей (внутренних и внешних) до программных систем и аппаратных устройств.

Подозрительную активность можно подразделить на:

злоумышленную,

аномальную (нетипичную).

*Злоумышленная активность* - это либо атаки, преследующие цель несанкционированного получения привилегий, либо действия, выполняемые в рамках имеющихся привилегий (возможно, полученных незаконно), но нарушающие политику безопасности. Последнее назовем – злоупотреблением полномочиями.

*Нетипичная активность* может впрямую не нарушать политику безопасности, но, как правило, она является следствием либо некорректной (или сознательно измененной) работы аппаратуры или программ, либо действий злоумышленников, маскирующихся под легальных пользователей.

Активный аудит дополняет такие традиционные защитные механизмы, как идентификация/аутентификация и разграничение доступа. Подобное дополнение необходимо по двум причинам. Во-первых, существующие средства разграничения доступа не способны реализовать все требования политики безопасности, если последние имеют более сложный вид, чем разрешение/запрет атомарных операций с ресурсами. Развитая политика безопасности может накладывать ограничения на суммарный объем прочитанной информации, запрещать доступ к ресурсу B, если ранее имел место доступ к ресурсу A, и т.п. Во-вторых, в самих защитных средствах есть ошибки и слабости, поэтому, помимо строительства заборов, приходится заботиться об отлавливании тех, кто смог через эти заборы перелезть.

Развитые системы активного аудита несут двойную нагрузку, образуя как первый, так и последний защитные рубежи (см. рисунок 7.2.). Первый рубеж предназначен для обнаружения атак и их оперативного пресечения. На последнем рубеже выявляются

симптомы происходящих в данный момент или ранее случившихся нарушений политики безопасности, принимаются меры по пресечению нарушений и минимизации ущерба.


Рис. 7.2. Защитные рубежи, контролируемые системами активного аудита

И на первом, и на последнем рубеже, помимо активного аудита, присутствуют другие сервисы безопасности. К первому рубежу можно отнести сканеры безопасности, помогающие выявлять и устранять слабые места в защите. На последнем рубеже для обнаружения симптомов нарушений могут использоваться средства контроля целостности. Иногда их включают в репертуар систем активного аудита; мы, однако, не будем этого делать, считая контроль целостности отдельным сервисом.

Между сервисами безопасности существуют и другие связи. Так, активный аудит может опираться на традиционные механизмы протоколирования. В свою очередь, после выявления нарушения зачастую требуется просмотр ранее накопленной регистрационной информации, оценить ущерб, понять, почему нарушение стало возможным, спланировать меры, исключающие повторение инцидента. Параллельно производится надежное восстановление первоначальной конфигурации, то есть не измененной нарушителем.

**Виды аудита**

Классифицировать виды аудита можно по средствам, а именно:

активный аудит,

авторизованный аудит.

*Активный аудит* – это проверка непосредственно компьютерной информационной сети по средствам программных продуктов. Активный аудит позволяет реализовать постоянную проверку внутренней сети предприятия.

*Авторизованный аудит* – это проверка защищенности информационных активов предприятия на всех уровнях защиты (законодательном, административном, процедурном и программно-техническом). Подобную проверку осуществляют специально аккредитованные аудиторские службы.

**Влияние аудита безопасности на развитие компании**

Большинство лиц, ответственных за обеспечение информационной безопасности, задавалось вопросом: «Как оцепить уровень безопасности корпоративной информационной системы нашего предприятия для управления им в целом и определения перспектив его развития?».

Темпы развития современных информационных технологий значительно опережают темпы разработки рекомендательной и нормативно-правовой базы руководящих документов, действующих на территории России. Поэтому вопрос «как оценить уровень безопасности корпоративной информационной системы» – обязательно влечет за собой следующие: в соответствии с какими критериями производить оценку эффективности защиты, как оценивать и переоценивать информационные риски предприятия? Вследствие этого, в дополнение к требованиям, рекомендациям и руководящим документам Гостехкомисии России и ФАПСИ приходится адаптировать к нашим условиям и применять методики международных стандартов (ISO 17799, 9001, 15408, BSI и пр.), а также использовать методы количественного анализа рисков в совокупности с оценками экономической эффективности инвестиций в обеспечение безопасности и защиты информации.

Такие методики работы по анализу рисков информационной безопасности, проектированию и сопровождению систем безопасности должны позволить:

произвести количественную оценку текущего уровня безопасности, задать допустимые уровни рисков, разработать план мероприятий по обеспечению требуемого уровня безопасности на организационно-управленческом, технологическом и техническом уровнях с использованием современных методик и средств;

рассчитать и экономически обосновать перед руководством или акционерами размер необходимых вложений в обеспечение безопасности на основе технологий анализа

рисков, соотнести расходы на обеспечение безопасности с потенциальным ущербом и вероятностью его возникновения;

выявить и провести первоочередное блокирование наиболее опасных уязвимостей до осуществления атак на уязвимые ресурсы;

определить функциональные отношения и зоны ответственности при взаимодействии подразделений и лиц по обеспечению информационной безопасности предприятия, создать необходимый пакет организационно-распорядительной документации;

разработать и согласовать со службами организации, надзорными органами проект внедрения необходимых комплексов защиты, учитывающий современный уровень и тенденции развития информационных технологий;

обеспечить поддержание внедренного комплекса защиты в соответствии с из меняющимися условиями работы организации, регулярными доработками организационно-распорядительной документации, модификацией технологических процессов и модернизацией технических средств защиты.

**Новые возможности развития компании**

Выполнение приведенных выше мероприятий открывает перед должностными лицами разного уровня новые широкие возможности:

*руководителям организаций и предприятий* позволяет обеспечить формирование единых *политики и концепции безопасности* предприятия; рассчитать, согласовать и обосновать необходимые затраты в защиту предприятия; объективно и независимо оценить текущей уровень информационной безопасности предприятия; обеспечить требуемый уровень безопасности и в целом повысить экономическую эффективность предприятия; эффективно создавать и использовать *профили защиты* конкретного предприятия на основе неоднократно апробированных и адаптированных качественных и количественных методик опенки информационной безопасности предприятий;

*начальникам служб автоматизации и информационной безопасности* предприятия – получить оперативную и объективную *качественную и количественную* оценку состояния информационной безопасности предприятия на всех основных уровнях рассмотрения вопросов безопасности: *организационно-управленческом, технологическом и техническом;* выработать и обосновать необходимые меры организационного характера (состав и структуру службы информационной безопасности, положение о коммерческой тайне, пакет должностных инструкций и инструкции действия в нештатных ситуациях); помогают составить экономическое обоснование необходимых инвестиций в защиту информации, обоснованно выбрать те или иные аппаратно-программные средства защиты информации в рамках единой *концепции безопасности* в соответствии с требованиями распоряжений и руководящих документов Гостехкомиссии России, ФАПСИ, а также международных

стандартов ISO 17799, 9001, 15408, BSI; адаптировать и использовать в своей работе предложенные количественные показатели опенки информационной безопасности, методики оценки и управления безопасностью с привязкой к экономической составляющей эффективности предприятия;

*системным, сетевым администраторам и администраторам безопасности предприятия* - объективно оценить безопасность всех основных компонентов и сервисов корпоративной информационной системы предприятия, техническое состояние аппаратно-программных средств защиты информации (межсетевых экранов, маршрутизаторов, хостов, серверов, корпоративных БД и приложений); успешно применять на практике рекомендации, полученные в ходе выполнения аналитического исследования, для нейтрализации и локализации выявленных уязвимостей аппаратно-программного уровня;

*сотрудникам и работникам предприятий и организаций - определить основные функциональные отношения и,* что особенно важно, *зоны ответственности,* в том числе финансовой, за надлежащее использование информационных ресурсов и состояние *политики безопасности* предприятия.

### 7.2.2. Основные этапы проведения аудита

Комплексный аудит информационной безопасности включает следующие виды работ:

обследование объекта - построение информационной модели АС заказчика;

инвентаризация ресурсов – ранжирование ресурсов компании по степени важности;

построение частной модели угроз – классификация угроз по степени опасности и вероятности;

построение модели нарушителя;

оценка потенциального ущерба от нарушения безопасности – оценка рисков с применением методики трехфакторного анализа;

оценка существующей системы безопасности на соответствие требованиям стандартов безопасности: ведомственным, государственным, международным;

выявление уязвимых мест и каналов утечки информации;

разработка и оценка предложений по применению контрмер;

проектирование комплекса средств защиты;

разработка организационных мероприятий - пакет организационно-распорядительной документации;

оценка остаточных рисков.

**Практические шаги авторизованного аудита безопасности**

Как на практике реализовать перечисленные возможности? По мнению специалистов, это становится возможным в ходе следующих практических шагов аудита безопасности.

1. Комплексный анализ ИС предприятия и подсистемы информационной безопасности на методологическом, организационно-управленческом, технологическом и техническом уровнях. Анализ рисков.

1.1. Исследование и оценка состояния информационной безопасности КИС и подсистемы информационной безопасности предприятия.

Комплексная оценка соответствия типовых требований РД Гостехкомиссии РФ системе информационной безопасности предприятия.

Комплексная оценка соответствия типовых требований международных стандартов ISO системе информационной безопасности предприятия.

Комплексная оценка соответствия специальных требований заказчика системе информационной безопасности предприятия.

1.2. Работы на основе анализа рисков.

Анализ рисков. Уровень управления рисками на основе качественных оценок рисков.

Анализ рисков. Уровень управления рисками на основе количественных оценок рисков.

1.3. Инструментальные исследования.

1.3.1. Инструментальное исследование элементов инфраструктуры компьютерной сети и корпоративной информационной системы на наличие уязвимостей.

1.3.2. Инструментальное исследование защищенности точек доступа предприятия в Internet.

1.4. Анализ документооборота предприятия.

2. Разработка комплексных рекомендаций по методологическому, организационно-управленческому, технологическому, общетехническому и программно-аппаратному обеспечению режима информационной безопасности предприятия.

2.1. Разработка концепции обеспечения информационной безопасности предприятия.

2.2. Разработка корпоративной политики обеспечения информационной безопасности предприятия на организационно-управленческом, правовом, технологическом и техническом уровнях.

2.3. Разработка плана защиты предприятия заказчика.

2.4. Дополнительные работы по анализу и созданию методологического, организационно-управленческого, технологического, инфраструктурного и технического обеспечения режима информационной безопасности предприятия заказчика.

3. Организационно-технологический анализ ИС предприятия.

3.1. Оценка организационно-управленческого уровня безопасности.

Оценка соответствия типовым требованиям руководящих документов РФ к системе информационной безопасности предприятия в области организационно-технологических норм.

Анализ документооборота предприятия категории «конфиденциально» на соответствие требованиям концепции информационной безопасности, положению о коммерческой тайне, прочим внутренним требованиям предприятия по обеспечению конфиденциальности информации.

Дополнительные работы по исследованию и оценке информационной безопасности объекта.

3.2. Разработка рекомендаций по организационно-управленческому, технологическому, общетехническому обеспечению режима информационной безопасности предприятия.

Разработка элементов концепции обеспечения информационной безопасности предприятия.

Разработка элементов корпоративной политики обеспечения информационной безопасности предприятия на организационно-управленческом, правовом и технологическом уровнях.

**4. Экспертиза решений и проектов.**

Экспертиза решений и проектов автоматизации на соответствие требованиям по обеспечению информационной безопасности экспертно-документальным методом.

Экспертиза проектов подсистем информационной безопасности на соответствие требованиям по безопасности экспертно-документальным методом.

5. Работы по анализу документооборота и поставке типовых комплектов организационно-распорядительной документации.

Анализ документооборота предприятия категории “конфиденциально” на соответствие требованиям концепции информационной безопасности, положению о коммерческой тайне, прочим внутренним требованиям предприятия по обеспечению конфиденциальности информации.

Поставка комплекта типовой организационно-распорядительной документации в соответствии с рекомендациями корпоративной политики ИБ предприятия на организационно-управленческом и правовом уровне.

**6. Работы, поддерживающие практическую реализацию плана защиты.**

Разработка технического проекта модернизации средств защиты КИС, установленных у заказчика по результатам проведенного комплексного аналитического исследования корпоративной сети.

Разработка системы поддержки принятия решений на предприятии заказчика по обеспечению информационной безопасности предприятия на основе CASE-систем и др.

Подготовка предприятия к аттестации.

6.3.1. Подготовка “под ключ” предприятия к аттестации объектов информатизации заказчика на соответствие требованиям РД РФ.

6.3.2. Подготовка предприятия к аттестации КИС на соответствие требованиям по безопасности международных стандартов ISO 15408, ISO 17799, стандарта ISO 9001 при обеспечении требований информационной безопасности предприятия.

6.4. Разработка организационно-распорядительной и технологической документации.

6.4.1. Разработка расширенного перечня сведений ограниченного распространения как части политики безопасности.

6.4.2. Разработка пакета организационно-распорядительной документации (ОРД) в соответствии с рекомендациями корпоративной политики ИБ предприятия на организационно-управленческом и правовом уровне.

6.4.3. Поставка комплекта типовой организационно-распорядительной документации в соответствии с рекомендациями корпоративной, политики ИБ предприятия на организационно-управленческом и правовом уровнях.

**7. Повышение квалификации и переподготовка специалистов.**

Тренинги в области организационно-правовой составляющей защиты информации.

Обучение основам экономической безопасности.

Тренинги в области технологии защиты информации.

Тренинги по применению продуктов (технических средств) защиты информации.

Обучение действиям при попытке взлома информационных систем.

Обучение и тренинги по восстановлению работоспособности системы после нарушения штатного режима ее функционирования, а также по восстановлению данных и программ из резервных копий.

Сопровождение системы информационной безопасности после проведенного комплексного анализа или анализа элементов системы ИБ предприятия.

**Ежегодная переоценка состояния ИБ.**

Здесь под термином *аудит* информационной безопасности корпоративной системы Internet/Intranet понимается *системный процесс* получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности компании в соответствии с определенными критериями и показателями безопасности на всех основных уровнях обеспечения безопасности: методологическом, организационно-управленческом, технологическом и техническом. Таких оценок, которые позволяют выработать практические рекомендации по управлению и обеспечению информационной безопасности компании, адекватные поставленным целям и задачам развития бизнеса.

В целом независимо от своей разновидности, состава и объема аудит безопасности корпоративной системы Internet/Intranet должен позволить решить следующие актуальные задачи каждой проверяемой компании:

обеспечить (при необходимости повысить) информационную безопасность предприятия;

снизить потенциальные потери предприятия путем повышения устойчивости функционирования корпоративной сети;

защитить конфиденциальную информацию, передаваемую по открытым каналам связи;

защитить информацию от умышленного искажения (разрушения), несанкционированного копирования, доступа или использования;

обеспечить контроль действий пользователей в корпоративной сети предприятия;

своевременно оценить и переоценить информационные риски бизнес деятельности компании;

выработать оптимальные планы развития и управления предприятием.

**Планирование авторизованного аудита информационной безопасности компании**

В соответствии с рекомендациями международных стандартов информационной безопасности процедура проведения аудита безопасности компании должна планироваться заранее. Для этого необходимо составить *план проведения аудита,* который должен отражать все мероприятия и процедуры, связанные с первоначальными и контрольными проверками продолжительностью более одного дня. Кроме того необходимо ознакомиться с соответствующей законодательной и нормативной базой для выявления требований по информационной безопасности, которые могут быть использованы для обеспечения информационной безопасности компании.

Для проведения аудита информационной безопасности компании необходимо подготовить все необходимые сведения о собственной структуре, бизнес деятельности, текущих проектах, состоянии информационной инфраструктуры и т. п. Кроме того, потребуется:

документально оформленные концепция и политика безопасности компании,

список используемого в компании системного и прикладного программного обеспечения,

описание технологии обработки данных,

состав и структура подсистемы защиты информации,

общая карта компьютерной сети компании.

План проведения аудита должен определять проверяемые области деятельности компании и время их проверки с указанием, какие именно требования международных стандартов, например ISO 17799, и руководящих документов Гостехкомиссии РФ будут

проверяться. Т.е. план подготовки и проведения аудита должен определять потребности компании в оценке и объективном анализе состояния информационной безопасности, потребности в соответствующих аппаратно-программных средствах защиты информации, потребности в обучении и переподготовке службы информационной безопасности, а также освещать другие вопросы, ответы на которые невозможно дать без проведения аудита. В дальнейшем план проведения аудита с внесенными в него изменениями по ходу проверок прилагается к отчету о проведении аудита. Кроме того, необходимо помнить о согласовании плана проведения аудита с Концепцией и Политикой информационной безопасности компании.

Рекомендуется выделять четыре возможных этапа планирования аудита:

Подготовка аудита безопасности;

Анализ требований и исходных данных;

Расчет трудоемкости и стоимости выполняемых работ;

Документирование процедуры проведения аудита.

**Подготовительный этап**

На *подготовительном этапе* исполнитель определяет общий порядок работ, устанавливающий последовательность выполнения и возможные затраты ресурсов, и согласовывает его с заказчиком. На этом этапе рассматриваются:

Назначение и цели предстоящего аудита, порядок их достижения.

Принципы установки рамок проведения аудита.

Функции, структура и состав корпоративной системы Internet/Intranet, узкие места и потенциальные уязвимости в системе управления информационной безопасностью.

Методики оценки квалификации специалистов и сотрудников службы информационной безопасности.

Способы категорирования обрабатываемой в корпоративной информационной системе информации, например на общедоступную, конфиденциальную и строго конфиденциальную;

Методы и инструментарии оценки временных затрат и затрат ресурсов компании на аудит информационной безопасности. Возможность использования результатов ранее проведенного аудита, в том числе анализа информационных рисков и анализа соответствия требованиям международных стандартов и руководящих документов Гостехкомиссии РФ;

Состав группы экспертов в области безопасности корпоративных систем Internet/Intranet и распределение обязанностей между ними;

Параметры корпоративной информационной сети компании и среды ее функционирования, оказывающие существенное влияние на качество аудита безопасности;

Совокупность учитываемых при проведении аудита безопасности требований международных, государственных, межведомственных и внутренних стандартов;

Внутренняя отчетная документация, оформление и при необходимости корректировка концепции и политики информационной безопасности компании;

Перспективы и тенденции развития корпоративной системы защиты информации компании, вопросы выработки стратегии и тактики ее развития.

Согласованный с заказчиком общий порядок проведения аудита безопасности компании может быть отражен в соответствующем техническом задании.

**Этап анализа требований и исходных данных**

Этап *анализа требований и исходных данных* составляет главную часть планирования аудита. В процессе анализа рассматриваются:

*Требования информационной безопасности.* Цель аудита – объективно и оперативно оценить и проверить соответствие исследуемой корпоративной системы защиты компании предъявляемым к ней требованиям информационной безопасности. Поэтому для такой оценки необходимо сначала рассмотреть требования информационной безопасности. Основными требованиями информационной безопасности для отечественных предприятий и компаний являются требования руководящих документов Гостехкомиссии РФ, законов Российской Федерации, внутриведомственных, межведомственных, национальных и международных стандартов. Кроме этого, для каждой корпоративной информационной системы необходимо учитывать специальные требования внутреннего использования, согласованные с концепцией и политикой безопасности компании. Такие внутренние требования рекомендуется формулировать по результатам анализа информационных рисков компании, учитывающих специфику конкретной компании;

*Исходные данные для проведения аудита.* В руководящем документе Гостехкомиссии «Положение по аттестации объектов информатизации по требованиям безопасности информации» приводится стандартный перечень исходных данных, необходимых для разработки программы и методики аттестационных испытаний. Помимо стандартных исходных данных могут использоваться и дополнительные исходные данные, специфичные для каждой конкретной компании, например статистика нарушений политики безопасности компании, статистика внешних и внутренних атак, уязвимости наиболее критичных корпоративных информационных ресурсов и т. д. Также нужно учитывать, что, как правило, руководство компании имеет собственные взгляды на информацию, предоставляемую в качестве исходных данных для аудита безопасности. Поэтому между заказчиком и исполнителем работ по аудиту информационной безопасности рекомендуется заключить специальное соглашение о конфиденциальности или соответствующий протокол о намерениях;

*Рамки проведения аудита.* При определении рамок проведения аудита необходимо в равной степени учитывать организационный, технологический, и программно-

технический уровни обеспечения информационной безопасности. В противном случае результаты аудита не будут объективно отражать реальный уровень информационной безопасности компании. Например, дорогостоящие аппаратно-программные средства защиты информации могут оказаться бесполезными, если неправильно определены и реализованы меры и мероприятия на организационном и технологическом уровнях. При определении рамок аудита необходимо зафиксировать штатные условия функционирования корпоративной информационной системы безопасности компании. Такая фиксация может быть отражена в «Аттестате соответствия» или «Паспорте компании» и является необходимым условием для обеспечения требуемого уровня информационной безопасности компании и разработки планов действия в случае возникновения нештатных условий функционирования корпоративной системы Internet/Intranet;

*Области детального изучения.* При проведении аудита основное внимание должно уделяться компонентам и подсистемам, осуществляющим обработку конфиденциальной информации компании. При этом необходимо уметь рассчитать возможный ущерб, который может быть нанесен компании в случае разглашения конфиденциальной информации и нарушения Политики безопасности. Это должно быть отражено в соответствующих документах компании, регламентирующих ее политику информационной безопасности. Для определения возможного ущерба могут использоваться разнообразные формальные методы, например методы экспертных оценок. В качестве исходных данных для принятия решения об областях детального изучения могут служить результаты ранее проведенного, текущего комплексного аудита безопасности компании, результаты анализа информационных рисков компании и другие данные. Кроме того при необходимости уязвимые места дополнительно могут быть исследованы специальными инструментальными проверками с помощью так называемых сканеров и систем проверки уровня защищенности;

*Требуемый уровень детализации и полноты.* В большинстве случаев для получения адекватных результатов достаточно провести базовый анализ корпоративной системы защиты информации, позволяющий определить общий уровень информационной безопасности компании и проверить его на соответствие некоторым требованиям безопасности. В некоторых случаях дополнительно требуется провести детальный анализ, цель которого — количественно оценить уровень информационной безопасности компании на основе специальных количественных метрик и мер информационной безопасности. Для этого сначала определяются все необходимые количественные показатели, а затем производится оценка уровня информационной безопасности компании. Существенно, что при этом становится возможным сравнивать уровень безопасности компании с некоторым эталоном, определять

тенденции и перспективы развития системы корпоративной безопасности, необходимые инвестиции и т. д.

**Этап расчета трудоемкости и стоимости**

На этапе *расчета трудоемкости и стоимости* проводимых работ по данным проведенного анализа оцениваются временные, финансовые, технические, информационные и прочие ресурсы, необходимые для аудита информационной безопасности. Выделение ресурсов рекомендуется производить с учетом возможных нештатных ситуаций, способных увеличить трудоемкость аудита безопасности.

**Этап формализации и документирования**

Завершается планирование аудита *формализацией и документированием* выполнения аудита, что прежде всего подразумевает подготовку и согласование плана проведения аудита. План проведения аудита в общем случае включает в себя следующие разделы:

*Краткая характеристика работ.* Включает все необходимые сведения о порядке проведения работ;

*Введение.* Указывается актуальность проведения аудита безопасности, особенности и требования к порядку проведения аудита, характеристика исследуемого объекта, рамки проведения аудита, общий порядок работ, требования по фиксации результатов аудита. Дополнительно приводятся сведения о категорировании корпоративной информации, например конфиденциальной и строго конфиденциальной. Также перечисляются основные решаемые задачи, ограничения, выполняемые функции и критерии оценивания уровня информационной безопасности компании, требования нормативных документов Российской Федерации, международных стандартов и внутренних требований компании;

*Распределение обязанностей.* Определяется штат и функциональные обязанности группы специалистов, которые будут проводить аудит безопасности;

*Требования информационной безопасности.* Фиксируется обоснованный выбор требований информационной безопасности, определяются критерии и показатели оценки информационной безопасности компании, выбираются количественные метрики и меры безопасности. Помимо нормативной и законодательной базы Российской Федерации дополнительно рекомендуется использовать требования международных и внутренних стандартов компании, актуальные для каждой отдельно взятой. Оценку инвестиций в модернизацию корпоративной системы защиты информации рекомендуется проводить на основе результатов анализа информационных рисков компании;

*Формализация оценок уровня безопасности компании.* Определяются качественные и количественные параметры для получения объективных оценок уровня информационной безопасности компании. Перечисляются задачи, выполняемые при проведении базового и детального анализа информационных рисков. Состав задач зависит от того, на каком этапе

жизненного цикла находится исследуемая безопасность корпоративной системы Internet/Intranet: этапе проектирования, эксплуатации или др. В этом разделе отражаются критичные информационные ресурсы компании, оценка экономической эффективности ее деятельности, используемые модели, методы средства проведения аудита безопасности, исходные данные;

*План-график работ.* Определяются сроки, календарный план выполняемых работ, время их окончания, формы отчетных документов, требования по приему-сдаче работы и прочее;

*Поддержка и сопровождение.* Перечисляются требования к административной, технологической и технической поддержке аудита информационной безопасности;

*Отчетные документы.* Основными отчетными документами являются отчет по результатам аудита безопасности, концепция и политика информационной безопасности, план защиты компании;

*Приложения.* В приложениях приводятся протоколы проверок, а также информация по методикам и инструментарии проведения аудита, выявленные замечания, рекомендации и прочее.

### 7.2.3. Методика анализа защищенности

В настоящее время не существует каких-либо стандартизированных методик анализа защищенности АС, поэтому в конкретных ситуациях алгоритмы действий аудиторов могут существенно различаться. Однако типовую методику анализа защищенности корпоративной сети предложить все-таки возможно. И хотя данная методика не претендует на всеобщность, ее эффективность многократно проверена на практике.

Типовая методика анализа защищенности корпоративной сети включает использование следующих методов:

Изучение исходных данных по АС;

Оценка рисков, связанных с осуществлением угроз безопасности в отношении ресурсов АС;

Анализ механизмов безопасности организационного уровня, политики безопасности организации и организационно-распорядительной документации по обеспечению режима информационной безопасности и оценка их соответствия требованиям существующих нормативных документов, а также их адекватности существующим рискам;

Ручной анализ конфигурационных файлов маршрутизаторов, МЭ и прокси-серверов, осуществляющих управление межсетевыми взаимодействиями, почтовых и DNS серверов, а также других критических элементов сетевой инфраструктуры;

Сканирование внешних сетевых адресов ЛВС из сети Интернет;

Сканирование ресурсов ЛВС изнутри;

Анализ конфигурации серверов и рабочих станций ЛВС при помощи специализированных программных средств.

**Исходные данные по обследуемой АС**

В соответствии с требованиями РД Гостехкомиссии при проведении работ по аттестации безопасности АС, включающих в себя предварительное обследование и анализ защищенности объекта информатизации, заказчиком работ должны быть предоставлены следующие исходные данные:

Полное и точное наименование объекта информатизации и его назначение.

Характер (научно-техническая, экономическая, производственная, финансовая, военная, политическая) информации и уровень секретности (конфиденциальности) обрабатываемой информации определен (в соответствии с какими перечнями (государственным, отраслевым, ведомственным, предприятия).

Организационная структура объекта информатизации.

Перечень помещений, состав комплекса технических средств (основных и вспомогательных), входящих в объект информатизации, в которых (на которых) обрабатывается указанная информация.

Особенности и схема расположения объекта информатизации с указанием границ контролируемой зоны.

Структура программного обеспечения (общесистемного и прикладного), используемого на аттестуемом объекте информатизации и предназначенного для обработки защищаемой информации, используемые протоколы обмена информацией.

Общая функциональная схема объекта информатизации, включая схему информационных потоков и режимы обработки защищаемой информации.

Наличие и характер взаимодействия с другими объектами информатизации.

Состав и структура системы защиты информации на аттестуемом объекте информатизации.

Перечень технических и программных средств в защищенном исполнении, средств защиты и контроля, используемых на аттестуемом объекте информатизации и имеющих соответствующий сертификат, предписание на эксплуатацию.

Сведения о разработчиках системы защиты информации, наличие у сторонних разработчиков (по отношению к предприятию, на котором расположен аттестуемый объект информатизации) лицензий на проведение подобных работ.

Наличие на объекте информатизации (на предприятии, на котором расположен объект информатизации) службы безопасности информации, службы администратора (автоматизированной системы, сети, баз данных).

Наличие и основные характеристики физической защиты объекта информатизации (помещений, где обрабатывается защищаемая информация и хранятся информационные носители).

Наличие и готовность проектной и эксплуатационной документации на объект информатизации и другие исходные данные по аттестуемому объекту информатизации, влияющие на безопасность информации.

Опыт показывает, что перечисленных исходных данных явно недостаточно для выполнения работ по анализу защищенности АС, и приведенный в РД Гостехкомиссии список нуждается в расширении и конкретизации. Пункт 14 приведенного списка предполагает предоставление других исходных данных по объекту информатизации, влияющих на безопасность информации. Как раз эти «дополнительные» данные и являются наиболее значимыми для оценки текущего положения дел с обеспечением безопасности АС. Их список включает следующие виды документов:

Дополнительная документация:

Нормативно-распорядительная документация по проведению регламентных работ.

Нормативно-распорядительная документация по обеспечению политики безопасности.

Должностные инструкции для администраторов, инженеров технической поддержки, службы безопасности.

Процедуры и планы предотвращения и реагирования на попытки НСД к информационным ресурсам.

Схема топологии корпоративной сети с указанием IP-адресов и структурная схема.

Данные по структуре информационных ресурсов с указанием степени критичности или конфиденциальности каждого ресурса.

Размещение информационных ресурсов в корпоративной сети.

Схема организационной структуры пользователей.

Схема организационной структуры обслуживающих подразделений.

Схемы размещения линий передачи данных.

Схемы и характеристики систем электропитания и заземления объектов АС.

Данные по используемым системам сетевого управления и мониторинга.

Проектная документация:

Функциональные схемы.

Описание автоматизированных функций.

Описание основных технических решений.

Эксплуатационная документация: Руководства пользователей и администраторов используемых программных и технических средств защиты информации (СЗИ) (в случае необходимости).

При анализе конфигурации средств защиты внешнего периметра ЛВС и управления межсетевыми взаимодействиями особое внимание обращается на следующие аспекты, определяемые их конфигурацией:

Настройка правил разграничения доступа (правил фильтрации сетевых пакетов) на МЭ и маршрутизаторах;

Используемые схемы и настройка параметров аутентификации;

Настройка параметров системы регистрации событий;

Использование механизмов, обеспечивающих сокрытие топологии защищаемой сети, включающих в себя трансляцию сетевых адресов (NAT), маскарадинг и использование системы split DNS;

Настройка механизмов оповещения об атаках и реагирования;

Наличие и работоспособность средств контроля целостности;

Версии используемого ПО и наличие установленных пакетов программных коррекций.

**Методы анализа защищенности информационной системы**

**Выявление злоумышленной активности**

Под злоумышленной активностью мы понимаем как атаки (очевидно, противоречащие любой политике безопасности), так и действия, нарушающие политику безопасности конкретной организации путем злоупотребления имеющимися полномочиями. Разделение двух видов злоумышленной активности представляется нам целесообразным по той причине, что настройка на выявление атак может быть выполнена поставщиком системы активного аудита (атаки носят универсальный характер), в то время как политика безопасности (если, конечно, она есть) у каждой организации своя и настраиваться на нее заказчикам придется самим.

Для выявления злоумышленной активности пытались и пытаются использовать несколько универсальных технологий: экспертные системы, нейронные сети, сопоставление с образцом, конечные автоматы и т.п. Одной из первых и до сих пор самой употребительной остается технология обнаружения сигнатур злоумышленных действий. Идея состоит в том, чтобы каким-либо образом задать характеристики злоумышленного поведения (это и называется сигнатурами), а затем отслеживать поток событий в поисках соответствия с предопределенными образцами. В более серьезных разработках уже свыше десяти лет используются экспертные системы, опирающиеся на наборы правил, задающие более мощные языки.

Самой сложной проблемой для сигнатурного подхода является обнаружение ранее неизвестных атак, ведь новые угрозы появляются практически каждый день. Бороться с ними можно двумя способами.

Во-первых, можно регулярно обновлять набор сигнатур. Здесь, помимо полноты, критически важной является частота обновлений. Сигнатуры новых атак должны предоставляться заказчикам на порядок быстрее, чем заплаты от производителей скомпрометированных аппаратных или программных продуктов. На практике это означает обновление в течение суток, но никак не раз в месяц. В противном случае системы активного аудита начинают напоминать фиговый листок, а не средство защиты от реальных угроз.

Во-вторых, можно сочетать сигнатурный подход с методами выявления аномальной активности (см. ниже). Атака или злоупотребление полномочиями - это почти всегда аномалия. Задача такова – не пропустить ее и не поднимать слишком часто ложных тревог.

**Выявление аномальной активности**

Для выявления аномальной активности предложено довольно много методов: нейронные сети, экспертные системы, статистический подход.

Статистический подход можно подразделить на кластерный и факторный анализ, а также дискриминантный (классификационный) анализ. Не вдаваясь в детали, укажем, что буквальное применение этих методов не дает хороших результатов; необходимо учитывать специфику предметной области - активного аудита.

Статистический анализ (с учетом сделанных оговорок) представляется наиболее перспективным, отчасти “от противного”, в силу недостатков, присущих другим подходам.

У нейронных сетей две основные проблемы:

непонятность результатов: нейронная сеть принимает решение, но не объясняет, почему оно было принято;

нехватка адекватного обучающего материала: невозможно создать базу всех типов аномалий.

Основной недостаток экспертных систем – неумение выявлять (и, следовательно, отражать) неизвестные атаки.

У статистического подхода также есть проблемы:

относительно высокая вероятность ложных тревог (не типичность поведения не всегда означает злой умысел);

плохая работа в случаях, когда действия пользователей не имеют определенного шаблона, когда с самого начала пользователи совершают злоумышленные действия (злоумышленные действия типичны), наконец, когда пользователь постепенно изменяет шаблон своего поведения в сторону злоумышленных действий.

Тем не менее, с этими проблемами можно бороться.

Выявление аномальной активности статистическими методами основывается на сравнении краткосрочного поведения с долгосрочным. Для этого измеряются значения

некоторых параметров работы субъектов (пользователей, приложений, аппаратуры). Параметры могут отличаться по своей природе; можно выделить следующие группы:

категориальные (измененные файлы, выполненные команды, номер порта и т.п.);

числовые (процессорное время, объем памяти, количество просмотренных файлов, число переданных байт и т.п.);

величины интенсивности (число событий в единицу времени);

распределение событий (таких как доступ к файлам, вывод на печать и т.п.).

Алгоритмы анализа могут работать с разнородными значениями, а могут преобразовать все параметры к одному типу (например, разбив область значения на конечное число подобластей и рассматривая все параметры как категориальные). Выбор измеряемых характеристик работы - очень важный момент. С одной стороны, недостаточное число фиксируемых параметров может привести к неполноте описания поведения субъекта и к большому числу пропуска атак; с другой стороны, слишком большое число отслеживаемых характеристик потребует слишком большого объема памяти и замедлит работу алгоритма анализа.

Измерения параметров накапливаются и преобразуются в профили - описания работы субъектов. Суть преобразования множества результатов измерения в профили - сжатие информации. В результате от каждого параметра должно остаться лишь несколько значений статистических функций, содержащих необходимые для анализирующего алгоритма данные. Для того чтобы профили адекватно описывали поведение субъекта, необходимо отбрасывать старые значения параметров при пересчете значений статистических функций. Для этого, как правило, используется один из двух методов:

*Метод скользящих окон* – результаты измерений за некоторый промежуток времени (для долгосрочных профилей - несколько недель, для краткосрочных - несколько часов) сохраняются; при добавлении новых результатов старые отбрасываются. Основным недостатком метода скользящих окон является большой объем хранимой информации.

*Метод взвешенных сумм* – при вычислении значений статистических функций более старые данные входят с меньшими весами (как правило, новые значения функций вычисляются по рекуррентной формуле, и необходимость хранения большого количества информации отпадает). Основным недостатком метода является более низкое качество описания поведения субъекта, чем в методе скользящих окон.

Итак, долгосрочные профили содержат в себе информацию о поведении субъектов за последние несколько недель; обычно они пересчитываются раз в сутки, когда загрузка системы минимальна. Краткосрочные профили содержат информацию о поведении за последние несколько часов или даже минут; они пересчитываются при поступлении новых результатов измерений.

Сравнение краткосрочных и долгосрочных профилей может производиться разными способами. Можно просто проверять, все ли краткосрочные значения попадают в доверительные интервалы, построенные по долгосрочному профилю. Однако в этом случае аномалии, распределенные по нескольким параметрам, могут остаться незамеченными. Поэтому предпочтительнее анализировать профили в совокупности. Далее, измеряемые характеристики, как правило, не являются независимыми, поэтому было бы желательным, чтобы влияние параметров на решение о типичности поведения было пропорционально степени их независимости.

Полезной числовой характеристикой является количество зафиксированных ошибок. При этом обнаруживается не только злоумышленное поведение, но и сбои и отказы аппаратуры и программ, что также можно считать нарушением информационной безопасности. Разумеется, целесообразно измерять и объем сетевого трафика. Аномальными являются отклонения в обе стороны (слишком большой трафик - сервис используют в злоумышленных целях, слишком маленький - нарушена доступность сервиса).

Применительно к сетевому трафику и некоторым другим событиям полезным классом величин оказывается интенсивность.

Для успеха статистического подхода важен правильный выбор субъектов, поведение которых анализируется. Например, целесообразно анализировать поведения сервисов или их компонентов (например, доступ анонимных пользователей к FTP-сервису). По сравнению с отдельными пользователями, поведение сервисов отличается большей стабильностью, да и для информационной безопасности организации важны именно сервисы. Совсем нет смысла анализировать сетевой трафик “вообще”, его также нужно структурировать по типам поддерживаемых сервисов (плюс служебные моменты сетевого и транспортного уровней, такие как установление соединений).

**Реагирование на подозрительные действия**

После того, как обнаружена сигнатура злоумышленного действия или нетипичная активность, необходимо выбрать достойный ответ. По многим соображениям удобно, чтобы компонент реагирования содержал собственную логику, фильтруя сигналы тревоги и сопоставляя сообщения, поступающие от подсистем анализа. Для активного аудита одинаково опасны:

пропуск атак - это значит, что не обеспечивается должной защиты,

большое количество ложных тревог – это значит, что активный аудит быстро отключат.

При выборе реакции особенно важно определить первопричину проблем. Для сетевых систем это особенно сложно в силу возможности подделки адресов в пакетах. Данный пример показывает, что сильнодействующие средства, пытающиеся воздействовать на злоумышленника, сами могут стать косвенным способом проведения атак.

Предпочтительны более спокойные, но также достаточно эффективные меры, такие как блокирование злоумышленного сетевого трафика средствами межсетевого экранирования (ряд систем активного аудита умеют управлять конфигурацией экранов) или принудительное завершение сеанса работы пользователя. Конечно, и здесь остается опасность наказать невиновного, так что политика безопасности каждой организации должна определять, что важнее - не пропустить нарушение или не обидеть лояльного пользователя.

С точки зрения быстрого реагирования, традиционные меры, связанные с информированием администратора, не особенно эффективны. Они хороши в долгосрочном плане, для глобального анализа защищенности командой профессионалов. Здесь активный аудит смыкается с пассивным, обеспечивая сжатие регистрационной информации и представление ее в виде, удобном для человека.

Разумная реакция на подозрительные действия может включать увеличение степени детализации протоколов и активизацию средств контроля целостности. В принципе, это пассивные меры, но они помогут понять причины и ход развития нарушения, так что человеку будет проще выбрать «меру пресечения».

**Методы тестирования системы защиты**

Тестирование системы защиты АС проводится с целью проверки эффективности используемых в ней механизмов защиты, их устойчивости в отношении возможных атак, а также с целью поиска уязвимостей в защите. Традиционно используются два основных метода тестирования:

тестирование по методу «черного ящика»;

тестирование по методу «белого ящика».

Тестирование по методу «черного ящика» предполагает отсутствие у тестирующей стороны каких-либо специальных знаний о конфигурации и внутренней структуре объекта испытаний. При этом против объекта испытаний реализуются все известные типы атак и проверяется устойчивость системы защиты в отношении этих атак. Используемые методы тестирования эмулируют действия потенциальных злоумышленников, пытающихся взломать систему защиты. Основным средством тестирования в данном случае являются сетевые сканеры, располагающие базами данных известных уязвимостей.

Метод «белого ящика» предполагает составление программы тестирования на основании знаний о структуре и конфигурации объекта испытаний. В ходе тестирования проверяются наличие и работоспособность механизмов безопасности, соответствие состава и конфигурации системы защиты требованиям безопасности и существующим рисками. Выводы о наличие уязвимостей делаются на основании анализа конфигурации используемых средств защиты и системного ПО, а затем проверяются на практике. Основным

инструментом анализа в данном случае являются программные агенты средств анализа защищенности системного уровня, рассматриваемые ниже.

### 7.2.4. Средства анализа защищенности

Арсенал программных средств, используемых для анализа защищенности АС достаточно широк. Причем во многих случаях свободно распространяемые программные продукты ничем не уступают коммерческим. Достаточно сравнить некоммерческий сканер NESSUS с его коммерческими аналогами.

Одним из методов автоматизации процессов анализа и контроля защищенности распределенных компьютерных систем является использование технологии интеллектуальных программных агентов. Система защиты строится на архитектуре консоль/менеджер/агент. На каждую из контролируемых систем устанавливается программный агент, который и выполняет соответствующие настройки ПО и проверяет их правильность, контролирует целостность файлов, своевременность установки пакетов программных коррекций, а также выполняет другие полезные задачи по контролю защищенности АС. Управление агентами осуществляется по сети программой менеджером.

Менеджеры являются центральными компонентами подобных систем. Они посылают управляющие команды всем агентам контролируемого ими домена и сохраняют все данные, полученные от агентов в центральной базе данных. Администратор управляет менеджерами при помощи графической консоли, позволяющей выбирать, настраивать и создавать политики безопасности, анализировать изменения состояния системы, осуществлять ранжирование уязвимостей и т. п. Все взаимодействия между агентами, менеджерами и управляющей консолью осуществляются по защищенному клиент-серверному протоколу. Такой подход был использован при построении комплексной системы управления безопасностью организации Symantec ESM.

Другим широко используемым методом анализа защищенности является активное тестирование механизмов защиты путем эмуляции действий злоумышленника по осуществлению попыток сетевого вторжения в АС. Для этих целей применяются сетевые сканеры, эмулирующие действия потенциальных нарушителей. В основе работы сетевых сканеров лежит база данных, содержащая описание известных уязвимостей ОС, МЭ, маршрутизаторов и сетевых сервисов, а также алгоритмов осуществления попыток вторжения (сценариев атак). Рассматриваемые ниже сетевые сканеры Nessus и Symantec NetRecon являются достойными представителями данного класса программных средств анализа защищенности.

Таким образом, программные средства анализа защищенности условно можно разделить на два класса. Первый класс, к которому принадлежат сетевые сканеры, иногда называют средствами анализа защищенности сетевого уровня. Второй класс, к которому относятся все

остальные рассмотренные здесь средства, иногда называют средствами анализа защищенности системного уровня. Данные классы средств имеют свои достоинства и недостатки, а на практике взаимно дополняют друг друга.

Для функционирования сетевого сканера необходим только один компьютер, имеющий сетевой доступ к анализируемым системам, поэтому в отличие от продуктов, построенных на технологии программных агентов, нет необходимости устанавливать в каждой анализируемой системе своего агента (своего для каждой ОС).

К недостаткам сетевых сканеров можно отнести большие временные затраты, необходимые для сканирования всех сетевых компьютеров из одной системы, и создание большой нагрузки на сеть. Кроме того, в общем случае трудно отличить сеанс сканирования от действительных попыток осуществления атак. Сетевыми сканерами также с успехом пользуются злоумышленники.

Системы анализа защищенности, построенные на интеллектуальных программных агентах, являются потенциально более мощным средством, чем сетевые сканеры. Однако, несмотря на все свои достоинства, использование программных агентов не может заменить сетевого сканирования, поэтому эти средства лучше применять совместно. Кроме того, сканеры являются более простым, доступным, дешевым и, во многих случаях, более эффективным средством анализа защищенности.

**Средства анализа параметров защиты (Security Benchmarks)**

Уровень защищенности компьютерных систем от угроз безопасности определяется многими факторами. При этом одним из определяющих факторов является адекватность конфигурации системного и прикладного ПО, средств защиты информации и активного сетевого оборудования существующим рискам. Перечисленные компоненты АС имеют сотни параметров, значения которых оказывают влияние на защищенности системы, что делает их ручной анализ трудновыполнимой задачей. Поэтому в современных АС для анализа конфигурационных параметров системного и прикладного ПО, технических средств и средств защиты информации зачастую используются специализированные программные средства.

Анализ параметров защиты осуществляется по шаблонам, содержащим списки параметров и их значений, которые должны быть установлены для обеспечения необходимого уровня защищенности. Различные шаблоны определяют конфигурации для различных программно-технических средств.

Относительно коммерческих корпоративных сетей, подключенных к сети Интернет, можно говорить о некотором базовом уровне защищенности, который в большинстве случаев можно признать достаточным. Разработка спецификаций (шаблонов) для конфигурации наиболее распространенных системных программных средств, позволяющих

обеспечить базовый уровень защищенности, в настоящее время осуществляется представителями международного сообщества в лице организаций и частных лиц, профессионально занимающихся вопросами информационной безопасности и аудита АС, под эгидой международной организации Центр Безопасности Интернет (Center of Internet Security). На данный момент закончены, либо находятся в разработке следующие спецификации (Security Benchmarks):

Solaris (Level-1)

Windows 2000 (Level-1)

CISCO IOS Router (Level-1/Level-2)

Linux (Level-1)

HP-UX (Level-1)

AIX (Level-1)

Check Point FW-1/VPN-1 (Level-2)

Apache Web Server (Level-2)

Windows NT (Level-1)

Windows 2000 Bastion Host (Level-2)

Windows 2000 Workstation (Level-2)

Windows IIS5 Web Server (Level-2)

В приведенном списке спецификации первого уровня (Level-1) определяют базовый (минимальный) уровень защиты, который требуется обеспечить для большинства систем, имеющих подключения к Интернет. Спецификации второго уровня (Level-2) определяют продвинутый уровень защиты, необходимый для систем, в которых предъявляются повышенные требования по безопасности.

Перечисленные спецификации являются результатом обобщения мирового опыта обеспечения информационной безопасности.

Для анализа конфигурации компонентов АС на соответствие этим спецификациям используются специализированные тестовые программные средства (CIS-certified scoring tools).

В качестве примера рассмотрим спецификацию базового уровня защиты для ОС MS Windows 2000 и соответствующий программный инструментарий для анализа конфигурации ОС.

**Сетевые сканеры**

Основным фактором, определяющим защищенность АС от угроз безопасности, является наличие в АС уязвимостей защиты. Уязвимости защиты могут быть обусловлены как ошибками в конфигурации компонентов АС, так и другими причинами, в число которых входят ошибки и программные закладки в коде ПО, отсутствие механизмов безопасности, их

неправильное использование, либо их неадекватность существующим рискам, а также уязвимости, обусловленные человеческим фактором. Наличие уязвимостей в системе защиты АС, в конечном счете, приводит к успешному осуществлению атак, использующих эти уязвимости.

Сетевые сканеры являются, пожалуй, наиболее доступными и широко используемыми средствами анализа защищенности. Основной принцип их функционирования заключается в эмуляции действий потенциального злоумышленника по осуществлению сетевых атак. Поиск уязвимостей путем имитации возможных атак является одним из наиболее эффективных способов анализа защищенности АС, который дополняет результаты анализа конфигурации по шаблонам, выполняемый локально с использованием шаблонов (списков проверки). Сканер является необходимым инструментом в арсенале любого администратора либо аудитора безопасности АС.

Современные сканеры способны обнаруживать сотни уязвимостей сетевых ресурсов, предоставляющих те или иные виды сетевых сервисов. Их предшественниками считаются сканеры телефонных номеров (war dialers), использовавшиеся с начала 80-х и непотерявшие актуальности по сей день. Первые сетевые сканеры представляли собой простейшие сценарии на языке Shell, сканировавшие различные TCP-порты. Сегодня они превратились в зрелые программные продукты, реализующие множество различных сценариев сканирования.

Современный сетевой сканер выполняет четыре основные задачи:

Идентификацию доступных сетевых ресурсов;

Идентификацию доступных сетевых сервисов;

Идентификацию имеющихся уязвимостей сетевых сервисов;

Выдачу рекомендаций по устранению уязвимостей.

В функциональность сетевого сканера не входит выдача рекомендаций по использованию найденных уязвимостей для реализации атак на сетевые ресурсы. Возможности сканера по анализу уязвимостей ограничены той информацией, которую могут предоставить ему доступные сетевые сервисы.

Принцип работы сканера заключается в моделировании действий злоумышленника, производящего анализ сети при помощи стандартных сетевых утилит, таких как host, showmount, traceout, rusers, finger, ping и т. п. При этом используются известные уязвимости сетевых сервисов, сетевых протоколов и ОС для осуществления удаленных атак на системные ресурсы и осуществляется документирование удачных попыток.

В настоящее время существует большое количество как коммерческих, так и свободно распространяемых сканеров, как универсальных, так и специализированных, предназначенных для выявления только определенного класса уязвимостей. Многие из них

можно найти в сети Интернет. Число уязвимостей в базах данных современных сканеров медленно, но уверенно приближается к 1000.

Одним из наиболее продвинутых коммерческих продуктов этого класса является сетевой сканер NetRecon компании Symantec, база данных которого содержит около 800 уязвимостей UNIX, Windows и NetWare систем и постоянно обновляется через Web. Рассмотрение его свойств позволит составить представление о всех продуктах этого класса.

**Сетевой сканер NetRecon**

Сетевой сканер NetRecon является инструментом администратора безопасности, предназначенным для исследования структуры сетей и сетевых сервисов и анализа защищенности сетевых сред. NetRecon позволяет осуществлять поиск уязвимостей в сетевых сервисах, ОС, МЭ, маршрутизаторах и других сетевых компонентах. Например, NetRecon позволяет находить уязвимости в таких сетевых сервисах, как ftp, telnet, DNS, электронная почта, Web-сервер и др. При этом проверяются версии и конфигурации сервисов, их защищенность от сетевых угроз и устойчивость к попыткам проникновения. Для поиска уязвимостей используются как стандартные средства тестирования и сбора информации о конфигурации и функционировании сети, так и специальные средства, которые реализуют алгоритмы, эмулирующие действия злоумышленника по осуществлению сетевых атак.

Программа работает в среде ОС Windows NT и имеет удобный графический интерфейс, позволяющий определять параметры сканирования, наблюдать за ходом сканирования, генерировать и просматривать отчеты о результатах сканирования. Результаты отображаются в графической и в табличной форме в реальном масштабе времени.

Создаваемые NetRecon отчеты содержат подробную информацию о найденных уязвимостях, включая слабость паролей пользователей, подверженность определенных сервисов угрозам отказа в обслуживании, уязвимые для сетевых атак конфигурации ОС и многие другие. Наряду с сообщениями о найденных уязвимостях и их описаниями, приводятся рекомендации по их устранению. Отчет о результатах сканирования позволяет наметить план мероприятий по устранению выявленных недостатков.

NetRecon самостоятельно определяет конфигурацию сети и позволяет выбрать сетевые ресурсы для сканирования. Может осуществляться параллельное сканирование всех сетевых ресурсов, сканирование по диапазону сетевых адресов, сканирование отдельных систем или подсетей. Сеанс сканирования может включать в себя все виды проверок либо отдельные проверки по выбору пользователя. Глубина сканирования определяется продолжительностью сеанса сканирования, которая задается пользователем. Например, проверки, связанные с подбором пользовательских паролей по словарю, сопряжены с существенными временными затратами и не могут быть завершены в течение короткого сеанса сканирования.

NetRecon дает возможность пользователю отслеживать путь поиска уязвимости, представляющий собой последовательность проверок, производимых NetRecon, которая привела к выявлению данной уязвимости. Путь поиска уязвимости позволяет проследить действия возможного нарушителя, осуществляющего атаку на сетевые ресурсы.

Используемая NetRecon база данных содержит описание известных уязвимостей и сценариев атак. Она регулярно пополняется новыми данными. Обновление этой базы данных производится через Web-узел компании Symantec автоматически, при помощи механизма LiveUpdate.

**Сетевой сканер NESSUS**

Сетевой сканер Nessus может рассматриваться в качестве достойной альтернативы коммерческим сканерам. Nessus является свободно распространяемым и постоянно обновляемым программным продуктом. Удобный графический интерфейс позволяет определять параметры сеанса сканирования, наблюдать за ходом сканирования, создавать и просматривать отчеты.

По своим функциональным возможностям сканер защищенности Nessus находится в одном ряду, а по некоторым параметрам и превосходит такие широко известные коммерческие сканеры, как NetRecon компании Symantec, Internet Scanner компании ISS.

Версия 0.99 серверной части сканера Nessus была сертифицирована в Гостехкомиссии России (Сертификат N 361 от 18 сентября 2000 г.).

Nessus предоставляет очень широкие возможности по поиску уязвимостей корпоративных сетей и исследованию структуры сетевых сервисов. Помимо использования стандартных способов сканирования TCP и UDP портов, Nessus позволяет осуществлять поиск уязвимостей в реализациях протоколов управления сетью ICMP и SNMP.

Высокая скорость сканирования достигается за счет использования при реализации сканера Nessus многопотоковой архитектуры программирования, позволяющей осуществлять одновременное параллельное сканирование сетевых хостов. Для сканирования каждого хоста сервером nessusd создается отдельный поток выполнения.

При реализации Nessus использована нетипичная для сетевых сканеров клиент/серверная архитектура. Взаимодействие между клиентом и сервером осуществляется по защищенному клиент-серверному протоколу, предусматривающему использование надежной схемы аутентификации и шифрование передаваемых данных.

Все сценарии сканирования разделены на группы по типам реализуемых ими сетевых атак, обнаруживаемых уязвимостей, а также по видам тестируемых сетевых сервисов. Так, имеются специальные группы сценариев:

Backdoors для обнаружения "троянских" программ:

Gain Shell Remotely - для реализации атак на получение пользовательских полномочий на удаленной UNIX системе;

Firewalls - для тестирования МЭ;

FTP - для тестирования FTP-серверов;

Windows - для поиска уязвимостей Windows-систем и т.п.

Особую группу сценариев сканирования Denail of Service составляют атаки на отказ в обслуживании (DoS). Единственный способ убедиться в том, что сканируемая система подвержена той или иной DoS - это выполнить эту атаку и посмотреть на реакцию системы. Эта группа сценариев, однако, является потенциально опасной, т.к. их запуск может привести к непредсказуемым последствиям для сканируемой сети, включая сбои в работе серверов и рабочих станций, потерю данных и "полный паралич" корпоративной сети. Поэтому большинство DoS в данной группе по умолчанию отключено.

### 7.2.5. Архитектура систем аудита

У систем активного аудита целесообразно различать локальную и глобальную архитектуру.

**Локальная архитектура**

В рамках локальной архитектуры реализуются элементарные составляющие, которые затем могут быть объединены для обслуживания корпоративных систем.

Основные элементы локальной архитектуры и связи между ними показаны на рисунке 7.3. Первичный сбор данных осуществляют агенты, называемые также *сенсорами.* Регистрационная информация может извлекаться из системных или прикладных журналов (технически несложно получать ее и напрямую от ядра ОС), либо добываться из сети с помощью соответствующих механизмов активного сетевого оборудования или путем перехвата пакетов посредством установленной в режим мониторинга сетевой карты.

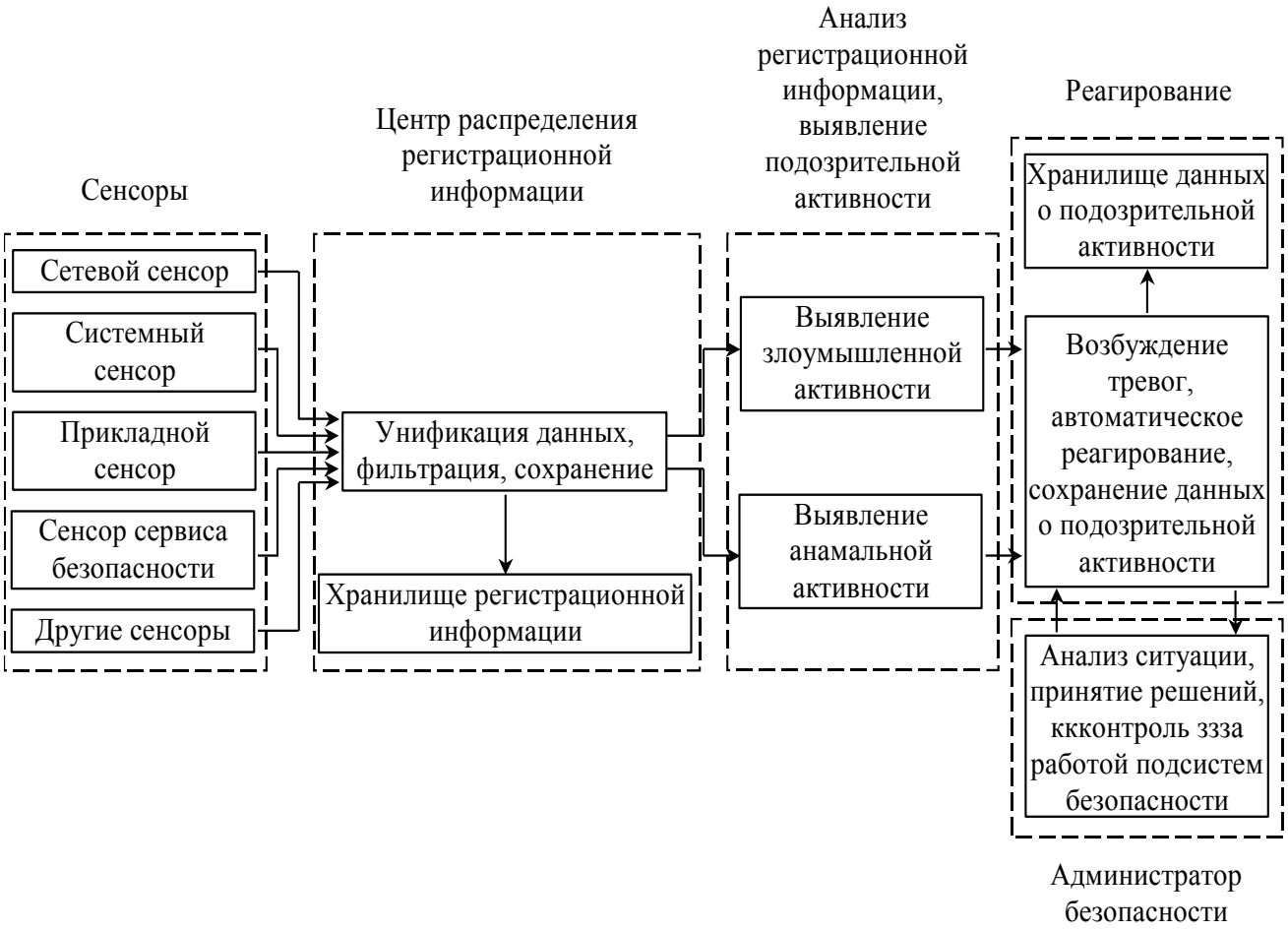



Рис. 7.3. Основные элементы локальной

архитектуры систем активного аудита.

На уровне агентов (сенсоров) может выполняться фильтрация данных с целью уменьшения их объема. Это требует от агентов некоторого интеллекта, но зато разгружает остальные компоненты системы.

Агенты передают информацию в центр распределения, который приводит ее к единому (стандартному для конкретной системы активного аудита) формату, возможно, осуществляет дальнейшую фильтрацию (редукцию), сохраняет в базе данных и направляет для анализа статистическому и экспертному компонентам. Один центр распределения может обслуживать несколько сенсоров.

Содержательный активный аудит начинается со статистического и экспертного компонентов (например, потому, что для однохостовых систем регистрационную информацию не надо каким-то особым образом извлекать и передавать). Мы детально рассмотрим их в двух следующих разделах.

Если в процессе статистического или экспертного анализа выявляется подозрительная активность, соответствующее сообщение направляется решателю, который определяет, является ли тревога оправданной, и выбирает способ реагирования.

Обычно, когда пишут о способах реагирования, перечисляют отправку сообщения на пейджер администратора, посылку электронного письма ему же и т.п., то есть имеют в виду “ручное” принятие мер после получения сигнала о подозрительной активности. К сожалению, многие современные атаки длятся секунды или даже доли секунды, поэтому включение в процесс реагирования человека вносит недопустимо большую задержку. Ответные меры должны быть в максимально возможной степени автоматизированы, иначе активность аудита во многом теряет смысл.

Автоматизация нужна еще и по той простой причине, что далеко не во всех организациях системные администраторы обладают достаточной квалификацией для адекватного реагирования на инциденты. Хорошая система активного аудита должна уметь внятно объяснить, почему она подняла тревогу, насколько серьезна ситуация и каковы рекомендуемые способы действия. Если выбор должен оставаться за человеком, то пусть он сводится к нескольким элементам меню, а не к решению концептуальных проблем.

**Глобальная архитектура**

Глобальная архитектура подразумевает организацию одно- и разно-ранговых связей между локальными системами активного аудита (см. рисунок 7.4). На одном уровне иерархии располагаются компоненты, анализирующие подозрительную активность с разных точек зрения. Например, на хосте могут располагаться подсистемы анализа поведения пользователей и приложений. Их может дополнять подсистема анализа сетевой активности. Когда один компонент обнаруживает что-то подозрительное, то во многих случаях целесообразно сообщить об этом соседям либо для принятия мер, либо для усиления внимания к определенным аспектам поведения системы.

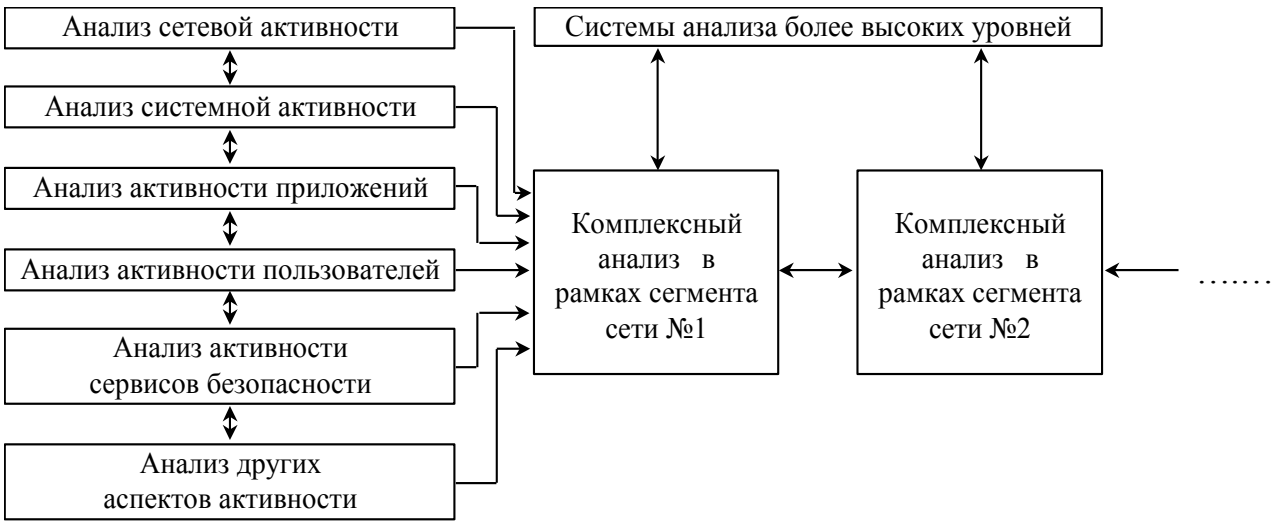



Рис. 7.4. Глобальная архитектура системы активного аудита.

Разно-ранговые связи используются для обобщения результатов анализа и получения целостной картины происходящего. Иногда у локального компонента недостаточно оснований для возбуждения тревоги, но «по совокупности» подозрительные ситуации могут быть объединены и совместно проанализированы, после чего порог подозрительности окажется превышенным. Целостная картина, возможно, позволит выявить скоординированные атаки на разные участки информационной системы и оценить ущерб в масштабе организации.

Очевидно, формирование иерархии компонентов активного аудита необходимо и для решения проблем масштабируемости, но этот аспект является стандартным для систем управления и мы не будем на нем останавливаться.

К числу важнейших архитектурных относится вопрос о том, какую информацию и в каких масштабах собирать и анализировать. Первые системы активного аудита были однохостовыми. Затем появились многохостовые конфигурации. Прорыву в области коммерческих продуктов мы обязаны сетевым системам, анализировавшим исключительно сетевые пакеты.

В настоящее время можно наблюдать конвергенцию архитектур, в результате чего рождаются комплексные системы, отслеживающие и анализирующие как компьютерную, так и сетевую регистрационную информацию.

Традиционным является вопрос: где размещать сенсоры систем активного аудита?

Столь же традиционный ответ гласит: «везде, где можно». Только анализ всех доступных источников информации позволит с достоверностью обнаруживать атаки и злоупотребления полномочиями и докапываться до их первопричин. Если вернуться к трактовке информационной системы в виде совокупности сервисов, то средства обнаружения атак должны располагаться перед защищаемыми ресурсами (имея в виду направление движения запросов к сервисам), а средства выявления злоупотреблений полномочиями - на самих сервисах. Обнаружение аномальной активности полезно во всех упомянутых точках. Только при таком размещении сенсоров будет выполнен важнейший принцип невозможности обхода защитных средств. Кроме того, будет минимизировано число сенсоров, что в условиях сегментации сетей и применения коммутационных технологий также оказывается проблемой.

Для того, чтобы система активного аудита, особенно распределенная, была практически полезной, необходимо обеспечить целостность анализируемой и передаваемой информации, а также целостность самой программной системы и ее живучесть в условиях отказа или компрометации отдельных компонентов (зачастую атака направляется сначала на средства безопасности, а уже потом - на прикладные компоненты). Ясно, что это проблема всех

распределенных систем, и для ее решения служат сервисы взаимной аутентификации и контроля целостности (в том числе проверка подлинности источника данных).

### 7.2.6. Требования к системам активного аудита

В этом пункте рассмотрим требования к системам активного аудита, существенные с точки зрения заказчиков. На первое место следует поставить требование полноты. Это весьма емкое понятие, включающее в себя следующие аспекты:

Полнота отслеживания информационных потоков к сервисам. Активный аудит должен охватывать все потоки всех сервисов. Это означает, что система активного аудита должна содержать сетевые и системные сенсоры, анализировать информацию на всех уровнях - от сетевого до прикладного. Очевидно, из рассматриваемого аспекта полноты вытекает требование расширяемости, поскольку ни один программный продукт не может быть изначально настроен на все сервисы.

Полнота спектра выявляемых атак и злоупотреблений полномочиями. Данное требование означает не только то, что у системы должен быть достаточно мощный язык описания подозрительной активности (как атак, так и злоупотреблений полномочиями). Этот язык должен быть прост, чтобы заказчики могли производить настройку системы в соответствии со своей политикой безопасности. Поставщик системы активного аудита должен в кратчайшие сроки (порядка суток) передавать заказчику сигнатуры новых атак. Система должна уметь выявлять аномальную активность, чтобы справляться с заранее неизвестными способами нарушений.

Достаточная производительность. Система активного аудита должна справляться с пиковыми нагрузками защищаемых сервисов.

Пропуск даже одного сетевого пакета может дать злоумышленнику шанс на успешную атаку. Если известно, что система активного аудита обладает недостаточной производительностью, она может стать объектом атаки на доступность, на фоне которой будут развиваться другие виды нападения. Для локальных сетей стандартными стали скорости 100 Мбит/с. Это требует от системы активного аудита очень высокого качества реализации, мощной аппаратной поддержки. Если учесть, что защищаемые сервисы находятся в постоянном развитии, то станет понятно, что требование производительности одновременно является и требованием масштабируемости.

Помимо полноты, системы активного аудита должны удовлетворять следующим требованиям:

Минимум ложных тревог. В абсолютном выражении допустимо не более одной ложной тревоги в час (лучше, если их будет еще на порядок меньше). При интенсивных потоках данных между сервисами и их клиентами подобное требование оказывается весьма жестким. Пусть, например, в секунду по контролируемому каналу проходит 1000 пакетов. За час

пакетов будет 3 600 000. Можно предположить, что почти все они не являются злоумышленными. И только один раз система активного аудита имеет право принять «своего» за «чужого», то есть вероятность ложной тревоги должна составлять в данном случае не более $3 \cdot 10^{-7}$.

Умение объяснять причину тревоги. Выполнение этого требования во-первых, помогает отличить обоснованную тревогу от ложной, во-вторых, помогает определить первопричину инцидента, что важно для оценки его последствий и недопущения повторных нарушений. Даже если реагирование на нарушение производится в автоматическом режиме, должна оставаться возможность последующего разбора ситуации специалистами.

Интеграция с системой управления и другими сервисами безопасности. Интеграция с системой управления имеет две стороны. Во-первых, сами средства активного аудита должны управляться (устанавливаться, конфигурироваться, контролироваться) наравне с другими инфраструктурными сервисами. Во-вторых, активный аудит может (и должен) поставлять данные в общую базу данных управления. Интеграция с сервисами безопасности необходима как для лучшего анализа ситуации (например, с привлечением средств контроля целостности), так и для оперативного реагирования на нарушения (средствами приложений, операционных систем или межсетевых экранов).

Наличие технической возможности удаленного мониторинга информационной системы. Это спорное требование, поскольку не все организации захотят оказаться под чьим-то «колпаком». Тем не менее, с технической точки зрения подобная мера вполне оправдана, поскольку большинство организаций не располагает квалифицированными специалистами по информационной безопасности. Удаленный мониторинг может быть использован и для бесспорных целей, таких как контроль из штаб-квартиры за работой удаленных отделений.

Сформулированные требования можно считать максималистскими. По-видимому, ни одна современная коммерческая система, ни один поставщик не удовлетворяют им в полной мере, однако, без их выполнения активный аудит превращается из серьезного оборонительного оружия в сигнализацию для отпугивания детей младшего школьного возраста. Захотят ли заказчики платить деньги за подобные игрушки? Нет, конечно, если только они достаточно разбираются в предмете.

Системы активного аудита принадлежат к области высоких технологий. У них развитая математическая база, продвинутая архитектура, они вобрали в себя знания по информационной безопасности. Мало кто из распространителей понимает, как работает то, что они продают; им остается пересказывать рекламные буклеты производителей, где, конечно, все выглядит замечательно. Заказчики тоже не обязаны вдаваться в детали, но они должны знать, о чем спрашивать поставщиков. Не всегда те смогут ответить, но и молчание многое скажет заказчику.

### 7.2.7. Возможные критерии оценки систем активного аудита

Предлагаемые критерии имеют много общего с критериями оценки систем управления. Это не случайно, так как активный аудит и управление по сути своей близки.

Под подозрительной активностью понимается поведение пользователя или компонента информационной системы, являющееся нетипичным для данного пользователя (компонента) или (в соответствии с заранее определенными критериями) злоумышленным.

Рассматриваемые в данных критериях системы должны выявлять подозрительную активность и предоставлять средства для автоматического реагирования на нетипичные или злоумышленные действия. Кроме того, они должны удовлетворять общим требованиям к сервисам информационной безопасности.

Основными показателями, характеризующими системы активного аудита, являются:

спектр контролируемых объектов;

спектр и степень детальности отслеживаемых характеристик;

расширяемость системы;

настраиваемость системы;

степень автоматизации функционирования системы;

возможность работы в рамках распределенных систем;

возможность работы в реальном масштабе времени;

технологичность системы.

**Показатели, используемые для оценки систем активного аудита**

Выделяются следующие показатели:

Отслеживание поведения пользователей и компонентов информационной системы.

Обеспечение конфиденциальности и целостности регистрационной информации.

Выявление злоумышленного поведения.

Выявление нетипичного поведения.

Администрирование.

Контроль целостности.

Масштабируемость.

Доступность.

Восстановление.

Документация.

Тестирование.

Отслеживание поведения пользователей и компонентов информационной системы

Возможность отслеживания базового набора характеристик поведения пользователей и компонентов информационной системы.

Возможность изменения (в том числе пополнения) набора отслеживаемых характеристик.

Возможность отслеживания характеристик в распределенных системах.

Возможность отслеживания поведения отдельных пользователей и компонентов информационной системы в реальном масштабе времени.

Возможность задания способа информирования администратора безопасности о выходе отслеживаемых характеристик за допустимые рамки.

Возможность задания способа автоматического реагирования на выход отслеживаемых характеристик за допустимые рамки.

Обеспечение конфиденциальности и целостности регистрационной информации

Защита регистрационной информации от несанкционированного доступа в рамках отдельных систем.

Контроль целостности (взаимной согласованности) регистрационной информации в рамках распределенных систем.

Защита регистрационной информации от несанкционированного доступа в рамках распределенных систем.

Возможность задания способа информирования администратора безопасности о нарушении целостности и/или конфиденциальности регистрационной информации.

Возможность задания способа автоматического реагирования на нарушение целостности и/или конфиденциальности регистрационной информации.

Выявление злоумышленного поведения

Возможность выявления базового набора злоумышленных действий.

Возможность пополнения базы правил, описывающих злоумышленные действия.

Возможность настройки базы правил на конкретные информационные сервисы.

Возможность выявления злоумышленных действий, распределенных во времени

Возможность выявления злоумышленных действий в распределенных системах

Возможность выявления злоумышленных действий в реальном масштабе времени

Возможность задания способа информирования администратора безопасности о выявленных злоумышленных действиях.

Возможность задания уровня детализации информации, подтверждающей наличие злоумышленных действий.

Возможность задания способа автоматического реагирования на выявленные злоумышленные действия.

Наличие средств автоматической проверки согласованности базы правил в рамках распределенной конфигурации.

Наличие средств анализа злоумышленных действий с выдачей рекомендаций по предотвращению подобных действий в будущем.

Наличие средств прогнозирования злоумышленных действий.

Выявление нетипичного поведения.

Наличие подсистемы статистического анализа для выявления нетипичного поведения.

Возможность выявления нетипичного поведения при использовании базового набора информационных сервисов.

Возможность пополнения и/или изменения набора контролируемых аспектов поведения.

Возможность настройки на конкретные информационные сервисы.

Наличие средств для изменения параметров статистического анализа с целью обеспечения заданного соотношения между ошибками первого рода (отсутствие реакции на нетипичное поведение) и ошибками второго рода (ложное срабатывание).

Возможность выявления нетипичного поведения в рамках распределенной системы.

Возможность выявления нетипичного поведения в реальном масштабе времени

Возможность задания способа информирования администратора безопасности о выявленном нетипичном поведении.

Возможность задания уровня детализации информации, подтверждающей наличие нетипичного поведения

Возможность задания способа автоматического реагирования на выявленное нетипичное поведение

Наличие средств автоматической проверки согласованности статистических параметров в рамках распределенной конфигурации

Наличие средств автоматической оценки соотношения между ошибками первого и второго рода при заданных статистических параметрах

Администрирование

Идентификация и аутентификация администраторов в рамках локальных систем

Идентификация и аутентификация администраторов в рамках распределенных систем

Регистрация административных действий в рамках локальных систем

Регистрация административных действий в рамках распределенных систем

Возможность централизованного выявления подозрительной активности в рамках распределенных систем

Возможность централизованного администрирования распределенных систем активного аудита

Контроль целостности

Наличие средств контроля целостности программной и информационной частей системы активного аудита (локальные, распределенные, использующие аттестованные алгоритмы)

Масштабируемость

Наличие средств масштабирования по числу отслеживаемых пользователей и компонентов информационной системы: возможность группирования пользователей (компонентов) с однородными характеристиками.

Наличие средств масштабирования по размеру обслуживаемой информационной системы, возможность варьирования между распределенной и централизованной обработкой регистрационной информации, возможность организации иерархии обрабатывающих центров.

Доступность

Наличие средств обеспечения высокой доступности: сбои и отказы отдельных подсистем или компонентов системы активного аудита не должны нарушать работоспособность других подсистем (компонентов).

Восстановление

Наличие средств восстановления после сбоев и отказов, в том числе отказов отдельных элементов распределенной системы.

Документация

Руководство администратора системы активного аудита (локальные, распределенные, с использованием аттестованных алгоритмов контроля целостности).

Руководство программиста (описание программных интерфейсов с системой сбора и анализа регистрационной информации).

Конструкторская (проектная) документация.

Тестовая документация.

Тестирование

Обеспечение возможности регламентного тестирования средств сбора регистрационной информации, подсистем выявления злоумышленного и нетипичного поведения, средств контроля целостности, средств администрирования, средств восстановления.

### 7.2.8. Результаты аудита

Результаты аудита ИС организации можно разделить на три основных группы:

1 Организационные: планирование, управление, документооборот функционирования ИС.

2 Технические: сбои, неисправности, оптимизация работы элементов ИС, непрерывное обслуживание, создание инфраструктуры и т.д.

3 Методологические: подходы к решению проблемных ситуаций, управлению и контролю, общая упорядоченность и структуризация.

Проведенный аудит позволит обоснованно создать следующие документы:

Долгосрочный план развития ИС.

Политика безопасности ИС организации.

Методология работы и доводки ИС организации.

План восстановления ИС в чрезвычайной ситуации.

## 8. Компьютерные лабораторные работы

**Лабораторная работа 1. Исследование защищенности беспроводных сетей передачи данных**

**1. Цель работы**

Объектом исследования является беспроводная высокозащищенная сеть передачи данных. Беспроводная высокозащищенная сеть передачи данных, работающая по стандарту 802.11g в диапазоне частот 2.4-2.483 ГГц. Скорость передачи данных составляет не менее 24 Мбит/сек, в расчете на одного пользователя. В системе, обеспечивается бесшовный роуминг, применяется надежная двухсторонняя аутентификация, для шифрования передаваемой по радиоканалу информации применяется алгоритм шифрования AES. В сети применяется оборудование компании D-Link.

Основными задачами сети являются:

- - обеспечение роуминга на территории охваченной беспроводной сетью;
- - определение зон покрытия каждой из точек доступа и частотное планирование;
- - обеспечение заданной скорости передачи;
- - выбор надежных метод аутентификации и шифрования трафика;
- - выбор программно – аппаратного комплекса.

**2. Краткие теоретические сведения**

Беспроводные сети стандарта 802.11 или Wi-Fi, приобретают все большую популярность. В качестве среды передачи используется радиоканал. По мере развития стандарта увеличивалась скорость передачи, совершенствовались методы защиты передаваемой информации. На сегодняшний день уровень защищенности трафика сравним с таковым в проводных сетях Ethernet, однако скорости передачи информации все еще значительно меньше чем в проводных сетях. Стандарты 802.11a/g предоставляют в распоряжение пользователей полудуплексный канал с пропускной способностью 54 Мбит/с. Однако беспроводные сети дарят пользователям мобильность, быстрее развертываются и в некоторых случаях дешевле. Беспроводные сети развертываются, как правило, там, где не нужны высокие скорости передачи (кафе, вокзалы, аэропорты).

**Назначение и область применения системы**

Сеть стандарта 802.11g относится к классу беспроводных сетей, т.е. в качестве среды передачи используется радиоканал. Передача ведется в диапазоне частот 2.4 ГГц. Беспроводные сети обеспечивают мобильность пользователю имеющему портативный ПК, технологии роуминга в сетях 802.11 позволяют абоненту перемещаться в пределах зоны обслуживания и при этом сохранять текущие соединения. Во многих компаниях используются телефоны стандарта 802.11, их применение дает возможность владельцам без потери связи перемещаться по зоне покрытой сетью. Такая связь значительно дешевле сотовой, так как затраты связаны только с приобретением и настройкой оборудования. Развертывать беспроводные сети значительно быстрее и в некоторых случаях дешевле, к тому же конфигурацию (зону покрытия, количество точек) можно менять без значительных затрат и в короткое время.

Основным назначением беспроводных сетей, как и любых сетей передачи данных, является предоставление пользователям возможности обмениваться данными друг с другом и предоставление доступа в Интернет. Важными характеристиками сети являются скорость передачи и задержки при передаче пакетов. Сети стандарта 802.11g предлагают потребителю полудуплексный канал с максимальной скоростью передачи 54 Мбит/с. Если предположить что одна точка доступа обслуживает 16 клиентов, то каждому из них достанется по 3.4 Мбит/с. Задержки в беспроводных сетях несколько больше чем в проводных, и сильно зависят от зашумленности эфира, однако это не мешает успешно передавать голосовой трафик.

**Функции сети**

Основные функции:

- - предоставление доступа к ресурсам корпоративной сети;
- - защита передаваемой по сети информации;
- - надежная аутентификация пользователей.

**Состав сети**

Исходя из перечисленных функций можно указать минимальный состав системы:

1. Клиентские устройства. Будем понимать любое оборудование пользователя соответствующее стандарту 802.11g. (например ПК или ноутбук с беспроводными сетевым адаптером).

2. Устройство беспроводного доступа в ЛВС. Программно-аппаратный комплекс, позволяющий передавать данные по беспроводному каналу (точка доступа).

3. Беспроводной коммутатор, в задачи которого входит обеспечение роуминга между точками доступа.

4. Система аутентификации. Система централизованного доступа на базе сервера RADIUS (Remote Access Dial-In User Service – сервис дистанционного пользовательского доступа).

**Методы построения современных беспроводных сетей**

Можно выделить три основных варианта построения (топологий) беспроводных сетей стандарта 802.11:

- - независимые базовые зоны обслуживания (independent basic service sets, IBSSs);
- - базовые зоны обслуживания (basic service sets, BSSs);
- - расширенные зоны обслуживания (extended service sets, ESSs).

Зона обслуживания (service set) в данном случае — это логически сгруппированные устройства. Технология WLAN обеспечивает доступ к сети путем передачи широковещательных сигналов через эфир на несущей в диапазоне радиочастот. Принимающая станция может получать сигналы в диапазоне работы нескольких передающих станций. Передающая станция вначале передает идентификатор зоны обслуживания (service set identifier, SSID). Станция-приемник использует SSID для фильтрации получаемых сигналов и выделения того, который ей нужен.

**Независимые базовые зоны обслуживания IBSS**

IBSS представляет собой группу работающих в соответствии со стандартом 802.11 станций, связывающихся непосредственно одна с другой. IBSS также называют специальной, или неплановой (ad-hoc) сетью, потому что она, по сути, представляет собой простую одноранговую WLAN. Специальная сеть, или независимая базовая зона обслуживания (IBSS), возникает, когда отдельные устройства-клиенты формируют самоподдерживающуюся сеть без использования отдельной точки доступа (рис. 1).

Рис. 1. Структура IBSS

При создании таких сетей не разрабатывают какие-либо карты места их развертывания и предварительные планы, поэтому они обычно невелики и имеют ограниченную протяженность, достаточную для передачи совместно используемых данных при возникновении такой необходимости. В отличие от варианта использования расширенной зоны обслуживания (ESS), клиенты непосредственно устанавливают соединения друг с другом, в результате чего создается

только одна базовая зона обслуживания (BSS), не имеющая интерфейса для подключения к проводной локальной сети (т.е. отсутствует какая-либо распределительная система, которая необходима для объединения BSS и организации таким образом ESS). На данный момент не существует каких-либо оговоренных стандартом ограничений на количество устройств, которые могут входить в одну независимую базовую зону обслуживания. Но, поскольку каждое устройство является клиентом, зачастую определенное число членов IBSS не может связываться один с другим вследствие проблемы скрытого узла (hidden node issue). Несмотря на это, в IBSS не существует какого-либо механизма для реализации функции ретрансляции.

Поскольку в IBSS отсутствует точка доступа, распределение времени (timing) осуществляется нецентрализованно. Клиент, начинающий передачу в IBSS, задает сигнальный (его еще называют маячковый) интервал (beacon interval) для создания набора моментов времени передачи маячкового сигнала (set of target beacon transmission time, TBTT). Когда завершается TBTT, каждый клиент IBSS выполняет следующее. Приостанавливает все несработавшие таймеры задержки (backoff timer) из предыдущего TBTT. Определяет новую случайную задержку.

- Если маячковый сигнал поступает до окончания случайной задержки, возобновляет работу приостановленных таймеров задержки. Если никакой маячковый сигнал не поступает до окончания случайной задержки, посылает маячковый сигнал и возобновляет работу приостановленных таймеров задержки.

Отсюда видно, что распределение времени для передачи маячковых сигналов осуществляется в специальных сетях не точкой доступа и не каким-то одним из клиентов. Поскольку такой схеме связи присуща проблема скрытого узла, вполне возможно, что в течение сигнального интервала будет передано множество маячковых сигналов от разных клиентов и другие клиенты получат множество маячковых сигналов. Однако, стандарт вполне допускает такую ситуацию и никаких проблем не возникает, поскольку клиенты ожидают приема только первого маячкового сигнала, относящегося к их собственному таймеру случайной задержки.

В маячковые сигналы встроена функция синхронизации таймера (timer synchronization function, TSF). Каждый клиент сравнивает TSF в маячковом сигнале со своим собственным таймером и, если полученное значение больше, считает, что часы передающей станции идут быстрее и подстраивает свой собственный таймер в соответствии с полученным значением. Это имеет долговременный эффект синхронизации работы всей неплановой сети по клиенту с самым быстрым таймером. В больших распределенных неплановых сетях, когда многие клиенты не могут связываться напрямую, может понадобиться некоторое время для достижения синхронизации всех клиентов.

**Базовые зоны обслуживания BSS**

BSS — это группа работающих по стандарту 802.11 станций, связывающихся одна с другой. Технология BSS предполагает наличие особой станции, которая называется точка доступа (access

point) (рис. 2).

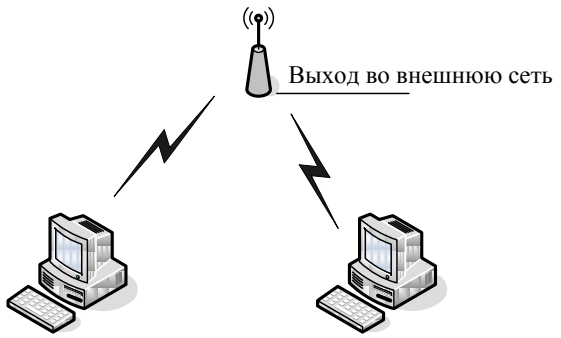



Рис. 2. Структура BSS

Точка доступа — это центральный пункт связи для всех станций BSS. Клиентские станции не связываются непосредственно одна с другой. Вместо этого они связываются с точкой доступа, а уже она направляет фреймы станции-адресату. Точка доступа может иметь порт восходящего канала (uplink port), через который BSS подключается к проводной сети (например, восходящий канал Ethernet). Поэтому BSS иногда называют инфраструктурой BSS.

**Расширенные зоны обслуживания ESS**

Несколько инфраструктур BSS могут быть соединены через их интерфейсы восходящего канала. Там, где действует стандарт 802.11, интерфейс восходящего канала соединяет BSS с распределительной системой (distribution system, DS). Несколько BSS, соединенных между собой через распределительную систему, образуют расширенную зону обслуживания (ESS). Восходящий канал к распределительной системе не обязательно должен использовать проводное соединение. На рисунке 4.3 представлен пример структуры ESS. Спецификация стандарта 802.11 оставляет возможность реализации этого канала в виде беспроводного. Но чаще восходящие каналы к распределительной системе представляют собой каналы проводной Ethernet.

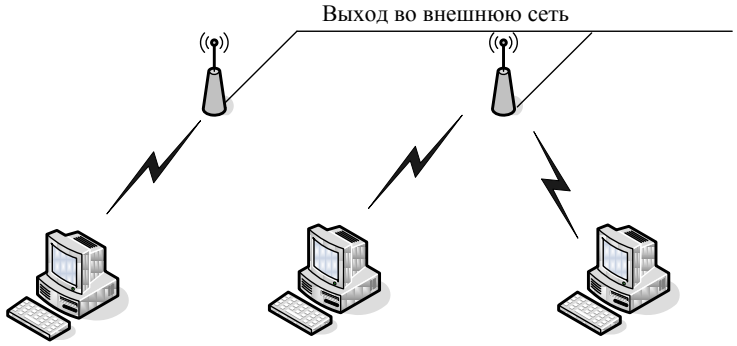



Рис. 3. Структура ESS

**Обзор механизмов доступа к среде**

Предотвращение коллизий является ключевым моментом для беспроводных сетей, поскольку последние не имеют явного механизма для их обнаружения. При использовании технологии CSMA/CA, коллизия обнаруживается только при неполучении передающей станцией ожидаемого подтверждения. Реализация технологии CSMA/CA стандартом 802.11 осуществляется при использовании распределенной функции координации (distributed coordination function, DCF). Для предотвращения коллизий в сетях с точкой доступа предусмотрен опциональный механизм централизованной функции координации PCF (Point Coordination Function).

Функция распределенной координации DCF

На первый взгляд организовать совместный доступ к среде передачи данных достаточно просто. Для этого необходимо лишь обеспечить, чтобы все узлы передавали данные только тогда, когда среда является свободной, то есть когда ни один из узлов не производит передачу данных. Однако такой механизм неизбежно приведет к коллизиям, поскольку велика вероятность того, что два или более узлов одновременно, пытаясь получить доступ к среде передачи данных, решат, что среда свободна и начнут одновременную передачу. Именно поэтому необходимо разработать алгоритм, способный снизить вероятность возникновения коллизий и в то же время гарантировать всем узлам сети равноправный доступ к среде передачи данных.

Одним из вариантов организации такого равноправного доступа к среде передачи данных является функция распределенной координации (DCF). Эта функция основана на методе коллективного доступа с обнаружением несущей и механизмом избежания коллизий (Carrier Sense Multiple Access/Collision Avoidance, CSMA/CA). При такой организации каждый узел, прежде чем начать передачу, «прослушивает» среду, пытаясь обнаружить несущий сигнал, и только при условии, что среда свободна, может начать передачу данных.

Однако, в этом случае велика вероятность возникновения коллизий: когда два или более узлов сети одновременно (или почти одновременно) решат, что среда свободна, и начнут предавать данные. Для того чтобы снизить вероятность возникновения подобных ситуаций, используется механизм избежания коллизий (Collision Avoidance, CA). Суть данного механизма заключается в следующем. Каждый узел сети, убедившись, что среда свободна, прежде чем начать передачу, выжидает в течение определенного промежутка времени. Этот промежуток является случайным и складывается из двух составляющих: обязательного промежутка DIFS (DCF Interframe Space) и выбираемого случайным образом промежутка обратного отсчета (backoff time). В результате каждый узел сети перед началом передачи выжидает в течение случайного промежутка времени, что, естественно, значительно снижает вероятность возникновения коллизий, поскольку вероятность того, что два узла сети будут выжидать в

течение одного и того же промежутка времени, чрезвычайно мала.

Для того чтобы гарантировать всем узлам сети равноправный доступ к среде передачи данных, необходимо соответствующим образом определить алгоритм выбора длительности промежутка обратного отсчета (backoff time). Промежуток обратного отсчета хотя и является случайным, но в то же время определяется на основании множества некоторых дискретных промежутков времени, то есть, равен целому числу элементарных временных промежутков, называемых тайм-слотами (SlotTime). Для выбора промежутка обратного отсчета каждый узел сети формирует так называемое окно конкурентного доступа (Contention Window, CW), использующееся для определения количества тайм-слотов, в течение которых станция выжидала перед передачей. Фактически окно CW – это диапазон для выбора количества тайм-слотов, причем минимальной размер окна определяется в 31 тайм-слот, а максимальный размер — в 1023 тайм-слота. Промежуток обратного отсчета определяется как количество тайм-слотов, определяемое исходя из размера окна CW:

$$Backoff\ time = Random[CW_{min}, CW_{max}] \times SlotTime$$

Когда узел сети пытается получить доступ к среде передачи данных, то после обязательного промежутка ожидания DIFS запускается процедура обратного отсчета, то есть включается обратный отсчет счетчика тайм-слотов начиная от выбранного значения окна CW. Если в течение всего промежутка ожидания среда оставалась свободной (счетчик обратного отсчета равен нулю), то узел начинает передачу.

После успешной передачи окно CW формируется вновь. Если же за время ожидания передачу начал другой узел сети, то значение счетчика обратного отсчет останавливается и передача данных откладывается. После того как среда станет свободной, данный узел снова начинает процедуру обратного отсчета, но уже с меньшим размером окна CW, определяемого предыдущим значением счетчика обратного отсчета и соответственно с меньшим значением времени ожидания. При этом очевидно, что чем большее число раз узел откладывает передачу по причине занятости среды, тем выше вероятность того, что в следующий раз он получит доступ к среде передачи данных (рис. 4).

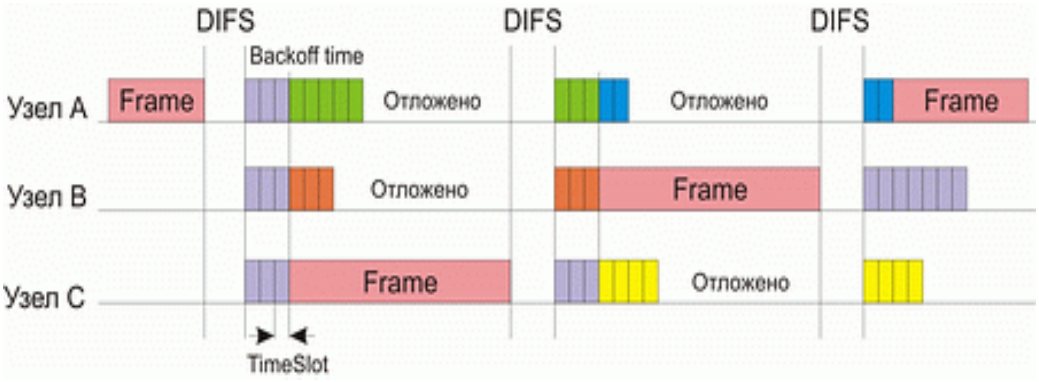


Рис. 4. Реализация равноправного доступа к среде передачи данных в методе DCF

Рассмотренный алгоритм реализации коллективного доступа к среде передачи данных гарантирует равноправный доступ всех узлов сети к среде. Однако при таком подходе вероятность возникновения коллизий хотя и мала, но все-таки существует. Понятно, что снизить вероятность возникновения коллизий можно путем увеличения максимального размера формируемого окна CW. В то же время это увеличит времена задержек при передачи и тем самым снизит производительность сети. Поэтому в методе DCF для минимизации коллизий используется следующий алгоритм. После каждого успешного приема кадра принимающая сторона через короткий промежуток SIFS (Short Interframe Space) подтверждает успешный прием, посылая ответную квитанцию – кадр ACK (ACKnowledgement) (рис. 5). Если в процессе передачи данных возникла коллизия, то передающая сторона не получает кадр ACK об успешном приеме. В этом случае размер CW-окна для передающего узла увеличивается почти вдвое. Так, если для первой передачи размер окна равен 31 слоту, то для второй попытки передачи он уже составляет 63 слота, для третьей – 127 слотов, для четвертой – 255, для пятой – 511, а для всех последующих – 1023 слота. То есть для каждой i-й передачи (если все предыдущие оказались безуспешными) размер CW-окна увеличивается по следующему правилу:

$$CW_i = 2CW_{i-1} + 1$$

Таким образом, увеличение размера окна происходит динамически по мере роста числа коллизий, что позволяет, с одной стороны, уменьшить временные задержки и, с другой стороны, снизить вероятность возникновения коллизий.

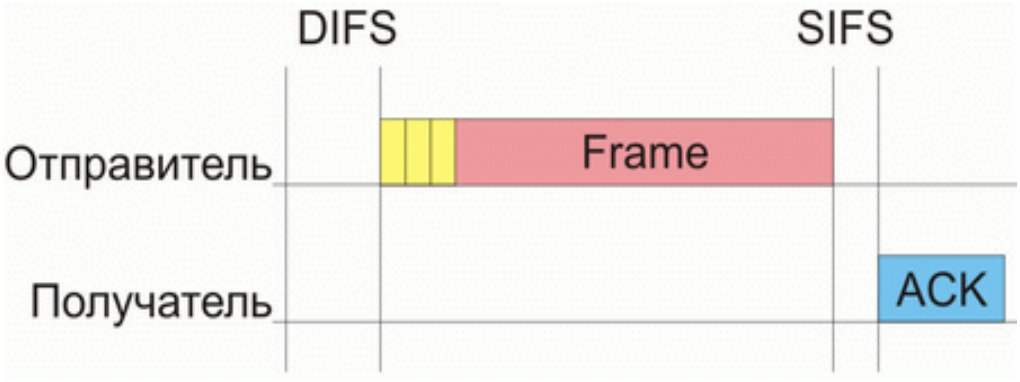



Рис. 5. Кадры квитанции, отсылаемые в случае успешной передачи данных

Говоря об алгоритме реализации равноправного доступа к среде передачи данных, необходимо также учитывать и размер кадра данных. Действительно, если кадры данных будут

слишком большими, то при возникновении коллизий придется повторно передавать большой объем информации, что приведет к снижению производительности сети. Кроме того, при большом размере кадров данных узлы сети вынуждены простаивать в течение довольно продолжительного времени, прежде чем начать передачу.

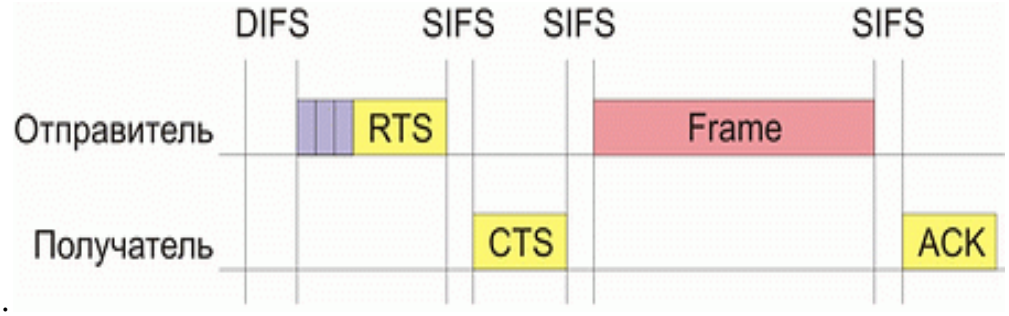
В то же время использование кадров данных небольшого размера, хотя и позволяет гарантировать равноправный доступ всех узлов к среде передачи данных и минимизирует издержки при возникновении коллизий, не может не отразиться негативно на полезном сетевом трафике. Дело в том, что каждый кадр наряду с полезной информацией содержит информацию служебную (заголовок кадра). При уменьшении размера кадра сокращается величина именно полезной информации (пользовательских данных), что обусловливает передачу по сети избыточного количества служебной информации. Поэтому размер кадра — это своего рода золотая середина, от правильного выбора которой зависит эффективность использования среды передачи данных.

Рассмотренный механизм регламентирования коллективного доступа к среде передачи данных имеет одно узкое место — так называемую проблему скрытых узлов. Из-за наличия естественных препятствий возможна ситуация, когда два узла сети не могут «слышать» друг друга напрямую. Такие узлы называют скрытыми.

Для того чтобы разрешить проблему скрытых узлов, функция DCF опционально предусматривает возможность использования алгоритма RTS/CTS.

Алгоритм RTS/CTS

В соответствии с алгоритмом RTS/CTS каждый узел сети, перед тем как послать данные в «эфир», сначала отправляет специальное короткое сообщение, которое называется RTS (Ready To Send) и означает готовность данного узла к отправке данных. Такое RTS-сообщение содержит информацию о продолжительности предстоящей передачи и об адресате и доступно всем узлам в сети (если только они не скрыты от отправителя). Это позволяет другим узлам задержать передачу на время, равное объявленной длительности сообщения. Приемная станция, получив сигнал RTS, отвечает посылкой сигнала CTS (Clear To Send), свидетельствующего о готовности станции к приему информации. После этого передающая станция посылает пакет данных, а приемная станция должна передать кадр ACK, подтверждающий безошибочный прием. Последовательность отправки кадров между двумя узлами сети показана на рис.6.




.

Рис. 6. Взаимодействие между двумя узлами сети в соответствии с алгоритмом RTS/CTS

Теперь рассмотрим ситуацию, когда сеть состоит из четырех узлов: A, B, C и D (рис. 4.4). Предположим, что узел C находится в зоне досягаемости только узла A, узел A находится в зоне досягаемости узлов C и B, узел B находится в зоне досягаемости узлов A и D, а узел D находится в зоне досягаемости только узла B. То есть в такой сети имеются скрытые узлы: узел C скрыт от узлов B и D, узел A скрыт от узла D.

В подобной сети алгоритм RTS/CTS позволяет справиться с проблемой возникновения коллизий, которая не решается посредством рассмотренного базового способа организации коллективного доступа в DCF. Действительно, пусть узел A пытается передать данные узлу B. Для этого он посылает сигнал RTS, который, помимо узла B, получает также узел C, но не получает узел D. Узел C, получив данный сигнал, блокируется, то есть приостанавливает попытки передавать сигнал до момента окончания передачи между узлами A и B. Узел B, в ответ на полученный сигнал RTS, посылает кадр CTS, который получают узлы A и D. Узел D, получив данный сигнал, также блокируется на время передачи между узлами A и B.

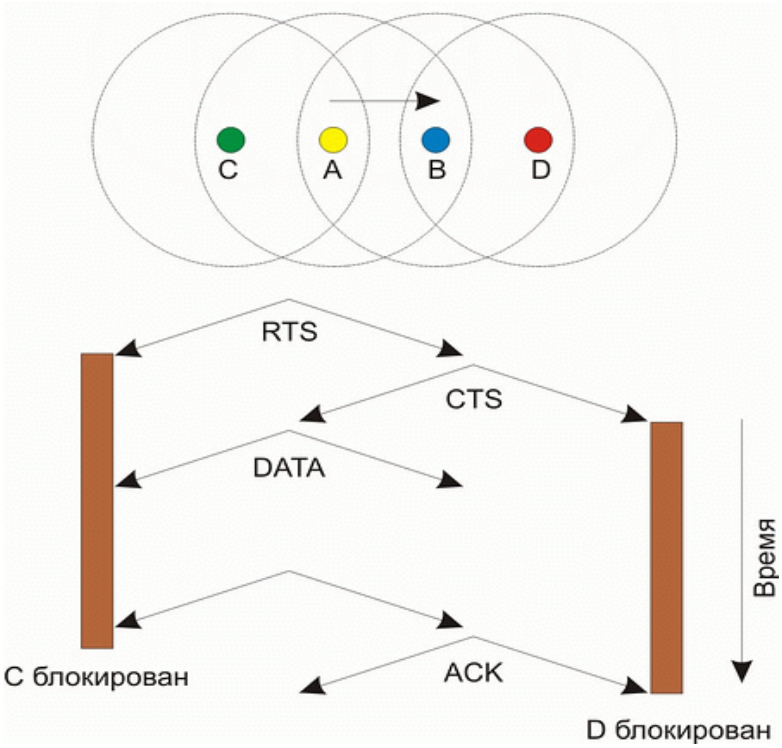



Рис.7. Решение проблемы скрытых узлов в алгоритме RTS/CTS

У алгоритма RTS/CTS имеются свои подводные камни, которые в определенных ситуациях могут приводить к снижению эффективности использования среды передачи данных. К примеру, в некоторых ситуациях возможно такое явление, как распространение эффекта ложных блокировок узлов, что в конечном счете может привести к ступору в сети.

Рассмотрим, к примеру, сеть, показанную на рис. 4.5. Пусть узел B пытается передать данные узлу A, посылая ему кадр RTS. Поскольку этот кадр получает также и узел C, то он блокируется

на время передачи между узлами A и B. Узел D, пытаясь передать данные узлу C, посылает кадр RTS, но поскольку узел C заблокирован, то он не получает ответа и начинает процедуру обратного отсчета с увеличенным размером окна. В то же время кадр RTS, посланный узлом D, получает и узел E, который, ложно предполагая, что за этим последует сеанс передачи данных от узла D к узлу C, блокируется. Однако это ложная блокировка, поскольку реально между узлами D и C передачи нет. Более того, если узел F попытается передать данные ложно заблокированному узлу E и пошлет свой кадр RTS, то он ложно заблокирует узел G.

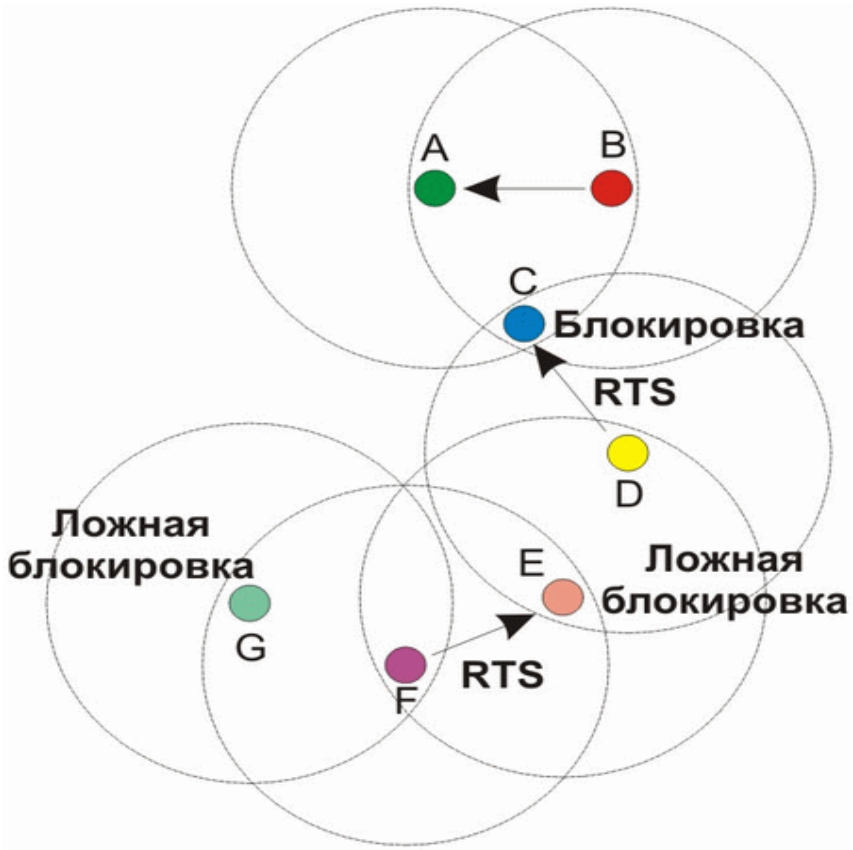



Рис. 7. Возникновение ложных блокировок узлов сети

Описанное явление ложной блокировки узлов может приводить к кратковременному ступору всей сети.

**Фрагментация фрейма по стандарту 802.11**

Фрагментация фрейма – это выполняемая на уровне MAC функция, назначение которой – повысить надежность передачи фреймов через беспроводную среду. Под фрагментацией понимается дробление фрейма на меньшие фрагменты и передача каждого из них отдельно. Предполагается, что вероятность успешной передачи меньшего фрагмента через зашумленную беспроводную среду выше. Получение каждого фрагмента фрейма подтверждается отдельно;

следовательно, если какой-нибудь фрагмент фрейма будет передан с ошибкой или вступит в коллизию, только его придется передавать повторно, а не весь фрейм. Это увеличивает пропускную способность среды.

Размер фрагмента может задавать администратор сети. Фрагментации подвергаются только одноадресные фреймы. Широковещательные, или многоадресные, фреймы передаются целиком. Кроме того, фрагменты фрейма передаются пакетом, с использованием только одной итерации механизма доступа к среде DSF.

Хотя за счет фрагментации можно повысить надежность передачи фреймов в беспроводных локальных сетях. Она приводит к увеличению «накладных расходов» MAC-протокола стандарта 802.11. Каждый фрагмент фрейма включает информацию, содержащуюся в заголовке 802.11 MAC, а также требует передачи соответствующего фрейма подтверждения. Это увеличивает число служебных сигналов MAC-протокола и снижает реальную производительность беспроводной станции. Фрагментация – это баланс между надежностью и непроизводительной загрузкой среды.

Функция централизованной координации PCF

Рассмотренный выше механизм распределенной координации DCF является базовым для протоколов 802.11 и может использоваться как в беспроводных сетях, функционирующих в режиме Ad-Hoc, так и в сетях, функционирующих в режиме Infrastructure, то есть в сетях, инфраструктура которых включает точку доступа.

Однако для сетей в режиме Infrastructure более естественным является несколько иной механизм регламентирования коллективного доступа, известный как функция централизованной координации (Point Coordination Function, PCF). Отметим, что механизм PCF является опциональным и применяется только в сетях с точкой доступа.

В случае задействования механизма PCF один из узлов сети (точка доступа) является центральным и называется центром координации (Point Coordinator, PC). На центр координации возлагается задача управления коллективным доступом всех остальных узлов сети к среде передачи данных на основе определенного алгоритма опроса или исходя из приоритетов узлов сети. То есть центр координации опрашивает все узлы сети, внесенные в его список, и на основании этого опроса организует передачу данных между всеми узлами сети. Важно, что такой подход полностью исключает конкурирующий доступ к среде, как в случае механизма DCF, и делает невозможным возникновение коллизий, а для времезависимых приложений гарантирует приоритетный доступ к среде. Таким образом, PCF может использоваться для организации приоритетного доступа к среде передачи данных.

Функция централизованной координации не отрицает функцию распределенной координации, а скорее, дополняет ее, накладываясь поверх. Фактически в сетях с механизмом

PCF реализуется как механизм PCF, так и традиционный механизм DCF. В течение определенного промежутка времени реализуется механизм PCF, затем – DCF, а потом все повторяется заново.

Для того чтобы иметь возможность чередовать режимы PCF и DCF, необходимо, чтобы точка доступа, выполняющая функции центра координации и реализующая режим PCF, имела бы приоритетный доступ к среде передачи данных. Это можно сделать, если использовать конкурентный доступ к среде передачи данных (как и в методе DCF), но для центра координации разрешить использовать промежуток ожидания, меньший DIFS. В этом случае если центр координации пытается получить доступ к среде, то он ожидает (как и все остальные узлы сети) окончания текущей передачи и, поскольку для него определяется минимальный режим ожидания после обнаружения «тишины» в эфире, первым получает доступ к среде. Промежуток ожидания, определяемый для центра координации, называется PIFS (PCF Interframe Space), причем SIFS<PIFS<DIFS.

Режимы DCF и PCF объединяются в так называемом суперфрейме, который образуется из промежутка бесконкурентного доступа к среде, называемого CFP (Contention-Free Period), и следующего за ним промежутка конкурентного доступа к среде CP (Contention Period) (рис. 8).

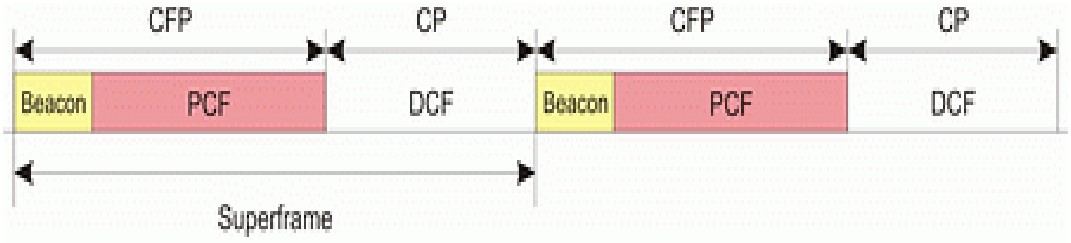



Рис. 8. Объединение режимов PCF и DCF в одном суперфрейме

Суперфрейм начинается с кадра-маячка (beacon), получив который все узлы сети приостанавливают попытки передавать данные на время, определяемое периодом CFP. Кадры маячки несут служебную информацию о продолжительности CFP-промежутка и позволяют синхронизировать работу всех узлов сети. Во время режима PCF точка доступа опрашивает все узлы сети о кадрах, которые стоят в очереди на передачу, посылая им служебные кадры CF_POLL. Опрашиваемые узлы в ответ на получение кадров CF_POLL посылают подтверждение CF_ACK. Если подтверждения не получено, то точка доступа переходит к опросу следующего узла.

Кроме того, чтобы иметь возможность организовать передачу данных между всеми узлами сети, точка доступа может передавать кадр данных (DATA) и совмещать кадр опроса с передачей данных (кадр DATA+CF_POLL). Аналогично узлы сети могут совмещать кадры подтверждения с передачей данных DATA+CF_ACK (рис. 4.7).

Допускаются следующие типы кадров во время режима PCF:

- DATA – кадр данных
- CF_ACK – кадр подтверждения
- CF_POLL – кадр опроса
- DATA+CF_ACK – комбинированный кадр данных и подтверждения
- DATA+CF_POLL – комбинированный кадр данных и опроса
- DATA+CF_ACK+CF_POLL — комбинированный кадр данных, подтверждения и опроса
- CF_ACK+CF_POLL – комбинированный кадр подтверждения и опроса

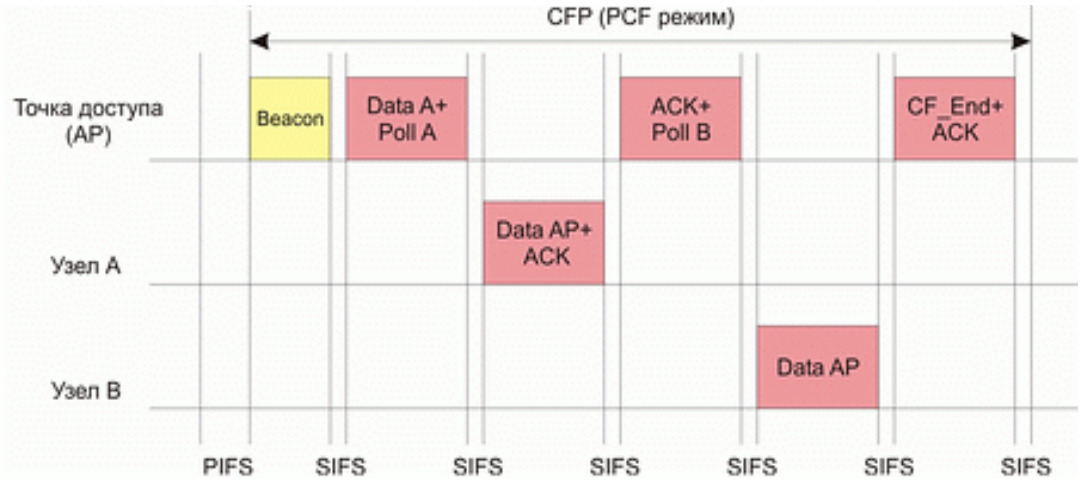



Рис. 9. Организация передачи данных между узлами сети в режиме PCF

**Физические уровни стандартов**

Основное назначение физических уровней стандарта 802.11 – обеспечение механизма беспроводной передачи для подуровня MAC, а также поддержание вторичных функций (оценка состояние беспроводной среды и сообщение об этом MAC). MAC и PHY не зависимы это дает возможность использовать более скоростные физические уровни, описанные в стандартах 802.11a/b/g.

Каждый физический уровень стандарта имеет два подуровня:

- - PLCP (Physical Layer Convergence Procedure) – процедура определения состояния физического уровня;
- - PMD (Physical Medium Dependent) – подуровень физического уровня, зависящий от среды передачи.

На рис. 10 показана как эти уровни соотносятся между собой и вышестоящими уровнями.

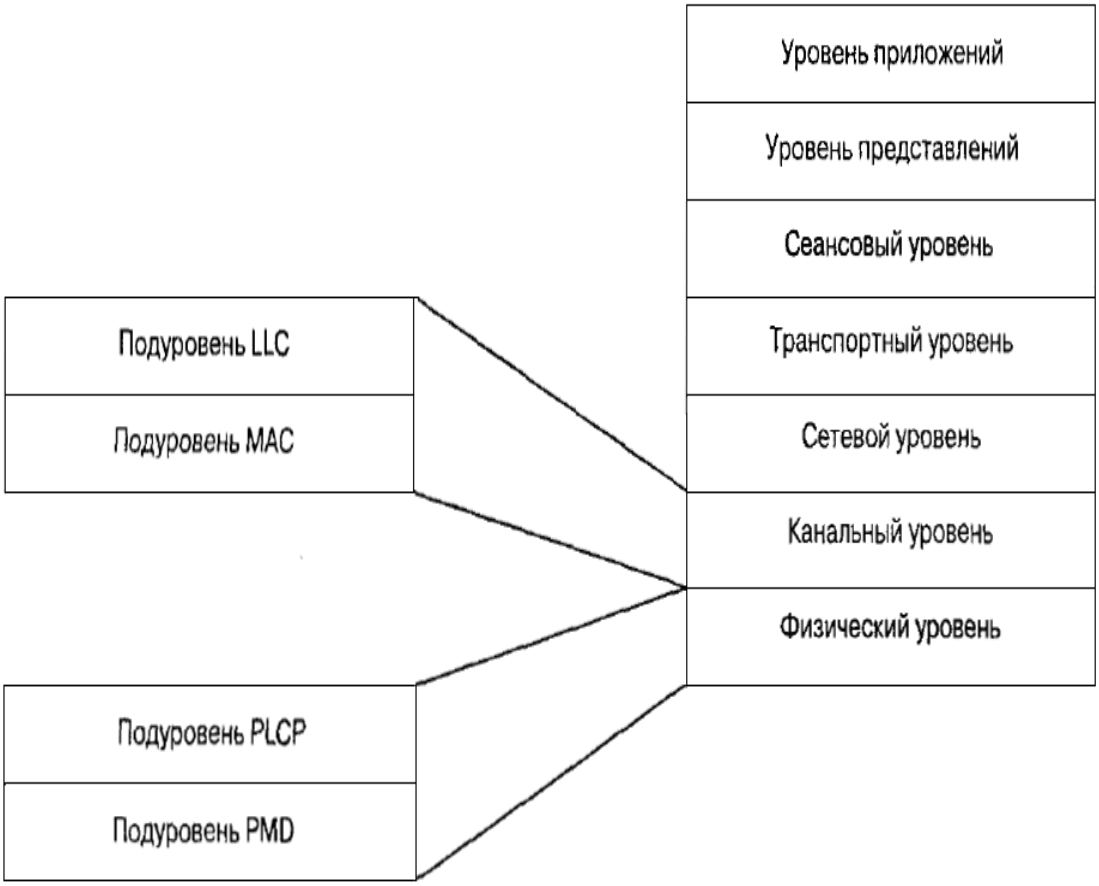



Рис. 10. Подуровни уровня PHY модели взаимодействия открытых систем (OSI)

Подуровень PLCP является уровнем обеспечения взаимодействия, на котором осуществляется перемещение элементов данных протокола MAC (MAC protocol data units, MPDU) между MAC – станциями с использованием подуровня PMD, на котором реализуется тот или иной метод передачи и приема данных через беспроводную сеть. Подуровни PLCP и PMD отличаются в разных вариантах стандарта 802.11.

**Физический уровень беспроводных сетей стандарта 802.11**

Исходный стандарт 802.11 определяет два метода передачи на физическом уровне.

- Технология расширения спектра путем скачкообразной перестройки частоты (FHSS)
- Технология широкополосной модуляции с расширением спектра методом прямой последовательности (DSSS)

Обе технологии работают в диапазоне 2,4 ГГц, в котором выделена полоса шириной 82 МГц для промышленного, научного и медицинского применения (ISM).

**Беспроводные локальные сети со скачкообразной перестройкой частоты (FHSS)**

Беспроводные локальные сети FHSS (Frequency Hopping Spread Spectrum) поддерживают скорости передачи 1 и 2 Мбит/с. Как следует из названия, устройства FHSS осуществляют скачкообразную перестройку частоты по предопределенной схеме, как показано на рис. 11.

Устройства FHSS делят предназначенную для их работы полосу частот от 2,402 до 2,480 ГГц на 79 неперекрывающихся каналов (это справедливо для Северной Америки и большей части Европы). Ширина каждого из 79 каналов составляет 1 МГц.

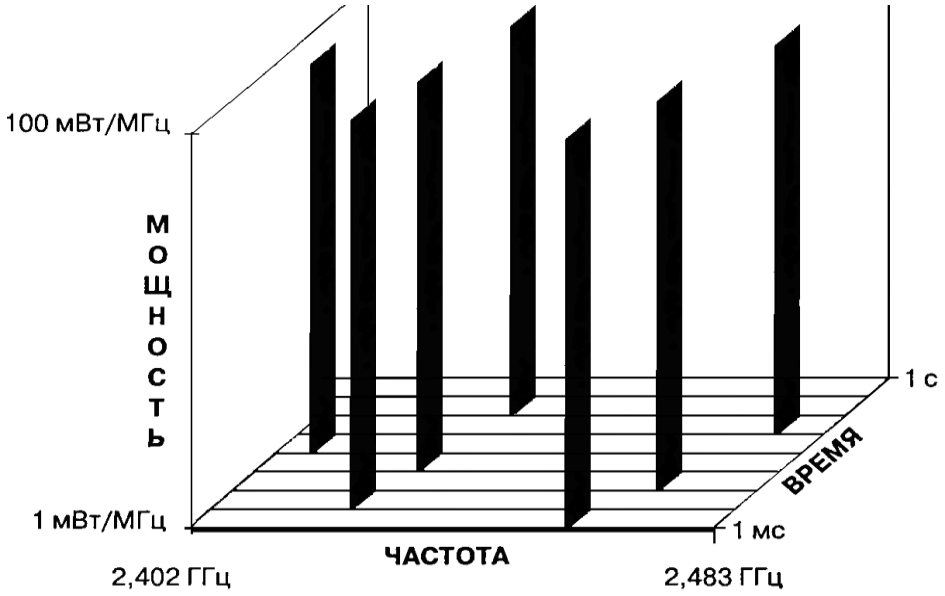



Рис. 11. Пример скачкообразной перестройки частоты

Последовательность перестройки частоты имеет следующие параметры: частота перескоков не менее 2,5 раз в секунду, как минимум между 6-ю каналами. Чтобы избежать коллизий между перекрывающимися зонами покрытия, возможные последовательности перескоков разбиты на три набора последовательностей, длина которых для северной Америки и большей части Европы равна 26. В таблице 4.1 представлены схемы скачкообразной перестройки частоты, обеспечивающие минимальные перекрытия.

Таблица 1. Схемы скачкообразной перестройки частоты

| Набор частот | Схема скачкообразной перестройки частоты |
|---|---|
| 1 | 0,3,6,9,12,15,18,21,24,27,30,33, 6,39,42,45,48,51,54,57,60,63,66,69,72,75 |
| 2 | 1,4,7,10,13,16,19,22,25,28,31,34,37,40,43,46,49,52,55,58,61,64,67,70,737 6 |
| 3 | 2,5,8,11,14,17,20,23,26,29,32,35,38,41,44,47,50,53,56,59,62,65,68,71,72, 77 |

После того как уровень MAC пропускает MAC – фрейм, который в локальных беспроводных сетях имеет название PSDU (сокращение от PLCP service data unit), подуровень PLCP добавляет

два поля в начало фрейма, чтобы сформировать таким образом фрейм PPDU (элемент данных протокола PLCP). Но рис. 12 представлен формат фрейма FHSS подуровня PLCP.

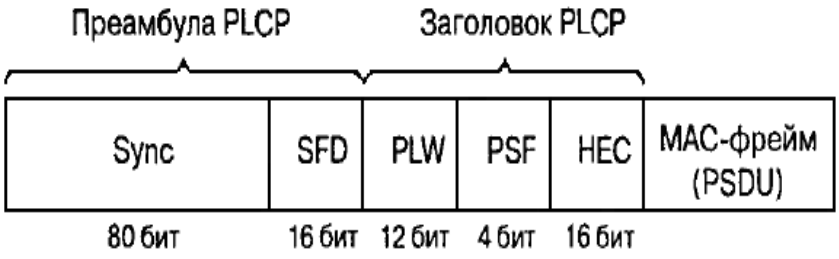



Рис. 12. Формат фрейма FHSS подуровня PLCP

Преамбула PLCP состоит из двух подполей. Подполе Sync размером 80 бит. Строка, состоящая из чередующихся 0 и 1, начинается с нуля. Приемная станция использует это поле, чтобы принять решение о выборе антенны при наличии такой возможности, откорректировать уход частоты (frequency offset) и синхронизировать распределение пакетов (packet timing). Подполе флага начала фрейма (start of frame delimiter, SFD) размером 16 бит. Состоит из специфической строки (0000 1100 1011 1101, крайний слева бит первый), применяется для синхронизации фреймов в приемной станции.

Заголовок фрейма PLCP состоит из трех подполей. PSDU Length Word (PLW) - слово длины служебного элемента данных PLCP (PSDU), указывает размер фрейма MAC в октетах. Сигнальное поле PLCP (signaling field PLCP, PSF) размером 4 бита. Указывает скорость передачи данных конкретного фрейма.

Подуровень PLCP преобразует фрейм в поток битов и передает его на подуровень PMD. Подуровень PMD технологии FHSS модулирует поток данных с использованием модуляции, основанной на гауссовом переключении частот (Gaussian frequency shift keying, GFSK). Для скорости 1 Мбит/с модулятор использует для передачи 0 и 1, два различных по частоте сигнала рис 4.13.

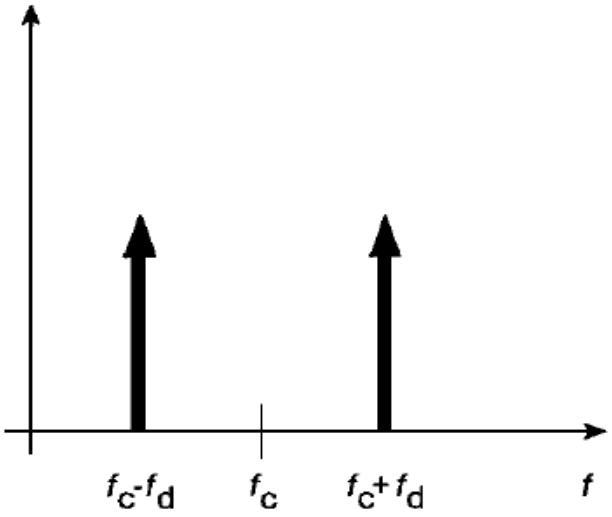



Рис. 13. Модуляция GFSK

Чтобы осуществлять передачу со скоростью 2 Мбит/с используется модуляция 4GFSK, в этом случае 2 бита модулируют сигнал одновременно. Для реализации этого метода требуется четыре различные частоты, в таблице 4.2 представлена карта преобразования символов в частоту.

Таблица 2. Карта преобразования символов в частоту при модуляции 4GFSK

| Символ | Частота |
|---|---|
| 01 | $f_c + f_{d1}$ |
| 11 | $f_c + f_{d2}$ |
| 01 | $f_c - f_{d1}$ |
| 00 | $f_c - f_{d2}$ |

Основные недостатки рассматриваемого метода:

- - не высокая скорость передачи (максимум 2 Мбит/с);
- - нет стандартизированных механизмов которые бы позволял исключать те частотные каналы, на которых помехи особенно ощутимы;
- - Нет механизма синхронизации или координации последовательностей переключения частоты для соседствующих точек доступа.
- В следствии чего последовательности переключений соседних точек доступа могут перекрываются.

**Беспроводные локальные сети, использующие широкополосную модуляцию DSSS с расширением спектра методом прямой последовательности**

Как было указано в стандарте 802.11 разработки 1997 года, технология DSSS поддерживает скорости передачи 1 и 2 Мбит/с. Беспроводные локальные сети DSSS используют каналы шириной 22 МГц. Каналы шириной 22 МГц позволяют создать в диапазоне 2,4—2,483 ГГц три не перекрывающихся канала передачи.

Аналогично подуровню PLCP, используемому в технологии FHSS, подуровень PLCP технологии DSSS стандарта 802.11 добавляет два поля во фрейм MAC, чтобы сформировать PPDU: преамбулу PLCP и заголовок PLCP. Формат фрейма представлен на рис. 14.

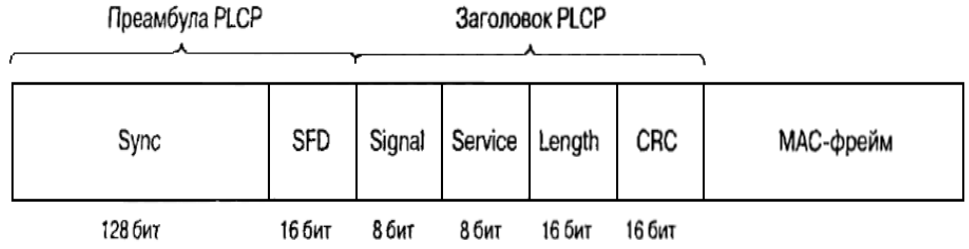



Рис. 14. Формат фрейма DSSS PPDU стандарта 802.11

Преамбула PLCP состоит из двух подполей. Подполе Sync шириной 128 бит, представляющее собой строку, состоящую из единиц. Задача этого поля – обеспечить синхронизацию для приемной станции. Подполе SFD шириной 16 бит, содержит специфическую строку 0xF3A0; обеспечивает тайминг для приемной станции

Заголовок PLCP состоит из четырех подполей. Подполе Signal шириной 8 бит, указывает тип модуляции и скорость передачи данного фрейма. Подполе Service шириной 8 бит, зарезервировано. Подполе Length шириной 16 бит, указывает количество микросекунд (из диапазона 16 – $2^{16}$-1), необходимое для передачи части MAC фрейма

Подуровень PLCP преобразует фрейм в поток битов и передает данные на подуровень PMD. Весь PPDU проходит через процесс скремблирования с целью рандомизации данных.

Скремблированная преамбула PLCP всегда передается со скоростью 1 Мбит/с, в то время как скремблированный фрейм MPDU передается со скоростью, указанной в подполе Signal. Подуровень PMD модулирует отделенный поток битов, используя следующие методы модуляции.

- Двоичная относительная фазовая манипуляция (differential binary phase shift keying, DBPSK) для скорости передачи 1 Мбит/с
- Квадратурная фазовая манипуляция (quadrature phase shift key, QPSK) для скорости передачи 2 Мбит/с

**Технологии расширения спектра**

При методе **DSSS** каждый информационный символ представляется 11-разрядным кодом

Баркера вида 11100010010. Коды Баркера обладают наилучшими среди известных псевдослучайных последовательностей свойствами шумоподобности, что и обусловило их применение в аппаратуре беспроводных сетей. Для передачи единичного и нулевого символов сообщения используются инверсная и прямая последовательности соответственно.

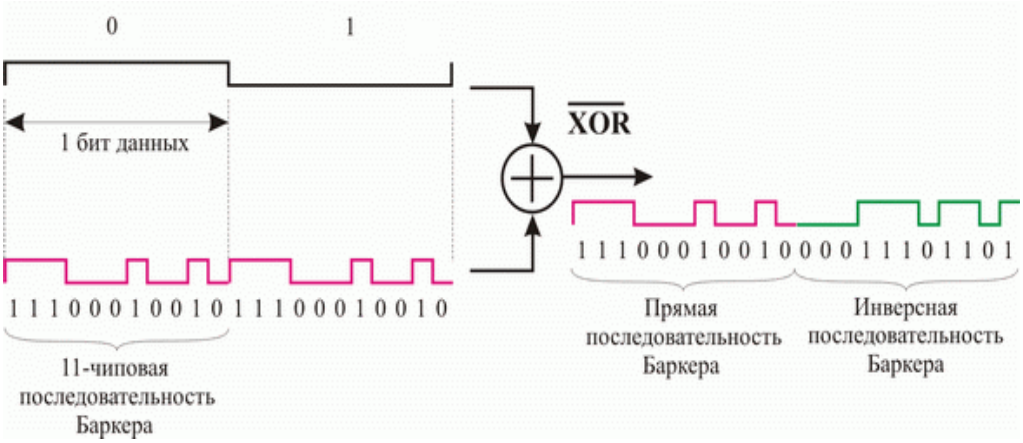



Рис. 15 Расширение спектра по технологии DSSS

Для модуляции несущего колебания в этом случае используются уже не исходные символы сообщения, а прямые или инверсные последовательности Баркера. При использовании **DSSS** происходит "размазывание" мощности сигнала в полосе частот, в 11 раз превышающей полосу исходного узкополосного сигнала. Здесь следует упомянуть о довольно часто встречающемся в литературе тезисе о том, что при переходе к технологии **DSSS** возможна работа на пониженных мощностях передатчика. Это верно только в том смысле, что снижается спектральная плотность мощности излучаемого сигнала при неизменной излучаемой передатчиком мощности.

В приемнике полученный сигнал снова складывается по модулю два с кодом Баркера, в результате он становится узкополосным, поэтому его фильтруют в узкой полосе частот, равной удвоенной скорости передачи. Любая помеха, попадающая в полосу исходного широкополосного сигнала, после умножения на код Баркера, наоборот, становится широкополосной, поэтому в узкую информационную полосу попадает лишь часть помехи, примерно в 11 раз меньшая по мощности помехи, действующей на входе приемника. Главной проблемой, возникающей при решении этой задачи, является обеспечение синхронизации приемника по передаваемому сигналу. На уровне физического канала необходимо обеспечить синхронизацию по фазе несущего колебания, тактовой частоте кода Баркера и тактовой частоте сообщения. Для решения этой задачи передатчик не реже, чем один раз за 100 мс передает специальный синхросигнал.

Применение технологии DSSS позволяет также эффективно бороться с интерференционной помехой, возникающей в результате отражения сигнала от стен и местных предметов, что особенно актуально для закрытых помещений.

**Двоичная относительная фазовая манипуляция (DBPSK)**

Данный вид модуляции используется для передачи информации со скорость 1 Мбит/с. Для модуляции синусоидального несущего сигнала используется относительная двоичная фазовая модуляция (Differential Binary Phase Shift Key, DBPSK). При этом кодирование информации происходит за счет сдвига фазы синусоидального сигнала по отношению к предыдущему состоянию сигнала. Двоичная фазовая модуляция предусматривает два возможных значения сдвига фазы — 0 и π. Тогда логический нуль может передаваться синфазным сигналом (сдвиг по фазе равен 0), а единица — сигналом, который сдвинут по фазе на π.

**Квадратурная фазовая манипуляция (QPSK)**

Для передачи данных на скорости 2 Мбит/с используется относительная квадратурная фазовая модуляция (Differential Quadrature Phase Shiftey). При относительной квадратурной фазовой модуляции сдвиг фаз может принимать четыре различных значения: 0, π/2, π и 3π/2. Используя четыре различных состояния сигнала, можно в одном дискретном состоянии закодировать последовательность двух информационных бит (дибит) и тем самым в два раза повысить информационную скорость передачи. Дибиту 00 соответствует сдвиг фазы, равный 0; дибиту 01 — сдвиг фазы, равный π/2; дибиту 11 — сдвиг фазы, равный π; дибиту 10 — сдвиг фазы, равный 3π/2.

В заключение рассмотрения физического уровня протокола 802.11 отметим, что при информационной скорости 2 Мбит/с скорость следования отдельных чипов последовательности Баркера остается прежней, то есть $11\times10^6$ чип/с, а следовательно, не меняется и ширина спектра передаваемого сигнала.

Главным недостатком технологий DSSS и FHSS является низкая скорость передачи. На сегодняшний день технологии являются устаревшими и не используются.

**Физический уровень сетей стандарта 802.11b**

Появившийся в 1999 году стандарт 802.11b регламентировал правила использования высокоскоростной технологии HR – DSSS, обеспечивающей скорость передачи 5,5 Мбит/с и 11 Мбит/с. Для достижения таких скоростей применялось кодирование с использованием комплементарных кодов (complementary code keying, CCK) или технологии двоичного пакетного сверточного кодирования (packet binary convolution coding, PBCC). В технологии HR-DSSS использовалась та же схема организации каналов что и DSSS – полоса канала 22 МГц, 11 каналов, 3 не перекрывающихся, ISM диапазон 2,4 ГГц.

**Подуровень PLCP технологии HR-DSSS стандарта 802.11b**

Подуровень PLCP технологии HR-DSSS использует фреймы PPDU двух типов: длинный и короткий. Преамбула и заголовок длинного фрейма всегда передаются со скоростью 1 Мбит/с, для обеспечения обратной совместимости с технологией DSSS. Длинный фрейм HR-DSSS почти такой же как в DSSS но с небольшими отличиями, направленными на повышения скорости передачи:

- В подполе Signal могут быть указаны дополнительные скорости передачи данных (0x37 – 5,5 Мбит/с; 0x6E – 11 Мбит/с)
- Подполе Service определяет ранее зарезервированные биты (Таблица 43)
- Подполе Length по прежнему указывает время в микросекундах, необходимое для передачи PSDU
-

Таблица 3. Определение битов подполя Service

| Бит | Наименование | Значение |
|---|---|---|
| B2 | Генераторы синхронизированы (locked clocks) | 0 = не сенхранизированы, 1 = задающие генераторы частоты и символов синхронизированы |
| B3 | Выбор модуляции (modulation selection) | 0 = CCK; 1 = PBCC |
| B7 | Увеличение длины | Используется подполем длины |

Короткий фрейм PLCP PPDU обеспечивает средство для минимизации числа служебных сигналов, все еще позволяющих, передатчику и приемнику связаться с друг другом надлежащим образом. Короткий фрейм показан на рисунке 5.7. Он использует те же заголовок, преамбулу и формат PSDU, но заголовок PLCP передается на скорости 2 Мбит/с, в то время как PSDU передается со скоростью 2; 5,5; 11 Мбит/с. Кроме того его подполя модифицированы следующим образом. Ширина поля Sync сокращена со 128 до 56 битов, оно представляет собой строку состоящую из одних нулей. Поле SFD шириной 16 бит указывает на начало фрейма и на используемый заголовок (короткий или длинный)

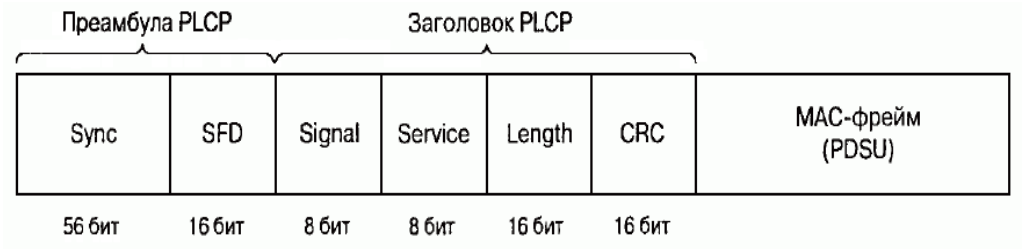



Рис. 16 Короткий PPDU технологии HR-DSSS

**Модуляция ССК на подуровне PMD стандарта 802.11b**

В стандарте IEEE 802.11b используются комплексные комплементарные 8-чиповые последовательности, определенные на множестве комплексных элементов {1, –1, j, –j}. Элементы 8-чиповой ССК-последовательности могут принимать одно из следующих восьми значений: 1, –1, j, –j, 1+j, 1–j, –1+j, –1–j. Основное отличие ССК-последовательностей от рассмотренных ранее кодов Баркера заключается в том, что существует не строго заданная последовательность, посредством которой можно было кодировать либо логический нуль, либо единицу, а целый набор последовательностей. Использование ССК-кодов позволяет кодировать 8 бит на один символ при скорости 11 Мбит/с и 4 бит на символ при скорости 5,5 Мбит/с.

Для того, чтобы передавать данные со скоростью 5,5 Мбит/с, нужно сгруппировать скремблированный поток битов в символы по 4 бита (b0, b1, b2 и b3). Последние два бита (b2 и b3) используются для определения 4 последовательностей комплексных чипов, как показано в табл. 4.1, где {cl, c2, c3, c4, c5, c6, c7, c8} представляют чипы последовательности.

Таблица 4. Последовательность чипов ССК

| b2,b | C | C | C | C | C | C | C | C |
|---|---|---|---|---|---|---|---|---|
| 00 | J | 1 | j | - | J | 1 | - | 1 |
| 01 | - | - | - | 1 | **J** | 1 | - | 1 |
| 10 | - | 1 | - | - | - | 1 | j | 1 |
| 11 | j | - | j | 1 | - | 1 | j | 1 |

Теперь, имея последовательность чипов, определенную битами (b2, b3), можно использовать первые два бита (b0, b1) для определения поворота фазы, осуществляемого при модуляции по методу DQPSK, который будет применен к последовательности.

Таблица 5. Поворот фазы при ССК модуляции

| 0 0 | 0 градусов |
|---|---|
| 0 1 | 90 градусов |

| | |
|---|---|
| 1 1 | 180 градусов |
| 1 0 | 90 градусов |

Определенное битами вращение фазы применяется по отношению к 8 комплексным чипам символа, затем осуществляется модуляция на подходящей несущей частоте.

Следует иметь ввиду, что речь идет об использовании DQPSK, а не QPSK, и поэтому представленные в таблице изменения фазы отсчитываются по отношению к предыдущему символу или, в случае первого символа PSDU, по отношению к последнему символу предыдущего DQPSK символа.

Для того чтобы передавать данные на скорости 11 Мбит/с, скремблированная последовательность битов разбивается на группы по 8 бит. Последние 6 битов выбирают одну последовательность, состоящую из 8 комплексных чипов из числа 64 возможных последовательностей, первые биты так же как и для скорости 5,5 Мбит/с определяют изменение фазы символов.

Двоичное пакетное сверточное кодирование PBCC

Идея сверточного кодирования заключается в следующем. Входящая последовательность информационных бит преобразуется в специальном сверточном кодере таким образом, чтобы каждому входному биту соответствовало более одного выходного. То есть сверточный кодер добавляет определенную избыточную информацию к исходной последовательности. Если, к примеру, каждому входному биту соответствует два выходных, то говорят о сверточном кодировании со скоростью r = 1/2.

Любой сверточный кодер строится на основе нескольких последовательно связанных запоминающих ячеек и логических элементов, связывающих эти ячейки между собой. Количество запоминающих ячеек определяет количество возможных состояний кодера. Если, к примеру, в сверточном кодере используется шесть запоминающих ячеек, то в кодере хранится информация о шести предыдущих состояниях сигнала, а с учетом значения входящего бита получим, что в таком кодере используется семь бит входной последовательности. Такой сверточный кодер называется кодером на семь состояний (K = 7).

Выходные биты, формируемые в сверточном кодере, определяются значениями входного бита и битами, хранимыми в запоминающих ячейках, то есть значение каждого формируемого выходного бита зависит не только от входящего информационного бита, но и от нескольких предыдущих битов.

В технологии PBCC используются сверточные кодеры на семь состояний (K = 7) со скоростью r=1/2. Главным достоинством сверточных кодеров является помехоустойчивость формируемой ими последовательности. Дело в том, что при избыточности кодирования даже в случае возникновения ошибок приема исходная последовательность бит может быть безошибочно восстановлена. Для восстановления исходной последовательности битов на стороне приемника применяется декодер Витерби.

Дибит, формируемый в сверточном кодере, используется в дальнейшем в качестве передаваемого символа, но предварительно этот дибит подвергается фазовой модуляции. Причем в зависимости от скорости передачи возможна двоичная, квадратурная или даже восьмипозиционная фазовая модуляция.

Метод пакетного сверточного кодирования опционально предусмотрен как альтернативный метод кодирования в протоколе 802.11b на скоростях передачи 5,5 и 11 Мбит/с. Кроме того, именно данный режим кодирования лег в основу протокола 802.11b+ — расширения протокола 802.11b. Собственно, протокола 802.11b+ как такового официально не существует, однако данное расширение поддержано многими производителями беспроводных устройств. В протоколе 802.11b+ предусматривается еще одна скорость передачи данных — 22 Мбит/с с использованием технологии PBCC.

При скорости передачи 5,5 Мбит/с для модуляции дибита, формируемого сверточным кодером, используется двоичная фазовая модуляция, а при скорости 11 Мбит/с — квадратурная фазовая модуляция. При этом для скорости 11 Мбит/с в каждом символе кодируется по одному входному биту и скорость передачи бит соответствует скорости передачи символов, а при скорости 5,5 Мбит/с скорость передачи битов равна половине скорости передачи символов (поскольку каждому входному биту в данном случае соответствует два выходных символа). Поэтому и для скорости 5,5 Мбит/с, и для скорости 11 Мбит/с символьная скорость составляет $11\times10^6$ символов в секунду.

Для скорости 22 Мбит/с по сравнению с уже рассмотренной нами схемой PBCC передача данных имеет две особенности. Прежде всего, используется 8-позиционная фазовая модуляция (8-PSK), то есть фаза сигнала может принимать восемь различных значений, что позволяет в одном символе кодировать уже 3 бита. Кроме того, в схему кроме сверточного кодера добавлен пунктурный кодер (Puncture). Смысл такого решения довольно прост: избыточность сверточного кодера, равная 2 (на каждый входной бит приходится два выходных), достаточно высока и при определенных условиях помеховой обстановки является излишней, поэтому можно уменьшить избыточность, чтобы, к примеру, каждым двум входным битам соответствовало три выходных.

Для этого можно, конечно, разработать соответствующий сверточный кодер, но лучше добавить в схему специальный пунктурный кодер, который будет просто уничтожать лишние биты.

Допустим, что пунктурный кодер удаляет один бит из каждых четырех входных битов. Тогда каждым четырем входящим битам будет соответствовать три выходящих. Скорость такого кодера составляет 4/3.

Если же такой кодер используется в паре со сверточным кодером со скоростью 1/2, то общая скорость кодирования составит уже 2/3, то есть каждым двум входным битам будет соответствовать три выходных.

Таблица 6. Соотношение между скоростями передачи и типом кодирования в стандарте 802.11b

| Скорость передачи, Мбит/с | | Метод кодирования | Модуляция | Скорость сверточного кодирования | Символьная скорость, 106 символ/с | Количество бит в одном символе |
|---|---|---|---|---|---|---|
| | (обязательно) | Код Баркера | DBPSK | - | 1 | 1 |
| | (обязательно) | Код Баркера | DQPSK | - | 1 | 2 |
| ,5 | (обязательно) | CCK | DQPSK | - | 1,375 | 2 |
| | (опционально) | PBCC | DBPSK | 1/2 | 11 | 0,5 |
| 1 | (обязательно) | CCK | DQPSK | - | 1,375 | 8 |
| | (опционально) | PBCC | DQPSK | 1/2 | 11 | 1 |

**Физический уровень стандарта 802.11g**

Стандарт IEEE 802.11g является логическим продолжением стандарта 802.11b и предполагает передачу данных в том же частотном диапазоне, но с более высокими скоростями. Кроме того, стандарт 802.11g полностью совместим с 802.11b, то есть любое устройство 802.11g должно поддерживать работу с устройствами 802.11b. Максимальная скорость передачи в стандарте 802.11g составляет 54 Мбит/с.

При разработке стандарта 802.11g рассматривались несколько конкурирующих технологий: метод ортогонального частотного разделения OFDM, предложенный к рассмотрению компанией Intersil, и метод двоичного пакетного сверточного кодирования PBCC, опционально

реализованный в стандарте 802.11b и предложенный компанией Texas Instruments. В результате стандарт 802.11g основан на компромиссном решении: в качестве базовых применяются технологии OFDM и CCK, а опционально предусмотрено использование технологии PBCC.

Ортогональное частотное разделение каналов с мультиплексированием

Распространение сигналов в открытой среде, коей является радиоэфир, сопровождается возникновением различного рода помех. Классический пример такого рода помех — эффект многолучевой интерференции сигналов, заключающийся в том, что в результате многократных отражений сигала от естественных преград один и тот же сигнал может попадать в приемник различными путями. Но подобные пути распространения имеют и разные длины, а потому для различных путей распространения ослабление сигнала будет неодинаковым. Следовательно, в точке приема результирующий сигнал представляет собой суперпозицию (интерференцию) многих сигналов, имеющих различные амплитуды и смещенных друг относительно друга по времени, что эквивалентно сложению сигналов с разными фазами.

Следствием многолучевой интерференции является искажение принимаемого сигнала. Многолучевая интерференция присуща любому типу сигналов, в результате интерференции определенные частоты складываются синфазно, что приводит к увеличению сигнала, а некоторые, наоборот, — противофазно, вызывая ослабление сигнала на данной частоте.

Говоря о многолучевой интерференции, возникающей при передаче сигналов, различают два крайних случая. В первом случае максимальная задержка между различными сигналами не превосходит времени длительности одного символа и интерференция возникает в пределах одного передаваемого символа. Во втором случае максимальная задержка между различными сигналами больше длительности одного символа, а в результате интерференции складываются сигналы, представляющие разные символы, и возникает так называемая межсимвольная интерференция (Inter Symbol Interference, ISI).

Наиболее отрицательно на искажение сигнала влияет межсимвольная интерференция. Поскольку символ — это дискретное состояние сигнала, характеризующееся значениями частоты несущей, амплитуды и фазы, то для различных символов меняются амплитуда и фаза сигнала, поэтому восстановить исходный сигнал крайне сложно.

Чтобы частично компенсировать эффект многолучевого распространения, используются частотные эквалайзеры, однако по мере роста скорости передачи данных либо за счет увеличения символьной скорости, либо из-за усложнения схемы кодирования, эффективность использования эквалайзеров падает.

Поэтому при более высоких скоростях передачи применяется принципиально иной метод кодирования данных – ортогональное частотное разделение каналов с мультиплексированием (Orthogonal Frequency Division Multiplexing, OFDM). Идея данного метода заключается в том, что

поток передаваемых данных распределяется по множеству частотных подканалов и передача ведется параллельно на всех этих подканалах. При этом высокая скорость передачи достигается именно за счет одновременной передачи данных по всем каналам, а скорость передачи в отдельном подканале может быть и невысокой. Поскольку в каждом из частотных подканалов скорость передачи данных можно сделать не слишком высокой, это создает предпосылки для эффективного подавления межсимвольной интерференции.

При частотном разделении каналов необходимо, чтобы ширина отдельного канала была, с одной стороны, достаточно узкой для минимизации искажения сигнала в пределах отдельного канала, а с другой — достаточно широкой для обеспечения требуемой скорости передачи. Кроме того, для экономного использования всей полосы канала, разделяемого на подканалы, желательно как можно более плотно расположить частотные подканалы, но при этом избежать межканальной интерференции, чтобы обеспечить полную независимость каналов друг от друга. Частотные каналы, удовлетворяющие перечисленным требованиям, называются ортогональными. Несущие сигналы всех частотных подканалов (а точнее, функции, описывающие эти сигналы) ортогональны друг другу.

Важно, что хотя сами частотные подканалы могут частично перекрывать друг друга, ортогональность несущих сигналов гарантирует частотную независимость каналов друг от друга, а, следовательно, и отсутствие межканальной интерференции (рис. 17).

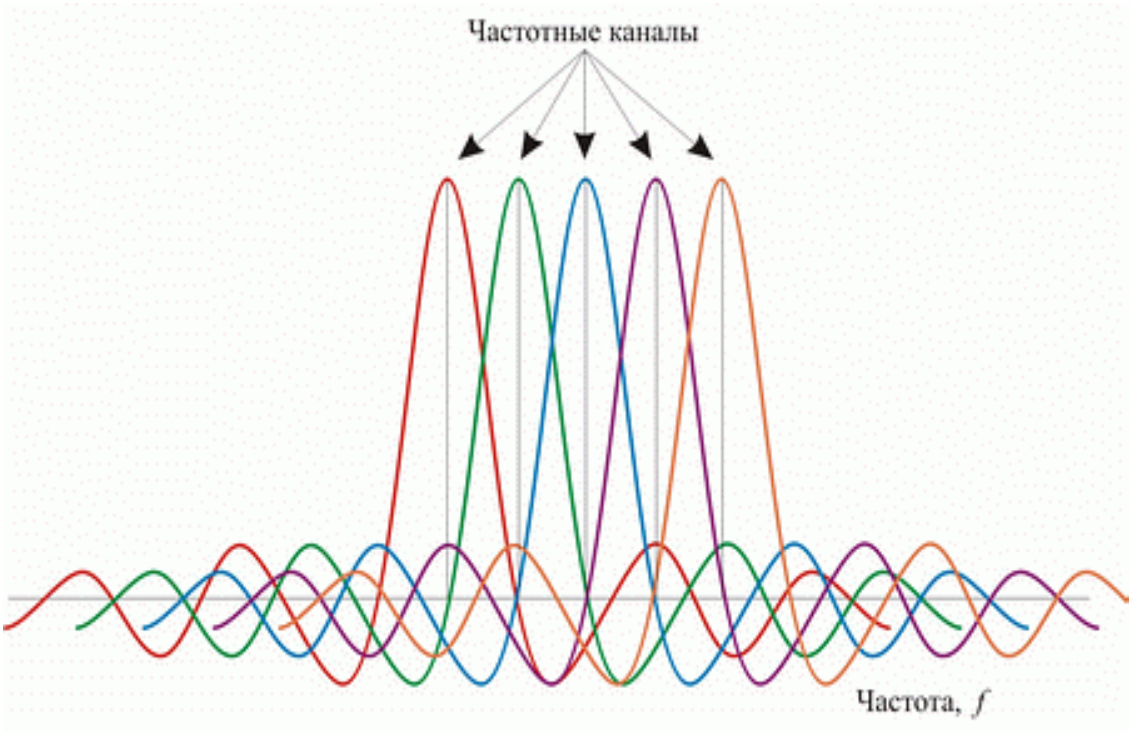



Рис. 17. Пример перекрывающихся частотных каналов с ортогональными несущими

Рассмотренный способ деления широкополосного канала на ортогональные частотные подканалы называется ортогональным частотным разделением с мультиплексированием (OFDM). Одним из ключевых преимуществ метода OFDM является сочетание высокой скорости передачи

с эффективным противостоянием многолучевому распространению. Если говорить точнее, то сама по себе технология OFDM не устраняет многолучевого распространения, но создает предпосылки для устранения эффекта межсимвольной интерференции. Неотъемлемой частью технологии OFDM является охранный интервал (Guard Interval, GI) — циклическое повторение окончания символа, пристраиваемое в начале символа (рис. 18).

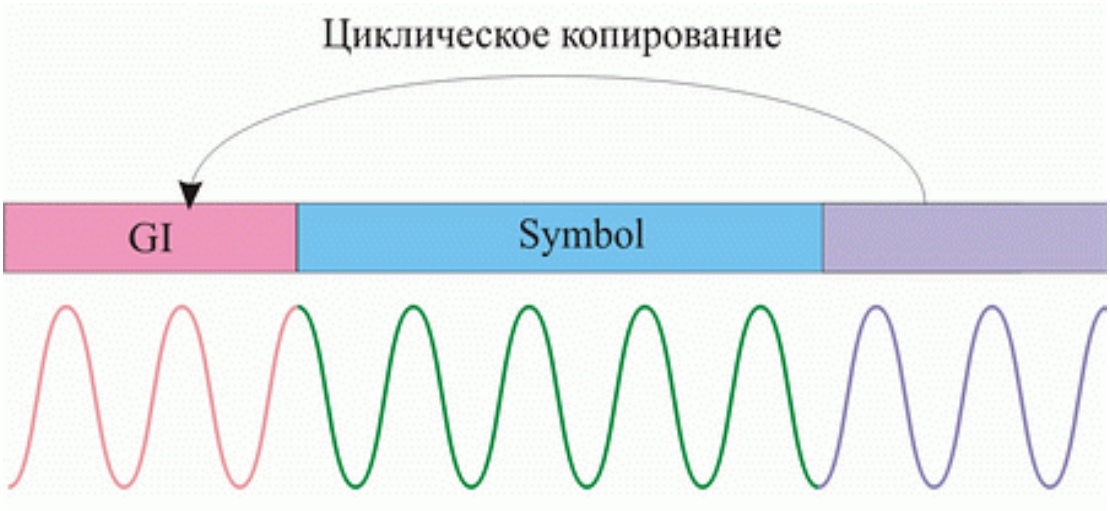



Рис. 18. Охранный интервал GI

Охранный интервал является избыточной информацией и в этом смысле снижает полезную (информационную) скорость передачи, но именно он служит защитой от возникновения межсимвольной интерференции. Эта избыточная информация добавляется к передаваемому символу в передатчике и отбрасывается при приеме символа в приемнике.

Наличие охранного интервала создает временные паузы между отдельными символами, и если длительность охранного интервала превышает максимальное время задержки сигнала в результате многолучевого распространения, то межсимвольной интерференции не возникает (рис. 19).

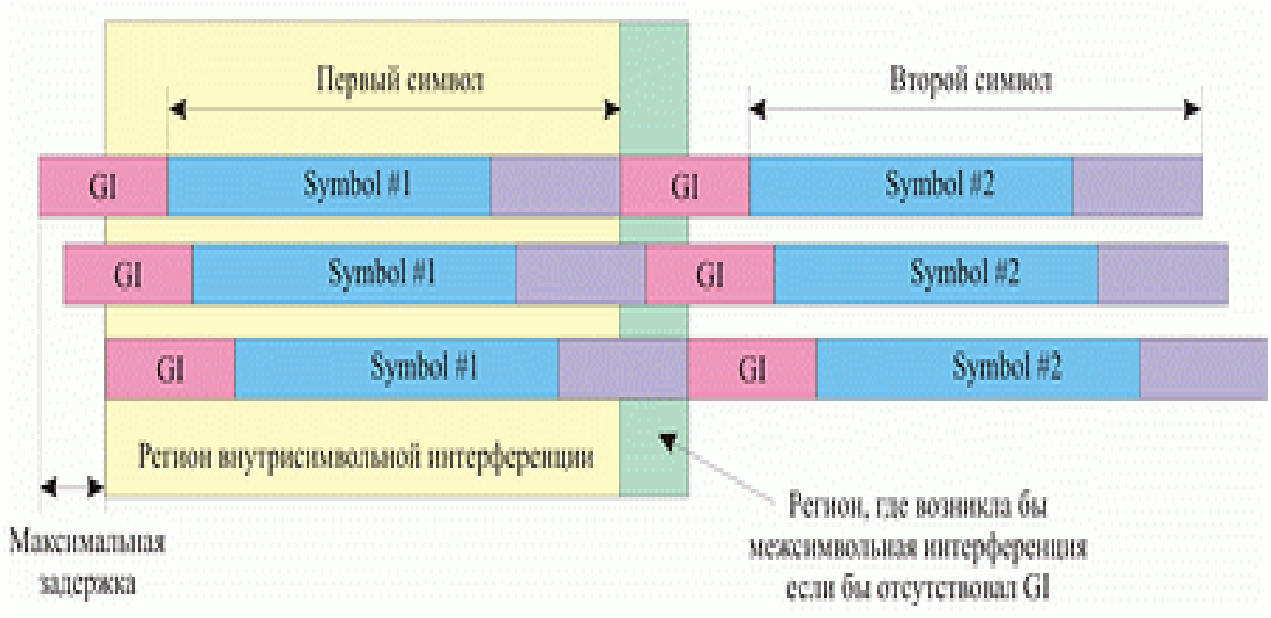



Рис. 19. Избежание межсимвольной интерференции за счет использования охранных интервалов

При использовании технологии OFDM длительность охранного интервала составляет одну четвертую длительности самого символа. При этом сам символ имеет длительность 3,2 мкс, а охранный интервал — 0,8 мкс. Таким образом, длительность символа вместе с охранным интервалом составляет 4 мкс.

Скоростные режимы и методы кодирования в протоколе 802.11g

В протоколе 802.11g предусмотрена передача на скоростях 1, 2, 5,5, 6, 9, 11, 12, 18, 22, 24, 33, 36, 48 и 54 Мбит/с. Обязательными являются скорости передачи 1; 2; 5,5; 6; 11; 12 и 24 Мбит/с, а более высокие скорости передачи (33, 36, 48 и 54 Мбит/с) — опциональными. Как уже отмечалось, протокол 802.11g включает в себя подмножество протоколы 802.11b. Технология кодирования PBCC опционально может использоваться на скоростях 5,5; 11; 22 и 33 Мбит/с. Кроме того, одна и та же скорость может реализовываться при различной технологии кодирования. Соотношение между различными скоростями передачи и используемыми методами кодирования отображено в табл. 7.

Говоря о технологии частотного ортогонального разделения каналов OFDM, применяемой на различных скоростях в протоколе 802.11g, мы до сих пор не касались вопроса о методе модуляции несущего сигнала.

Перейдем к рассмотрению методов модуляции применяемых стандартом 802.11g.

Напомню, что в протоколе 802.11b для модуляции использовалась либо двоичная (BDPSK), либо квадратурная (QDPSK) относительная фазовая модуляция. В протоколе 802.11g на низких скоростях передачи также используется фазовая модуляция (только не относительная), то есть

двоичная и квадратурная фазовые модуляции BPSK и QPSK. При использовании BPSK-модуляции в одном символе кодируется только один информационный бит, а при использовании QPSK-модуляции — два информационных бита. Модуляция BPSK используется для передачи данных на скоростях 6 и 9 Мбит/с, а модуляция QPSK — на скоростях 12 и 18 Мбит/с.

Для передачи на более высоких скоростях используется квадратурная амплитудная модуляция QAM (Quadrature Amplitude Modulation), при которой информация кодируется за счет изменения фазы и амплитуды сигнала. В протоколе 802.11g используется модуляция 16-QAM и 64-QAM. В первом случае имеется 16 различных состояний сигнала, что позволяет закодировать 4 бита в одном символе. Во втором случае имеется уже 64 возможных состояний сигнала, что позволяет закодировать последовательность 6 бит в одном символе. Модуляция 16-QAM применяется на скоростях 24 и 36 Мбит/с, а модуляция 64-QAM — на скоростях 48 и 54 Мбит/с.

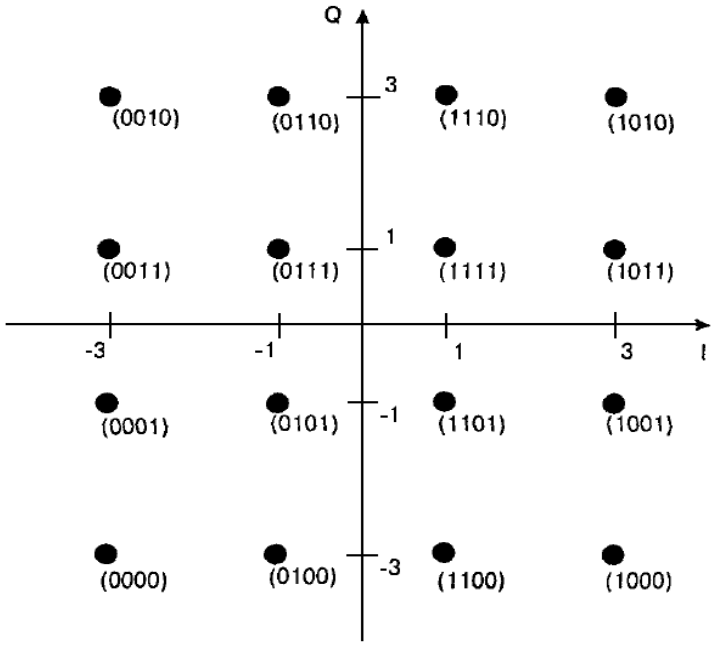



Рис. 20. Представление сигнала при QAM-16

Из таблицы 7 видно, что при одном и том же типе модуляции возможны различные скорости передачи. Рассмотрим как они получаются на примере модуляции BPSK, при которой скорость передачи данных составляет 6 или 9 Мбит/с. При использовании технологии OFDM используется сверточное кодирование с различными пунктурными кодерами, что приводит к различной скорости сверточного кодирования. В результате при использовании одного и того же типа модуляции могут получаться разные значения информационной скорости — все зависит от скорости сверточного кодирования. Так, при использовании BPSK-модуляции со скоростью сверточного кодирования 1/2 получаем информационную скорость 6 Мбит/с, а при использовании сверточного кодирования со скоростью 3/4 — 9 Мбит/с.

Таблица 7. Соотношение между скоростями передачи и типом кодирования в стандарте 802.11g

| Скорость передачи (Мбит/с) | | Метод кодирования | Модуляция |
|---|---|---|---|
| 1 | (опционально) | Код Баркера | DBPSK |
| 2 | (опциональн ) | Код Баркера | DQPSK |
| 5.5 | (обязательно) | CCK | DQPSK |
| | (опционально) | PBCC | DBPSK |
| 6 | (обязательно) | OFDM | BPSK |
| | (опционально) | CCK-OFDM | BPSK |
| 9 | (опционально) | OFDM, CCK-OFDM | BPSK |
| 11 | (обязательно) | CCK | DQPSK |
| | (опционально) | PBCC | DQPSK |
| 12 | (обязательно) | OFDM | Q SK |
| | (опционально) | CCK-OFDM | QPSK |
| 18 | (обязательно) | OFDM, CCK-OFDM | QPSK |
| 22 | (опционально) | PBCC | DQPSK |
| 24 | (обязательно) | OFDM | 16-QAM |
| | (опционально) | CCK-OFDM | |
| 33 | (опционально) | PBCC | |
| 36 | (опционально) | OFDM, CCK-OFDM | 16-QAM |
| 48 | (опционально) | OFDM, CCK-OFDM | 16 QAM |
| 54 | (опционально) | OFDM, CCK-OFDM | 16-QAM |

Стандарт также предусматривает применение гибридного кодирования. Для того чтобы понять сущность этого термина, вспомним, что любой передаваемый пакет данных содержит заголовок/преамбулу со служебный информацией и поле данных. Когда речь идет о пакете в формате CCK, имеется в виду, что заголовок и данные кадра передаются в формате CCK. Аналогично при использовании технологии OFDM заголовок кадра и данные передаются

посредством OFDM-кодирования. При применении технологии CCK-OFDM заголовок кадра кодируется с помощью CCK-кодов, но сами данные кадра передаются посредством многочастотного OFDM-кодирования. Таким образом, технология CCK-OFDM является своеобразным гибридом CCK и OFDM. Технология CCK-OFDM — не единственная гибридная технология: при использовании пакетного кодирования PBCC заголовок кадра передается с помощью CCK-кодов и только данные кадра кодируются посредством PBCC.

**Безопасность беспроводных LAN**

Так как беспроводные сети используют в качестве среды передачи радиоэфир они больше остальных подвержены опасности, любой желающий может получить доступ к информации передаваемой по радиоканалу. Единственным вариантом обеспечения конфиденциальности и целостности информации является применение стойких алгоритмов шифрования и надежных методов аутентификации. В первых редакциях стандарта защите, на мой взгляд, было уделено не достаточно внимания, отсутствовала возможность идентификации пользователя, применялся не стойкий алгоритм шифрования WEP. Однако с тех пор многое изменилось, и по мере повышения пропускной способности и надежности беспроводных сетей совершенствовались и стандарты обеспечения их безопасности. WPA и WPA2 — новейшие протоколы обеспечения безопасности беспроводных сетей, разработанные на основе стандарта IEEE 802.11i, — помогают надежно защитить трафик в беспроводных сетях даже в ситуациях, предъявляющих повышенные требования к безопасности. При правильной настройке системы с поддержкой этих стандартов защищены гораздо надежнее, чем прежние решения, и их можно смело использовать в корпоративных системах среднего размера.

В таблице приведены основные подходы к обеспечению безопасности беспроводных сетей.

Таблица 8. Сравнение подходов к обеспечению безопасности беспроводных сетей

| **Характеристики** | **WPA** | **WPA2** | **WEP** | **VPN** | **IPsec** |
|---|---|---|---|---|---|
| Строгая проверка подлинности | Да | Да | нет | Да[1] | Да[2] |
| Надежное шифрование данных | Да | Да | нет | Да | Да |
| Прозрачное подключение и восстановление подключения | Да | Да | Да | нет | Нет |
| Проверка подлинности пользователей | Да | Да | нет | Да | нет |

| | | | | | |
|---|---|---|---|---|---|
| Проверка подлинности компьютеров | Да | Да | Да | Нет | Да |
| Защита трафика при широковещательной и многоадресной передаче | Да | Да | Да | Да | нет |
| Потребность в дополнительных сетевых устройствах | Да[3] | Да[3] | Нет | Да[4] | Нет |
| Защита доступа к беспроводной сети помимо доступа к пакетам | Да | Да | Да | Нет | Нет |

1 - если не используется проверка подлинности с помощью общих ключей

2 - если используется проверка подлинности с помощью сертификатов или по протоколу Kerberos

3 - требуются серверы RADIUS

4 - требуются системы VPN и серверы RADIUS

Рассмотрим более подробно каждый из подходов к обеспечению безопасности.

**Алгоритм шифрования WEP**

Первая Спецификация стандарта 802.11 предусматривает обеспечение защиты данных с использованием алгоритма WEP (Wired Equivalent Protection). Этот алгоритм основан на применении симметричного поточного шифра RC4. Симметричность RC4 означает, что согласованные WEP-ключи размером 40 или 104 бит статично конфигурируются на клиентских устройствах и в точках доступа. Производители оборудования предлагают два способа конфигурирования ключей, ведение в поле «key» n-битного HEX числа или более удобный с точки зрения пользователя способ, введение некоторой последовательности ASCII символов которая в дальнейшем трансформируется в ключ. Алгоритм WEP был выбран главным образом потому, что он не требует объемных вычислений. WEP — простой в применении алгоритм, для записи которого в некоторых случаях достаточно 30 строк кода. Малые непроизводительные расходы, возникающие при применении этого алгоритма, делают его идеальным алгоритмом шифрования для специализированных устройств.

Чтобы избежать шифрования в режиме ECB (Electronic Code Book – при использовании этого режима  один и тот же открытый текст после шифрования преобразуется в один и тот же зашифрованный текст). Этот фактор потенциально представляет собой угрозу для безопасности, поскольку злоумышленники могут получать образцы зашифрованного текста и выдвигать какие-то предположения об исходном тексте ), WEP использует 24-разрядный вектор инициализации, который добавляется к ключу перед выполнением обработки по алгоритму RC4. Вектор инициализации должен изменяться пофреймово во избежание коллизий. Коллизии такого рода

происходят, когда используются один и тот же вектор инициализации и один и тот же WEP-ключ, в результате чего для шифрования фрейма используется один и тот же ключевой поток. Такая коллизия предоставляет злоумышленникам большие возможности по разгадыванию данных открытого текста путем сопоставления подобных элементов. При использовании вектора инициализации важно предотвратить подобный сценарий, поэтому вектор инициализации часто меняют. Большинство производителей предлагают пофреймовые векторы инициализации в своих устройствах для беспроводных LAN. На рисунке 4.21 показан фрейм зашифрованный с использованием алгоритма WEP.


Рис. 21. Фрейм, зашифрованный алгоритмом WEP

Спецификация стандарта 802.11 требует, чтобы одинаковые WEP-ключи были сконфигурированы как на клиентах, так и на устройствах, образующих инфраструктуру сети. Можно определять до четырех ключей на одно устройство, но одновременно для шифрования отправляемых фреймов используется только один из них.WEP-шифрование используется только по отношению к фреймам данных и во время процедуры аутентификации с совместно используемым ключом. По алгоритму WEP шифруются следующие поля фрейма данных стандарта 802.11. Данные или полезная нагрузка (payload).

- Контрольный признак целостности (integrity check value, ICV).

Значения всех остальных полей передаются без шифрования. Вектор инициализации должен быть послан незашифрованным внутри фрейма, чтобы приемная станция могла получить его и использовать для корректной расшифровки полезной нагрузки и ICV. На рис. 22 схематично представлен процесс шифрования.

В дополнение к шифрованию данных спецификация стандарта 802.11 предлагает использовать 32-разрядное значение, функция которого — осуществлять контроль целостности. Этот контрольный признак целостности говорит приемнику о том, что фрейм был получен без повреждения в процессе передачи. Контрольный признак целостности вычисляется по всем полям фрейма с использованием 32-разрядной полиномиальной функции контроля и с помощью циклического избыточного кода (CRC-32). Станция отправитель вычисляет это значение и

помещает его в поле ICV, приемная сторона расшифровывает фрейм вычисляет значение ICV и сравнивает его со значением в поле ICV. Если значения совпадают считается что фрейм не поддельный, в противном случае фрейм отбрасывается. На рис. 22 и 23 показан процесс дешифрования фреймов и вычисления контрольного признака целостности.

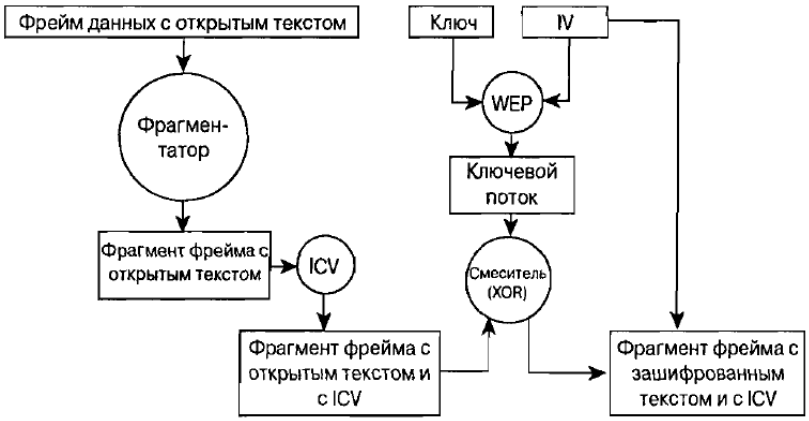



Рис. 22. Шифрование по алгоритму WEP

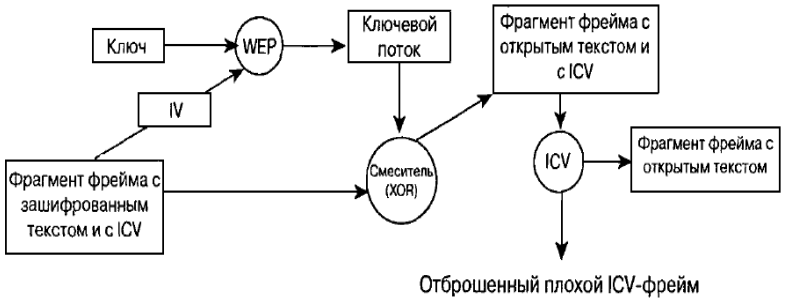



Рис. 23. Дешифрование по алгоритму WEP

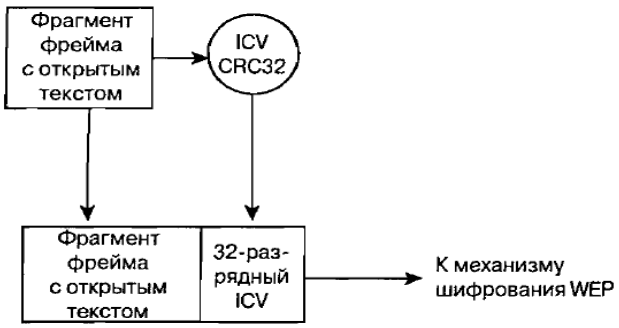



Рис. 24. Диаграмма функционирования механизма ICV

**Механизмы аутентификации стандарта 802.11**

Спецификация стандарта 802.11 оговаривает два механизма, которые могут применяться для аутентификации клиентов WLAN.

- Открытая аутентификация (open authentication).
- Аутентификация с совместно используемым ключом (shared key authentication).

Открытая аутентификация по сути представляет собой алгоритм с нулевой аутентификацией (null authentication algorithm). Точка доступа принимает любой запрос на аутентификацию. Это может быть просто бессмысленный сигнал, используемый для указания на применение именно этого алгоритма аутентификации, тем не менее открытая аутентификация играет определенную роль в сетях стандарта 802.11. Столь простые требования к аутентификации позволяют устройствам быстро получить доступ к сети.

Контроль доступа при открытой аутентификации осуществляется с использованием заранее сконфигурированного WEP-ключа в точке доступа и на клиентской станции. Эта станция и точка доступа должны иметь одинаковые ключи, тогда они могут связываться между собой. Если станция и точка доступа не поддерживают алгоритм WEP, в BSS невозможно обеспечить защиту. Любое устройство может подключиться к такому BSS, и все фреймы данных передаются незашифрованными.

После выполнения открытой аутентификации и завершения процесса ассоциирования клиент может начать передачу и прием данных. Если клиент сконфигурирован так, что его ключ отличается от ключа точки доступа, он не сможет правильно зашифровывать и расшифровывать фреймы, и такие фреймы будут отброшены как точкой доступа, так и клиентской станцией. Этот процесс предоставляет собой довольно-таки эффективное средство контроля доступа.

В отличие от открытой аутентификации, при аутентификации с совместно используемым ключом требуется, чтобы клиентская станция и точка доступа были способны поддерживать WEP и имели одинаковые WEP-ключи. Процесс аутентификации с совместно используемым ключом осуществляется следующим образом. Клиент посылает точке доступа запрос на аутентификацию с совместно используемым ключом. Точка доступа отвечает фреймом вызова (challenge frame), содержащим открытый текст. Клиент шифрует вызов и посылает его обратно точке доступа. Если точка доступа может правильно расшифровать этот фрейм и получить свой исходный вызов, клиенту посылается сообщение об успешной аутентификации. Клиент получает доступ WLAN.

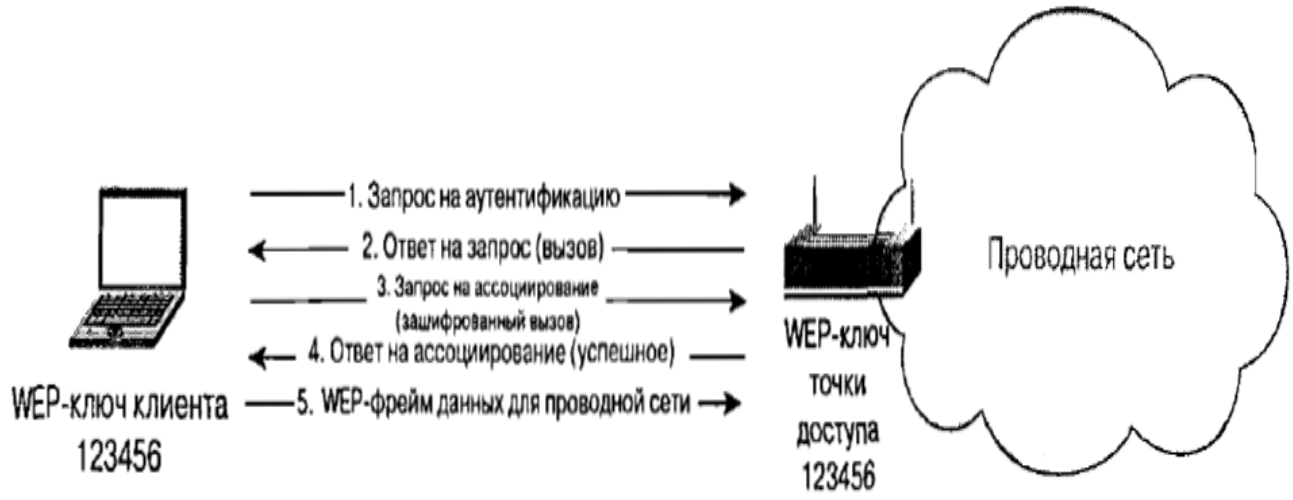



Рис. 25. Процесс аутентификации с совместно используемым ключом

Предпосылки, на которых основана аутентификация с совместно используемым ключом, точно такие же, как и те, которые предполагались при открытой аутентификации, использующей WEP-ключи в качестве средства контроля доступа. Разница между этими двумя схемами состоит в том, что клиент не может ассоциировать себя с точкой доступа при использовании механизма аутентификации с совместно используемым ключом, если его ключ не сконфигурирован должным образом.

**Уязвимости алгоритма WEP**

Проблемы алгоритма WEP носят комплексный характер и кроются в целой серии слабых мест: механизме обмена ключами (а точнее, практически полном его отсутствии); малых разрядностях ключа и вектора инициализации (Initialization Vector - IV); механизме проверки целостности передаваемых данных; способе аутентификации и алгоритме шифрования RC4.

Процесс шифрования WEP выполняется в два этапа. Вначале подсчитывается контрольная сумма (Integrity Checksum Value - ICV) с применением алгоритма Cyclic Redundancy Check (CRC-32), добавляемая в конец незашифрованного сообщения и служащая для проверки его целостности принимаемой стороной. На втором этапе осуществляется непосредственно шифрование. Ключ для WEP-шифрования - общий секретный ключ, который должны знать устройства на обеих сторонах беспроводного канала передачи данных. Этот секретный 40-битный ключ вместе со случайным 24-битным IV является входной последовательностью для генератора псевдослучайных чисел, базирующегося на шифре Вернама для генерации строки случайных символов, называемой ключевым потоком (key stream). Данная операция выполняется с целью избежания методов взлома, основанных на статистических свойствах открытого текста.

Initialization Vector (IV) используется, чтобы обеспечить для каждого сообщения свой уникальный ключевой поток. Зашифрованное сообщение образуется в результате выполнения операции XOR над незашифрованным сообщением с ICV и ключевым потоком. Чтобы

получатель мог прочитать его, в передаваемый пакет в открытом виде добавляется IV. Когда информация принимается на другой стороне, производится обратный процесс.

Таким образом, мы можем получить незашифрованный текст, являющийся результатом операции XOR между двумя другими оригинальными текстами. Процедура их извлечения не составляет большого труда. Наличие оригинального текста и IV позволяет вычислить ключ, что в дальнейшем даст возможность читать все сообщения данной беспроводной сети.

После несложного анализа можно легко рассчитать, когда повторится ключевой поток. Так как ключ постоянный, а количество вариантов IV составляет $2^{24}$=16 777 216, то при достаточной загрузке точки доступа, среднем размере пакета в беспроводной сети, равном 1500 байт (12 000 бит), и средней скорости передачи данных, например 5 Mbps (при максимальной 11 Mbps), мы получим, что точкой доступа будет передаваться 416 сообщений в секунду, или же 1 497 600 сообщений в час, т. е. повторение произойдет через 11 ч 12 мин ($2^{24}$/1 497 600=11,2 ч). Данная проблема носит название "коллизия векторов". Существует большое количество способов, позволяющих ускорить этот процесс. Кроме того, могут применяться атаки "с известным простым текстом", когда одному из пользователей сети посылается сообщение с заранее известным содержанием и прослушивается зашифрованный трафик. В этом случае, имея три составляющие из четырех (незашифрованный текст, вектор инициализации и зашифрованный текст), можно вычислить ключ. В работе "Intercepting Mobile Communications: The Insecurity of 802.11" было описано множество типов атак, включая довольно сложные, использующие манипуляции с сообщениями и их подмену, основанные на ненадежном методе проверки целостности сообщений (CRC-32) и аутентификации клиентов. С ICV, используемым в WEP-алгоритме, дела обстоят аналогично. Значение CRC-32 подсчитывается на основе поля данных сообщения. Это хороший метод для определения ошибок, возникающих при передаче информации, но он не обеспечивает целостность данных, т. е. не гарантирует, что они не были подменены в процессе передачи. Контрольная сумма CRC-32 имеет линейное свойство: CRC(A XOR B)=CRC(A)XOR CRC(B), предоставляющее нарушителю возможность легко модифицировать зашифрованный пакет без знания WEP-ключа и пересчитать для него новое значение ICV. Появившаяся в 2001 г. спецификация WEP2, которая увеличила длину ключа до 104 бит, не решила проблемы, так как длина вектора инициализации и способ проверки целостности данных остались прежними. Большинство типов атак реализовывались так же просто, как и раньше. На сегодняшний день использование алгоритма WEP для построение защищенных беспроводных сетей не допустимо.

**VPN**

Сегодня технология VPN (Virtual Private Network - виртуальная частная сеть) завоевала всеобщее признание и практически все компания организовывают VPN-каналы для сотрудников, работающих вне офиса. С помощью VPN можно организовать защищенный виртуальный канал

через публичные сети. Зашита трафика основана на криптографии. Наиболее часто используемым алгоритмом кодирования является Triple DES, который обеспечивает тройное шифрование (168 разрядов) с использованием трех разных ключей. Технология включает в себя проверку целостности данных и идентификацию пользователей, задействованных в VPN. Первая гарантирует, что данные дошли до адресата именно в том виде, в каком были посланы. Самые популярные алгоритмы проверки целостности данных - MD5 и SHA1. Далее система проверяет, не были ли изменены данные во время движения по сетям, по ошибке или злонамеренно. Таким образом, построение VPN предполагает создание защищенных от постороннего доступа туннелей между несколькими локальными сетями или удаленными пользователями. Для построения VPN необходимо иметь на обоих концах линии связи программы шифрования исходящего и дешифрования входящего трафиков. Они могут работать как на специализированных аппаратных устройствах, так и на ПК с такими операционными системами как Windows, Linux или NetWare. Чтобы организовать надежную защиту передаваемых данных и обеспечить прозрачность для устройств находящихся между концами виртуального туннеля применяется инкапсуляция, т.е. кадр сгенерированный узлом-отправителем шифруется и снабжается дополнительным заголовком содержащим информацию о маршруте. На другом конце туннеля заголовок отбрасывается, кадр дешифруется и доставляется по указанному в нем адресу.

Для формирования туннелей VPN используются протоколы PPTP, L2TP, IPsec, IP-IP. Протокол PPTP - позволяет инкапсулировать IP-, IPX- и NetBEUI-трафик в заголовки IP для передачи по IP-сети, например Internet.

Протокол L2TP - позволяет шифровать и передавать IP-трафик с использованием любых протоколов, поддерживающих режим `точка-точка` доставки дейтаграмм. Например, к ним относятся протокол IP, ретрансляция кадров и асинхронный режим передачи (ATM). Протокол IPsec - позволяет шифровать и инкапсулировать полезную информацию протокола IP в заголовки IP для передачи по IP-сетям.

Для технической реализации VPN, кроме стандартного сетевого оборудования, понадобится шлюз VPN, выполняющий все функции по формированию туннелей, защите информации, контролю трафика, а нередко и функции централизованного управления. Рассмотренная технология является достаточно мощным средством зашиты передаваемого трафика, однако ее применение в беспроводных сетях имеет ряд недостатков. Основной из них: для реализации технологии необходим VPN шлюз, для большого числа клиентов этот участок сети может стать узким местом и снизит пропускную способность. К тому же беспроводным клиентам придется сначала проходить процедуру аутентификации на точке а затем устанавливать VPN соединение, что не совсем удобно. По этой причине рассматривать технологию VPN как вариант зашиты при проектировании беспроводной сети не стоит, технология может применятся лишь в сетях не поддерживающих современные методы зашиты данных (WPA или WPA2) как последняя

возможность повышения безопасности без глобального обновления оборудования.

**IPSec. Архитектура IPSec**

IP Security - это комплект протоколов, касающихся вопросов шифрования, аутентификации и обеспечения защиты при транспортировке IP-пакетов; в его состав сейчас входят почти 20 предложений по стандартам и 18 RFC. Спецификация IP Security (известная сегодня как IPsec) разрабатывается рабочей группой IP Security Protocol IETF. Первоначально IPsec включал в себя 3 алгоритмо-независимые базовые спецификации, опубликованные в качестве RFC-документов "Архитектура безопасности IP", "Аутентифицирующий заголовок (AH)", "Инкапсуляция зашифрованных данных (ESP)" (RFC1825, 1826 и 1827). Сейчас предложены новые версии этих спецификаций, это RFC2401 - RFC2412. Отмечу, что RFC1825-27 на протяжении уже нескольких лет считаются устаревшими. Кроме этого, существуют несколько алгоритмо-зависимых спецификаций, использующих протоколы MD5, SHA, DES.

Гарантии целостности и конфиденциальности данных в спецификации IPsec обеспечиваются за счет использования механизмов аутентификации и шифрования соответственно. Последние, в свою очередь, основаны на предварительном согласовании сторонами информационного обмена т.н. "контекста безопасности" – применяемых криптографических алгоритмов, алгоритмов управления ключевой информацией и их параметров. Спецификация IPsec предусматривает возможность поддержки сторонами информационного обмена различных протоколов и параметров аутентификации и шифрования пакетов данных, а также различных схем распределения ключей. При этом результатом согласования контекста безопасности является установление индекса параметров безопасности (SPI), представляющего собой указатель на определенный элемент внутренней структуры стороны информационного обмена, описывающей возможные наборы параметров безопасности.

По сути, IPSec, работает на третьем уровне, т. е. на сетевом уровне. В результате передаваемые IP-пакеты защищены прозрачным для сетевых приложений и инфраструктуры образом. В отличие от SSL (Secure Socket Layer), который работает на четвертом (т. е. транспортном) уровне и теснее связан с более высокими уровнями модели OSI, IPSec призван обеспечить низкоуровневую защиту.

К IP-данным, готовым к передаче по виртуальной частной сети, IPSec добавляет заголовок для идентификации защищенных пакетов. Перед передачей по Internet эти пакеты инкапсулируются в другие IP-пакеты. IPSec поддерживает несколько типов шифрования, в том числе Data Encryption Standard (DES) и Message Digest 5 (MD5).

Чтобы установить защищенное соединение, оба участника сеанса должны иметь возможность быстро согласовать параметры защиты, такие как алгоритмы аутентификации и ключи. IPSec поддерживает два типа схем управления ключами, с помощью которых участники могут согласовать параметры сеанса.

С текущей версией IP, IPv4, могут быть использованы или Internet Secure Association Key Management Protocol (ISAKMP), или Simple Key Management for Internet Protocol. С версией IPv6, придется использовать ISAKMP.

**Заголовок AH**

Аутентифицирующий заголовок (AH) является обычным опциональным заголовком и, как правило, располагается между основным заголовком пакета IP и полем данных. Наличие AH никак не влияет на процесс передачи информации транспортного и более высокого уровней. Основным и единственным назначением AH является обеспечение защиты от атак, связанных с несанкционированным изменением содержимого пакета, и в том числе от подмены исходного адреса сетевого уровня. Протоколы более высокого уровня должны быть модифицированы в целях осуществления проверки аутентичности полученных данных.

Формат AH достаточно прост и состоит из 96-битового заголовка и данных переменной длины, состоящих из 32-битовых слов. Названия полей достаточно ясно отражают их содержимое: Next Header указывает на следующий заголовок, Payload Len представляет длину пакета, SPI является указателем на контекст безопасности и Sequence Number Field содержит последовательный номер пакета.

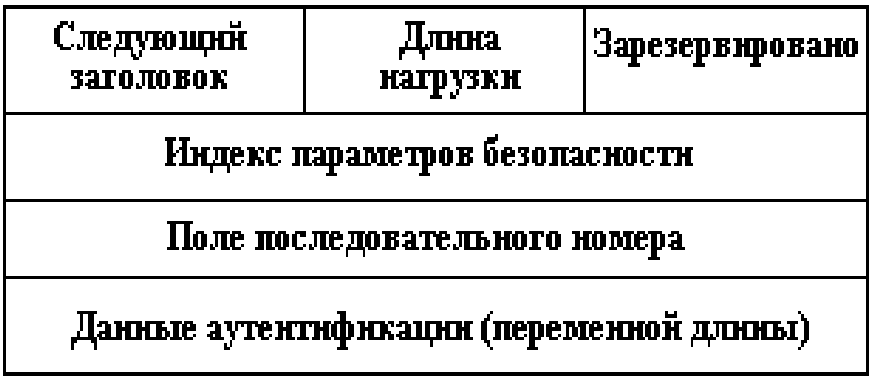



Рис. 26. Формат заголовка AH

Последовательный номер пакета был введен в AH в 1997 году в ходе процесса пересмотра спецификации IPsec. Значение этого поля формируется отправителем и служит для защиты от атак, связанных с повторным использованием данных процесса аутентификации. Поскольку сеть Интернет не гарантирует порядок доставки пакетов, получатель должен хранить информацию о максимальном последовательном номере пакета, прошедшего успешную аутентификацию, и о получении некоторого числа пакетов, содержащих предыдущие последовательные номера (обычно это число равно 64).

В отличие от алгоритмов вычисления контрольной суммы, применяемых в протоколах передачи информации по коммутируемым линиям связи или по каналам локальных сетей и ориентированных на исправление случайных ошибок среды передачи, механизмы обеспечения

целостности данных в открытых телекоммуникационных сетях должны иметь средства защиты от внесения целенаправленных изменений. Одним из таких механизмов является специальное применение алгоритма MD5: в процессе формирования AH последовательно вычисляется хэш-функция от объединения самого пакета и некоторого предварительно согласованного ключа, а затем от объединения полученного результата и преобразованного ключа.

**Заголовок ESP**

В случае использования инкапсуляции зашифрованных данных заголовок ESP является последним в ряду опциональных заголовков, "видимых" в пакете. Поскольку основной целью ESP является обеспечение конфиденциальности данных, разные виды информации могут требовать применения существенно различных алгоритмов шифрования. Следовательно, формат ESP может претерпевать значительные изменения в зависимости от используемых криптографических алгоритмов. Тем не менее, можно выделить следующие обязательные поля: SPI, указывающее на контекст безопасности и Sequence Number Field, содержащее последовательный номер пакета. Поле "ESP Authentication Data" (контрольная сумма), не является обязательным в заголовке ESP. Получатель пакета ESP расшифровывает ESP заголовок и использует параметры и данные применяемого алгоритма шифрования для декодирования информации транспортного уровня.


Рис. 27. Формат заголовка ESP

Различают два режима применения ESP и AH - транспортный и туннельный.

**Транспортный режим**

Транспортный режим используется для шифрования поля данных IP пакета, содержащего протоколы транспортного уровня (TCP, UDP, ICMP), которое, в свою очередь, содержит информацию прикладных служб. Примером применения транспортного режима является передача электронной почты. Все промежуточные узлы на маршруте пакета от отправителя к

получателю используют только открытую информацию сетевого уровня и, возможно, некоторые опциональные заголовки пакета (в IPv6). Недостатком транспортного режима является отсутствие механизмов скрытия конкретных отправителя и получателя пакета, а также возможность проведения анализа трафика. Результатом такого анализа может стать информация об объемах и направлениях передачи информации, области интересов абонентов, расположение руководителей.

**Туннельный режим**

Туннельный режим предполагает шифрование всего пакета, включая заголовок сетевого уровня. Туннельный режим применяется в случае необходимости скрытия информационного обмена организации с внешним миром. При этом, адресные поля заголовка сетевого уровня пакета, использующего туннельный режим, заполняются межсетевым экраном организации и не содержат информации о конкретном отправителе пакета. При передаче информации из внешнего мира в локальную сеть организации в качестве адреса назначения используется сетевой адрес межсетевого экрана. После расшифровки межсетевым экраном начального заголовка сетевого уровня пакет направляется получателю.

**Security Associations**

Security Association (SA) – это соединение, которое предоставляет службы обеспечения безопасности трафика, который передаётся через него. Два компьютера на каждой стороне SA хранят режим, протокол, алгоритмы и ключи, используемые в SA. Каждый SA используется только в одном направлении. Для двунаправленной связи требуется два SA. Каждый SA реализует один режим и протокол; таким образом, если для одного пакета необходимо использовать два протокола (как например AH и ESP), то требуется два SA.

**Политика безопасности**

Политика безопасности хранится в SPD (База данных политики безопасности). SPD может указать для пакета данных одно из трёх действий: отбросить пакет, не обрабатывать пакет с помощью IPSec, обработать пакет с помощью IPSec. В последнем случае SPD также указывает, какой SA необходимо использовать (если, конечно, подходящий SA уже был создан) или указывает, с какими параметрами должен быть создан новый SA.

SPD является очень гибким механизмом управления, который допускает очень хорошее управление обработкой каждого пакета. Пакеты классифицируются по большому числу полей, и SPD может проверять некоторые или все поля для того, чтобы определить соответствующее действие. Это может привести к тому, что весь трафик между двумя машинами будет передаваться при помощи одного SA, либо отдельные SA будут использоваться для каждого приложения, или даже для каждого TCP соединения.

IPsec достаточно хорошо противостоит большинству известным сетевым атакам (sniffing, spoofing, hijacking). Благодаря тому что предусмотрен механизм отбраковки пакетов не удовлетворяющих политики безопасности, IPsec не плохо справляется с атаками Denial-Of-Service

(DOS). Replay Attack - нивелируется за счет использования Sequence Number.

К сожалению, с использованием протокола IPsec для защиты беспроводных сетей связаны некоторые проблемы. Протокол IPsec не позволяет защищать трафик при широковещательной или многоадресной передаче, потому что его действие может распространяться только на взаимодействие двух сторон, обменявшихся ключами и выполнивших взаимную проверку их подлинности. Протокол IPsec защищает только сетевые пакеты, но не саму беспроводную сеть. Несмотря на прозрачность протокола IPsec для пользователей, для сетевых устройств он прозрачен не полностью, потому что работает на сетевом уровне, а не на MAC-уровне. Это предъявляет дополнительные требования к правилам для брандмауэров. Все устройства, не поддерживающие IPsec, уязвимы перед зондированием или атаками со стороны любых пользователей, способных осуществлять мониторинг трафика в беспроводной сети. Если протокол IPsec используется в крупной системе не только для защиты трафика беспроводной сети, но и для комплексной защиты трафика других приложений, управлять политиками IPSec будет сложно

**Потокол WPA**

WPA включает в себя улучшенный механизм аутентификации и шифрования. Эти изменения были внесены в проект стандарта 802.11i, однако Альянс Wi-Fi собрав поднабор компонентов, соответствующих стандарту 802.11i  не дожидаясь официального принятия внедрил их поддержку в выпускаемое оборудование. Протокол получил название «защищенный доступ к Wi-Fi» (Wi-Fi Protected Access, WPA).

Защита беспроводных сетей имеет четыре составляющие. Базовая аутентификация (authentication framework). Представляет собой механизм, который усиливает действие алгоритма аутентификации путем организации защищенного обмена сообщениями между клиентом, точкой доступа и сервером аутентификации. Алгоритм аутентификации. Представляет собой алгоритм, посредством которого подтверждаются полномочия пользователя.

- Алгоритм защиты данных. Обеспечивает защиту при передаче через беспроводную среду фреймов данных. Алгоритм обеспечения целостности. (data integrity algorithm). Обеспечивает целостность данных при передаче их через беспроводную среду, позволяя приемнику убедиться в том, что данные не были подменены.

**Базовая аутентификация**

Основные компоненты, обеспечивающие эффективную аутентификацию – это :

1. - централизованная аутентификация, ориентированная на пользователя;
2. - динамические ключи;
3. - управление зашифрованными ключами;
4. - взаимная аутентификация.

Аутентификация, ориентированная на пользователя, чрезвычайно важна для обеспечения

защиты сети. Аутентификация, ориентированная на устройства, подобная скрытой аутентификации и аутентификации с совместно используемым ключом, не способна воспрепятствовать неавторизованным пользователям воспользоваться авторизованным устройством. Из этого следует, что при потере и краже такого устройства или по окончании работы по найму администратор сети будет вынужден вручную изменять ключи всех точек доступа и клиентов сети стандарта 802.11. При централизованном, ориентированном на пользователя управлении через сервер аутентификации, авторизации и учета (authentication, authorization and accounting, AAA), такой как Radius, администратор может запретить доступ к сети отдельным пользователям, а не их устройствам.

Аутентификация, которая поддерживает создание динамических ключей, хорошо подходит для улучшения защиты беспроводных LAN и модели управления ими. Динамические ключи, индивидуальные для каждого пользователя, освобождают администратора от необходимости использования статически управляемых ключей. Динамические ключи сами назначаются и аннулируются, когда пользователь проходит аутентификацию.

Взаимная аутентификация – это аутентификация, при которой не только сеть аутентифицирует пользователя, но и пользователь сеть. Технология WPA, призванная временно (в ожидании перехода к 802.11i) закрыть бреши WEP, состоит из нескольких компонентов:

- - протокол 802.1x - универсальный протокол для аутентификации, авторизации и учета (AAA);
- - протокол EAP - расширяемый протокол аутентификации (Extensible Authentication Protocol);
- - протокол TKIP - протокол временной целостности ключей, другой вариант перевода - протокол целостности ключей во времени (Temporal Key Integrity Protocol);
- - MIC - криптографическая проверка целостности пакетов (Message Integrity Code);
- - протокол RADIUS.

**Проктокол 802.1X**

Протокол 802.1x может выполнять несколько функций. В данном случае нас интересуют функции аутентификации пользователя и распределение ключей шифрования. Необходимо отметить, что аутентификация происходит «на уровне порта» - то есть пока пользователь не будет аутентифицирован, ему разрешено посылать/принимать пакеты, касающиеся только процесса его аутентификации (учетных данных) и не более того. И только после успешной аутентификации порт устройства (будь то точка доступа или коммутатор) будет открыт и пользователь получит доступ к ресурсам сети. IEEE 802.11x определяет три основных компонента в сетевом окружении: Саппликант (supplicant) – объект которому необходима аутентификация. Сервер аутентификации (authentication server) – объект, обеспечивающий службы аутентификации. В стандарте четко не

определено, что должно выступать в качестве сервера аутентификации, но, как правило, им является сервер RADIUS (Remote Access Dial In User Service).

Аутентификатор (authenticator) – объект на конце сегмента "точка--точка" локальной вычислительной сети, который способствует аутентификации объектов. Другими словами, это устройство-посредник, располагаемое между сервером аутентификации и саппликантом. Обычно его роль выполняет беспроводная точка доступа.

Аутентификатор создает логический порт для устройства саппликанта. Этот логический порт имеет два тракта прохождения данных: неконтролируемый и контролируемый. Неконтролируемый порт позволяет проходить через тракт всему трафику аутентификации. Контролируемый тракт блокирует прохождение трафика до тех пор, пока не будет осуществлена успешная аутентификация клиента. См. рисунок 6.8.

Во время аутентификации обмен сообщениями осуществляется следующим образом. Клиент-проситель ассоциируется с аутентификатором точкой доступа. Аутентификатор предоставляет порт просителю. Переводит порт в неавторизованное состояние. Клиент начинает аутентификацию. Аутентификатор отвечает сообщением с EAP запросом на аутентификацию просителю, чтобы удостовериться в идентичности клиента. На сервер аутентификации отправляется пакет, содержащий идентификационные данные клиента.

1. В завершении посылается пакет RADUIS-ACCEPS, RADIUS-REJECT, направленный от сервера аутентификации к точке доступа.
2. Аутентификатор переводит порт клиента в состояние “авторизован”.

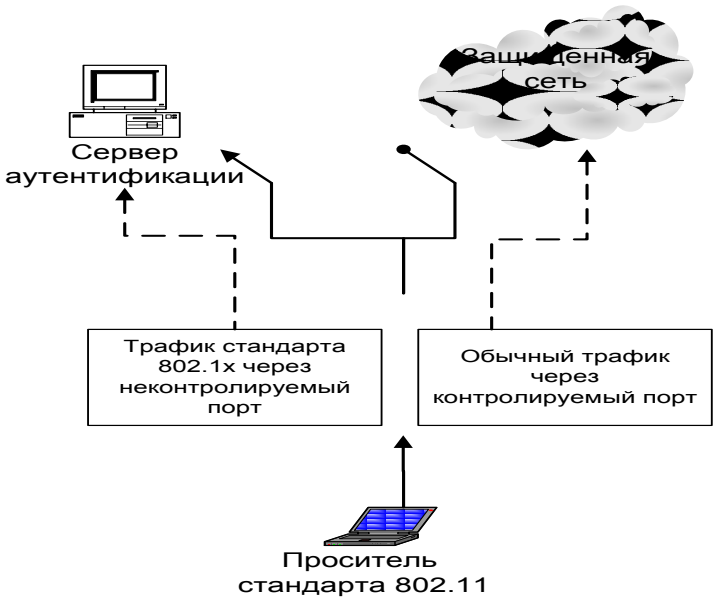



Рис. 28. Логические порты аутентификатора стандарта 802.1X

**Протокол EAP**

Протокол EAP (Extensible Authentication Protocol) был создан с целью упразднения частных механизмов аутентификации и распространения стандартизированных подходов – схем типа "запрос-ответ" (challenge-response) и инфраструктуры, основанной на публичных ключах и пользовательских сертификатах. Стандартизация механизмов EAP позволила сделать процедуру аутентификации прозрачной для серверов доступа различных производителей. Например, при подключении пользователя к серверу удаленного доступа и использовании механизма EAP протокола PPP для аутентификации сам сервер доступа не должен знать или поддерживать конкретные механизмы или алгоритмы аутентификации, его задача в этом случае – лишь передать пакеты EAP-сообщений RADIUS-серверу, на котором фактически производится аутентификация. В этом случае сервер доступа исполняет роль посредника между клиентом и RADIUS-сервером, в задачи которого входит передача EAP-сообщений между ними.

Перечислим наиболее распространенные методы аутентификации

- LEAP – алгоритм взаимной аутентификации с использованием пароля. Пропреоретарный метод от Cisco systems. Поддерживается оборудованием компании Cisco.
- EAP-MD5 - процедура односторонней аутентификации саппликанта сервером аутентификации, основанная на применении хэш-суммы MD5 имени пользователя и пароля как подтверждение для сервера RADIUS. Данный метод не поддерживает ни управления ключами, ни создания динамических ключей. Является простейшим и не стойким методом.
- EAP-TLS - процедура аутентификации, которая предполагает использование цифровых сертификатов X.509 в рамках инфраструктуры открытых ключей (Public Key Infrastructure – PKI). EAP-TLS поддерживает динамическое создание ключей и взаимную аутентификацию между саппликантом и сервером аутентификации. Недостатком данного метода является необходимость поддержки инфраструктуры открытых ключей. EAP-TTLS - EAP, разработанный компаниями Funk Software и Certicom и расширяющий возможности EAP-TLS. EAP-TTLS использует безопасное соединение, установленное в результате TLS-квитирования для обмена дополнительной информацией между саппликантом и сервером аутентификации. В результате дальнейший процесс может производиться с помощью других протоколов аутентификации, например таких, как: PAP, CHAP, MS-CHAP или MS-CHAP-V2. EAP-PEAP – этот метод перед непосредственной аутентификацией пользователя сначала образует TLS-туннель между клиентом и сервером аутентификации. А уже внутри этого туннеля осуществляется сама аутентификация с использованием стандартного EAP (MD5, TLS, MSCHAP V2). EAP-MSCHAP V2 - метод аутентификации на основе логина/пароля пользователя в MS-сетях. Данный метод поддерживает функции управления ключами и создания динамических ключей.

**Протокол TKIP**

Temporal Key Integrity Protocol (TKIP) – протокол, предусмотренный спецификацией WPA. TKIP предназначен для решения основных проблем WEP в области шифрования данных. Для совместимости с существующим аппаратным обеспечением TKIP использует тот же алгоритм шифрования, что и WEP – RC4. TKIP подразумевает несколько способов повышения защищенности беспроводных сетей:

- - динамические ключи;
- - измененный метод генерации ключей;
- - более надежный механизм проверки целостности сообщений;
- - увеличенный по длине вектор инициализации (до 48-разрядного);
- - нумерация пакетов.

Основные усовершенствования, внесенные протоколом TKIP, следующие. Пофреймовое изменение ключей шифрования. Контроль целостности сообщения (message integrity check, MIC). Обеспечивается эффективный контроль целостности фреймов данных с целью предотвращения проведения тайных манипуляций с фреймами и воспроизведения фреймов.

Основной принцип, на котором основано пофреймовое изменение ключа, состоит в том, что IV, MAC - адрес передатчика и WEP – ключ обрабатывается вместе с помощью двухступенчатой функции перемешивания. Вектор инициализации имеет 48 разрядный размер (в отличие от 24 разрядного в других протоколах) и он разбит на две части – старшие 32 разряда и младшие 16 разрядов.

Пофреймово изменяемый ключ имеет силу только тогда, когда 16-разрядные значения IV не используются повторно. Если 16-разрядные значения IV используются дважды, происходит коллизия, в результате чего появляется возможность провести атаку и вывести ключевой поток. Чтобы избежать коллизий IV, значение ключа 1-ой фазы вычисляется заново путем увеличения старших 32 разрядов IV на 1 и повторного вычисления пофреймового ключа.

Процесс пофреймового изменения ключа происходит следующим образом.

1. Базовый ключ, полученный во время аутентификации и имеющий размерность в 128 разрядов, перемешивается со старшими 32 разрядами 48 разрядного вектора инициализации и 48-разрядным MAC адресом передатчика (TA). Результат этого действия называется ключом первой фазы (80-разрядный). Ключ первой фазы снова перемешивается с IV и TA для выработки значения пофреймового ключа (128-разрядный, первые 16 разрядов – это IV). IV, используемый для передачи фрейма имеет размер 16 битов (0-65535). Пофреймовый ключ используется для шифрования данных. Когда 16-битовое пространство IV оказывается исчерпанным, ключ 1-й фазы отбрасывается и 32 старших разряда увеличиваются на 1. Заново вычисляется значение пофреймового ключа (рис. 29)

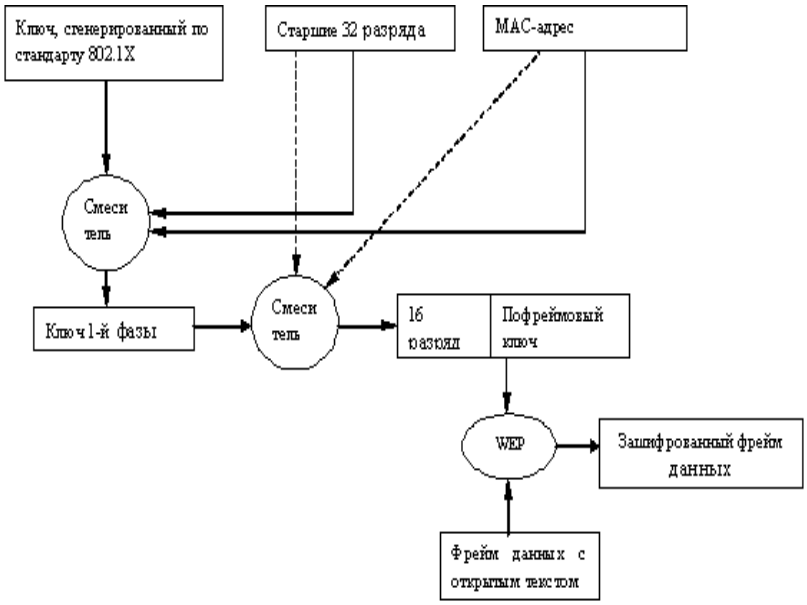



Рис. 29. Пофреймовое изменение ключей

### 6.5.5 Проверка целостности сообщений MIC

MIC Проверка целостности сообщений (Message Integrity Check, MIC) предназначена для предотвращения захвата пакетов данных, изменения их содержимого и повторной пересылки. MIC построена на базе мощной математической функции, которую применяют отправитель и получатель, а затем сравнивают результат. Если он не совпадает, то данные считаются ложными и пакет отбрасывается.

В отличие от WEP, где для контроля целостности передаваемых данных использовалась CRC-32, TKIP применяет MIC, обеспечивающий криптографическую контрольную сумму от нескольких полей (адрес источника, адрес назначения и поля данных). Так как классические MIC-алгоритмы (например, HMAC-MD5 или HMAC-SHA1) для существующего беспроводного оборудования являлись очень "тяжелыми" и требовали больших вычислительных затрат, то специально для использования в беспроводных сетях Нильсом Фергюсоном (Niels Ferguson) был разработан алгоритм Michael. Для шифрования он применяет 64-битный ключ и выполняет действия над 32-битными блоками данных. MIC включается в зашифрованную часть фрейма между полем данных и полем ICV.

Для обеспечения целостности данных в протоколе TKIP, помимо механизма MIC, предусмотрена еще одна функция, отсутствовавшая в WEP, -- нумерация пакетов. В качестве номера используется IV, который теперь называется TKIP Sequence Counter (TSC) и имеет длину 48 бит, в отличие от 24 бит в WEP. Увеличение длины IV до 48 бит позволяет избежать коллизии векторов и гарантирует, что они не повторятся на протяжении многих лет.

Основным и самым важным отличием TKIP от WEP является механизм управления ключами, позволяющий периодически изменять ключи и производить обмен ими между всеми участниками

сетевого взаимодействия: саппликантом, аутентификатором и сервером аутентификации. В процессе работы и аутентификации на разных этапах взаимодействия и для различных целей генерируются специализированные ключи. На рис. 30 показан механизм работы алгоритма MIC.

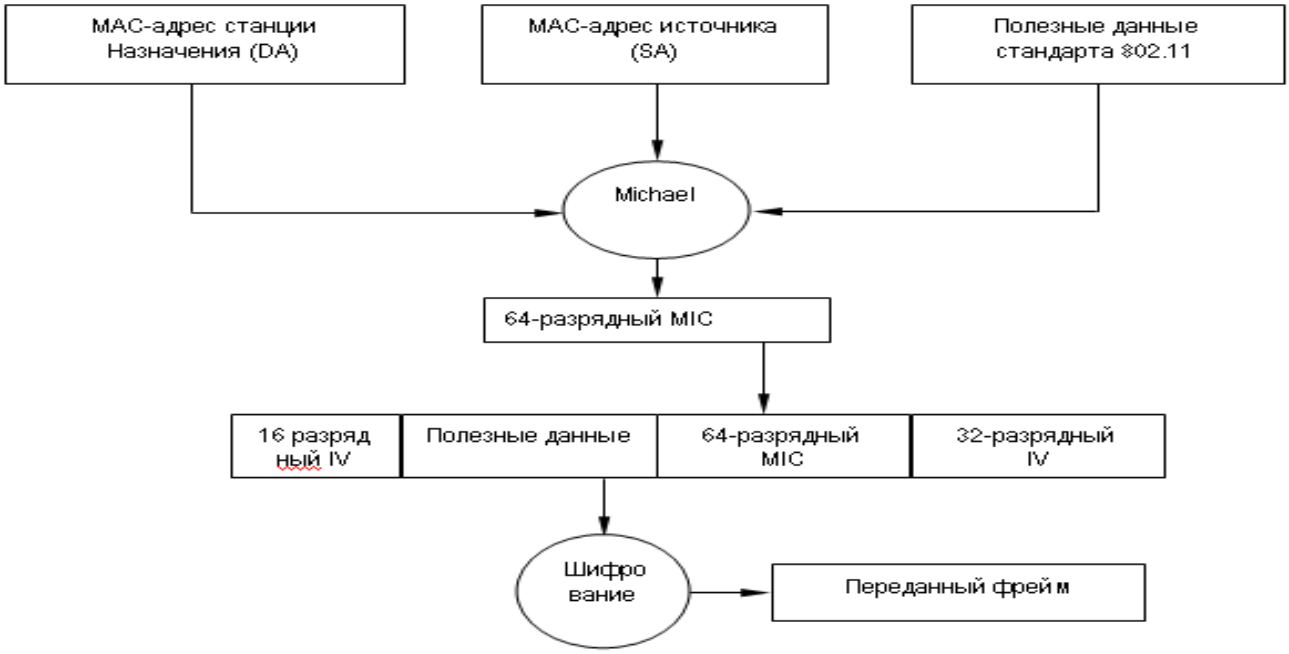



Рис. 30. Работа алгоритма MIC

Итак, зная каким образом происходит пофреймовое изменение ключей, а также понимая принцип работы алгоритма контроля целостности сообщений MIC, можно рассмотреть алгоритм шифрования данных TKIP (рис. 31).

1. Генерируется пофреймовый ключ. Алгоритм MIC генерирует MIC для фрейма вцелом. Фрейм фрагментируется в соответствии с установками MAC для фрейма в целом. Фрагменты фрейма шифруются с помощью пофреймового ключа. Осуществляется передача зашифрованных фреймов.

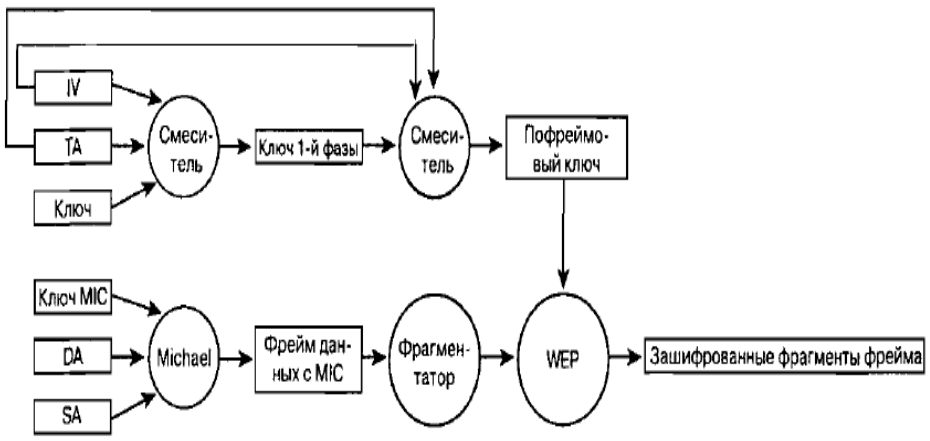



Рис. 31 – Алгоритм шифрования TKIP

**Стандарт 802.11i**

Стандарт 802.11i или WPA2 был принят в сентябре 2004 года организацией Wi-Fi Alliance и представляет собой сертифицированную совместимую версию полной спецификации IEEE 802.11i, принятой в июне 2004 года. Как и предшествующий ему стандарт, WPA2 поддерживает проверку подлинности по протоколу IEEE 802.1X/EAP или технологию предварительных ключей, но, в отличие от своего предшественника, содержит новый усовершенствованный механизм шифрования AES (Advanced Encryption Standard) со 128 битным ключом.

AES пришел на смену DES, в его основе лежит алгоритм Rijndael. Согласно оценкам, Rijndael не подвержен следующим видам криптоаналитических атак:

1. У алгоритма отсутствуют слабые ключи, а также возможности его вскрытия с помощью атак на связанных ключах.
2. К алгоритму не применим дифференциальный криптоанализ.
3. Алгоритм не атакуем с помощью линейного криптоанализа и усеченных дифференциалов.
4. Square-атака (специфичная атака на алгоритмы со структурой «квадрат», к которым относится и AES) также не применима к алгоритму Rijndael.
5. Алгоритм не вскрывается методом интерполяции.

1. Сервер устанавливает с клиентом TLS – туннель (в моем случае у клиента имеется сертификат сервера аутентификации. Сервер передает зашифрованный ключ сеанса, клиент используя открытый ключ содержащийся в сертификате и расшифровывает ключ сеанса). Сервер аутентификации внутри сформированного туннеля начинает аутентификацию клиента, для этого посылается запрос на предоставление необходимой для аутентификации информации. Так как используется MSCHAP V2 клиент пересылает свой логин и пароль. Сервер аутентификации проверяет имя пользователя и пароль в Active Directory и после удачной проверки посылает беспроводному коммутатору сообщение RADIUS ACCEPT содержащее динамический ключ для шифрования трафика. Коммутатор передает динамический ключ клиенту используя ключ сеанса. Коммутатор устанавливает с клиентом защищенное VPN соединения и переводит клиентский порт в состояние допускающее перенаправление трафика

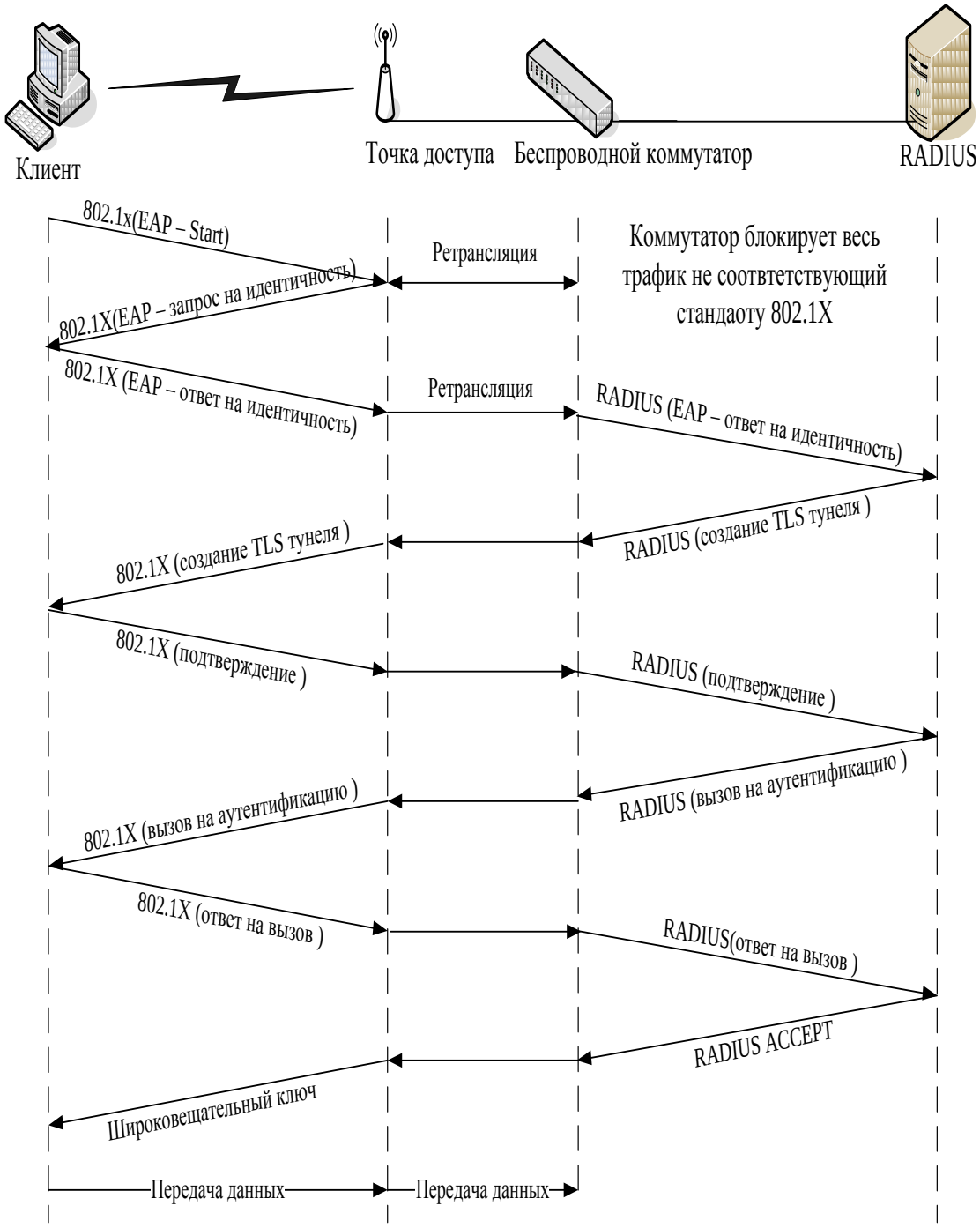



Рис. 37. Процедура прохождения аутентификации EAP-PEAP-MSCHAP V2

**Роуминг в сетях 802.11**

Роуминг делится на два основных вида:

- - бесшовный роуминг (seamless roaming);
- - кочевой роуминг (nomadic roaming).

Бесшовный роуминг обеспечивает «незаметный» для абонента переход в зону обслуживания новой базовой станции, т.е. без потери соединения и за небольшой промежуток времени (например, при переходе абонента сети GSM он может продолжать говорить). Кочевой роуминг означает, что абонент должен разорвать текущий сеанс связи найти новую базовую станцию и

ассоциироваться с ней. Именно кочевой роуминг может быть организован, в сетях стандарта 802.11 без применения дополнительного оборудования. Для этого на клиентском ПК необходимо настроить соединения с каждой из точек доступа (настроить параметры аутентификации). Однако это не очень удобно так как переходя в зону обслуживания клиент должен будет вновь восстанавливать все сетевые сеансы, к тому же он должен будет повторно проходить процедуру аутентификации которая занимает 10 – 40 секунд. По этому в проектируемой сети будет реализован бесшовный роуминг. Прежде чем переходить к рассмотрению процесса бесшовного роуминга познакомимся с основными понятиями.

Домен роуминга. Под доменом роуминга понимается совокупность точек доступа, относящихся к одному широковещательному домену, и сконфигурированных, так что они имеют одинаковый идентификатор зоны обслуживания (SSID).

Длительность роуминга. Под длительностью роуминга понимается время необходимое для осоциирования абонента с новой точкой доступа. Этот процесс включает следующие фазы: процесс зондирования; процесс аутентификации по стандарту 802.11; процесс ассоциирования по стандарту 802.11; процесс аутентификации по стандарту 802.1X. Суммарная длительность этих процессов и составляет длительность роуминга.

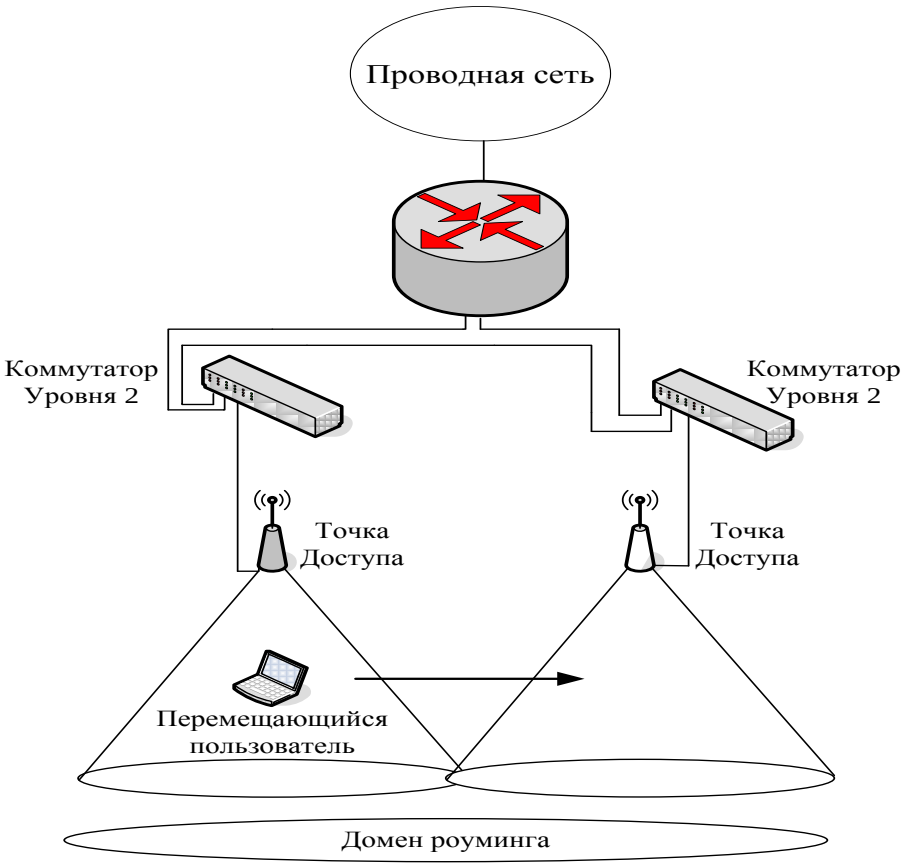



Рис. 38. Домен роуминга уровня два

**Определения направления движения абонента**

Механизм определяющий точку доступа, в направлении которой движется абонент не определен стандартом, каждый производитель решает эту задачу по своему. Можно выделить два варианта реализации. Предварительное обнаружение точки доступа. Обнаружение точки доступа во время перемещения. Каждый из двух вариантов может в свою очередь использовать один из следующих механизмов.

Активное сканирование. Клиент активно ищет точку доступа. Этот процесс обычно включает отправку клиентом зондирующих запросов по каждому из сконфигурированных на нем каналов и ожидание ответов от точек доступа на зондирующие запросы. Затем клиент определяет, какая из точек подходит для него лучше всего.

Пассивное сканирование. Клиент не передает фреймы, а просто прослушивает сигнальные фреймы, передаваемые по каждому из каналов. Клиент продолжает переходить с канала на канал через определенные промежутки времени, как при активном сканировании, но при этом не посылает зондирующие запросы.

Активное сканирование считается более совершенным механизмом поиска точки доступа, потому что при его использовании активно рассылаются запросы по всем частотным каналам. При этом требуется чтобы клиент оставался на одном и том же канале от 10 до 20 мс, ожидая ответ на зондирующий запрос.

При пассивном сканировании клиент медленнее проходит по каналам, чем при активном, так как прослушивает сигнальные фреймы, посылаемые точками доступа с предопределенной частотой (обычно 10 сигнальных фреймов в секунду). Такой клиент должен оставаться на канале дольше чтобы быть уверенным что получил сигнальные фреймы от максимального числа точек доступа для данного канала. Иногда пассивное сканирование не применимо, например, если администратор, в целях безопасности, отключил передачу в сигнальных фреймах имени SSID, клиент не может определить принадлежность точки к домену роуминга.

**Предварительное обнаружение точки доступа**

Предварительный роуминг — это функция, которая наделяет клиента способностью переходить к обслуживанию предварительно определенной точкой доступа после того, как клиент примет решение перемещаться. Этот процесс требует минимального общего времени роуминга, благодаря чему снижается воздействие роуминга на работу приложений. Однако предварительный роуминг не свободен от недостатков.

Для того чтобы клиент мог определить, к какой точке доступа нужно осуществлять подключение, он должен сканировать точки доступа **в** течение периода нормальной, без роуминга, работы. Когда клиент осуществляет сканирование, он должен переходить с канала на канал, чтобы или прослушивать другие точки доступа, или рассылать зондирующие запросы.

Такое изменение может потенциально привести к возникновению двух проблем для клиента, которые могут повлиять на работу приложений.

- Клиент не может получать данные от точки доступа, с которой он в данное время ассоциирован, пока он сканирует каналы (активно или пассивно). Если точка доступа посылает данные клиенту в то время, когда он сканирует каналы (предполагается, что клиент работает на другом канале, нежели точка доступа), клиент пропустит эти данные и потребуется повторная передач их точкой доступа.
- Приложение клиента может испытать воздействие снижения пропускной способности. Клиент не может передавать данные во время сканирования каналов (активного либо пассивного), поэтому некоторые приложения, выполняемые клиентом, могут ощутить снижение пропускной способности.

**Обнаружение точки доступа во время перемещения**

Другой вариант обнаружения точки доступа состоит в том, что ее поиск начинается уже после принятия решения о роуминге. Этот процесс похож на таковой, когда клиент осуществляет начальное включение, за исключением того что запрос на ассоциацию, посылаемый клиентом новой точке доступа, является в действительности фреймом запроса на реассоциацию.

Обнаружение точки доступа во время перемещения не приводит к повышению накладных расходов, характерному для предварительного обнаружения точки доступа (в то время, когда роуминг не осуществляется), потому что клиент не знает, с какой точкой доступа он должен реассоциироваться, но зато больше времени тратится на сам процесс роуминга.

**Принцип работы беспроводных коммутаторов**

В современной модели беспроводных сетей точки доступа работают как изолированные системы, обеспечивая такие функции стандарта 802.11, как шифрование данных и аутентификация пользователя. В архитектуре, базирующейся на технологии беспроводной коммутации, все интеллектуальные функции, которые выполнялись точками доступа, делегируются центральному беспроводному коммутатору, специально спроектированному для скоростной обработки пакетов. Таким образом, упрощаются задачи точек доступа, которые, по сути, выполняют роль трансиверов. Соединенные непосредственно с беспроводным коммутатором, они становятся как бы его удаленными портами доступа, направляющими пользовательский трафик коммутатору для обработки.

Функции безопасности, например шифрование, аутентификация и управление доступом, реализованы в беспроводном коммутаторе так, что они "отслеживают" пользователя, позволяя ему передвигаться между точками доступа, коммутаторами, виртуальными сетями и подсетями

без потери соединения.

Беспроводные коммутаторы обеспечивают также новый подход к автоматизации управления сетями Wi-Fi. Поскольку конфигурации точек доступа хранятся в коммутаторе и запитываются, как правило, также от него (Power over Ethernet -- PoE), то беспроводной коммутатор способен автоматически определить отказавшую точку доступа и дать команду соседним увеличить мощность и изменить настройки каналов, чтобы компенсировать неисправность. Когда вышедшее из строя устройство заменяется, коммутатор регистрирует это событие и конфигурирует новую точку доступа. Беспроводной коммутатор постоянно выполняет мониторинг эфира с целью определения подключенных пользователей и загрузки сети и в соответствии с маршрутами передвижения пользователей динамически настраивает полосу пропускания, управляет доступом, качеством обслуживания и другими параметрами.

**Архитектура**

Для выполнения расширенного набора функций стандартные уровни 2 и 3 (канальный и сетевой, соответственно) стека протоколов в системе, базированной на беспроводных коммутаторах, пополняются тремя уникальными блоками:

- - mobility management (управление мобильностью);
- - security management (управление безопасностью);
- - air traffic management (управление радиотрафиком).

Блок управления мобильностью объединяет протоколы Mobile IP и DHCP (Dynamic Host Configuration Protocol) с такими функциями блока управления безопасностью, как аутентификация пользователя и мобильный брандмауэр, политики управления доступом, мониторинг состояния беспроводных соединений. Статусы активных пользователей содержатся в глобальной базе данных (Active User Database), что позволяет непрерывно поставлять необходимые сервисы в процессе их перемещений с соблюдением соответствующих политик безопасности.

Уровень безопасности в дополнение к процедуре аутентификации и защите с помощью мобильного брандмауэра выполняет также VPN-шифрование для каждого порта, гарантируя конфиденциальность беспроводной передачи данных. Работая совместно с блоком управления радиотрафиком, он блокирует трафик от неисправных точек доступа.

Уровень управления радиотрафиком обеспечивает обнаружение сигнала в зоне покрытия. Он регулирует полосу пропускания и предоставляет необходимый класс обслуживания беспроводным клиентам. Все инструменты, включающие автоматическое обнаружение и калибровку точек доступа, беспроводной удаленный мониторинг (RMON) и захват пакетов данных, строятся вокруг уровня управления радиотрафиком.

**Алгоритм работы**

Беспроводной клиент получает доступ к сети, пытаясь подключиться для этого к точке доступа с наиболее сильным сигналом. Запрос на соединение может исходить от нового пользователя, регистрирующегося в сети, или от активного, изменившего свое местонахождение. Запрос на соединение направляется к беспроводному коммутатору, который пытается восстановить состояние клиента из БД активных пользователей. Если пославший запрос не был ранее активен, то коммутатор начнет процесс регистрации с помощью протокола 802.11x и базовых механизмов аутентификации, например RADIUS, Active Directory. Процесс аутентификации завершается добавлением нового клиента в БД со всей необходимой информацией о его статусе. Затем между пользователем и беспроводным коммутатором устанавливается VPN-сессия.

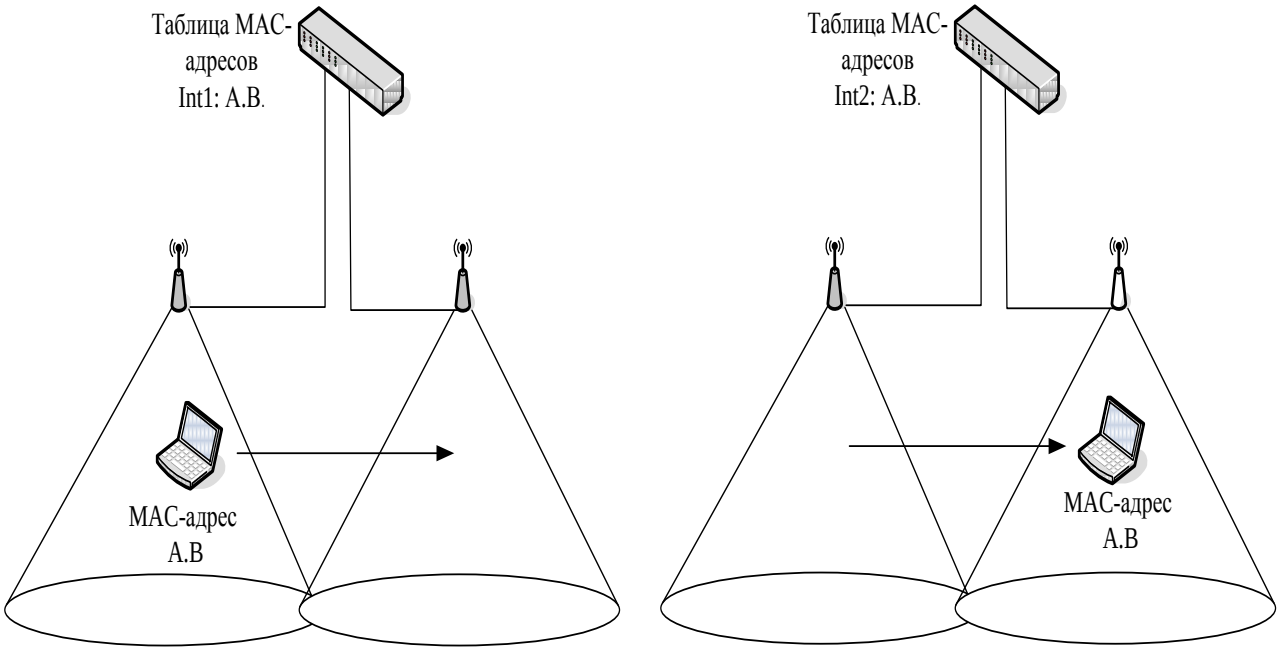



Рис. 39. Процесс роуминга с использованием беспроводного коммутатора

**Описание аппаратно-программного комплекса**

**Критерии оптимальности системы**

Для проектирования беспроводной сети, необходимо задаться некоторыми качественными требованиями к системе. Это позволит, в дальнейшем, определить технологию, наилучшим образом подходящую для решения поставленной задачи.

Итак, сформулируем и поясним основные требования, предъявляемые к выбираемому стандарту, а, следовательно, и к программно-аппаратному комплексу:

1. **Диапазон рабочих частот**. Данный параметр является особенно важным, поскольку

развертываемая беспроводная сеть передачи данных должна использовать аппаратуру, работающую в частотном диапазоне, разрешенном ГКРЧ РФ (Государственная комиссия по радиочастотам). На сегодняшний день в России, для внутриофисных систем передачи данных, разрешено использование полосы частот 2400 - 2483,5 МГц (решение № 04-03-04-003 от 6.12.2004г.). По этому применение стандарта 802.11a, расчитаного на работу в диапазоне 5 ГГц, не представляется возможным.

2. **Дальность действия радиосистемы.** Для обеспечения качественной связи мобильных устройств с сетью во всех требуемых участках помещения, радиосистема должна обеспечить достаточное для уверенного приема сигналов покрытие радиоизлучением. Стандарты 802.11b и 802.11g примерно одинаково подготовлены к работе в условиях многолучевого распространения сигналов. Покрытие любого помещения беспроводной сетью требует не столько инженерского расчета, сколько большого количества замеров.

3. **Скорость передачи информации.** Требования к скорости передачи данных беспроводной сети являются одними из основных. Они определяются требованиями к скорости доступа ко всем используемым сервисам и ресурсам сети (к базам данных, терминальным и файловым серверам). Из рассмотренных выше стандартов, оптимальным с точки зрения скорости, является стандарт передачи данных 802.11g, позволяющий передавать информацию со скорость до 54 Мбит/с.

4. **Безопасность и защищенность сети**. Для корпоративной сети, ключевой задачей является обеспечение требуемого уровня безопасности информации, циркулирующей в сети. Вопросы информационной и технической безопасности беспроводной сети становятся основополагающими при проектировании такой системы. Острота этой проблемы связана, прежде всего, с используемой средой передачи данных - радиоэфиром. Осуществить перехват информации в радиоэфире намного проще, чем в проводных сетях, - достаточно иметь комплект пользовательского оборудования и специализированный софт. Обеспечение безопасности радиосети, как и любой другой коммуникационной системы, сводится к решению трех проблем – защиты от подключения к сети нелегальных пользователей, предотвращения несанкционированного доступа к ресурсам сети зарегистрированных потребителей и гарантированной поддержки целостности и конфиденциальности данных, передаваемых по радиоканалам. Выбираемый стандарт, в равной степени, как и программно-аппаратный комплекс, должны обеспечить решение этих проблем. Для решения первых двух задач сегодня применяются процедуры аутентификации, авторизации и учета, для решения третьей проблемы применяются процедуры шифрования, проверки целостности пакетов и т.д.

- Аутентификация представляет собой процесс установления подлинности абонента.
- Авторизация обеспечивает контроль над доступом легальных пользователей к ресурсам сети. Успешно пройдя данную процедуру, потребитель получает только те права,

которые предоставлены ему администратором сети.

- Система учета фиксирует все события, происходящие в сети. Эта система регистрирует количество ресурсов, потребляемых каждым пользователем, время его работы в сети и т. д., что необходимо в первую очередь для управления сетью, в том числе для контроля доступа. Шифрация данных производится с помощью специальных алгоритмов, защищенных кодовыми ключами, с предусмотренными процедурами динамической смены ключей шифрования и т.п.

На основе сформулированных критериев можно выбрать подходящий стандарт. Сразу исключаем из рассмотрения стандарт 802.11a так как он использует не разрешенный в России частотный диапазон. Из двух оставшихся стандартов наиболее перспективным является 802.11g так как он обеспечивает большую скорость передачи, оборудование соответствующее этому стандарту поддерживает спецификацию WPA2, которая в свою очередь обеспечивает надежную защиту передаваемой по радиоканалу информации (используется алгоритм шифрования AES) и разнообразные методы надежной аутентификации.

**Описание и выбор сервера аутентификации**

Для предоставления доступа правомочных пользователей к проектируемой сети будет применяться RADIUS сервер. В его задачи входит проверка подлинности и авторизация пользователей, зашита сети от несанкционированного доступа, протоколирование событий. Работа сервера основана на протоколе RADIUS (Remote Authentication Dial-In User Service) — это отраслевой стандартный протокол, описанный в документах RFC 2865 «Remote Authentication Dial-in User Service (RADIUS)» и RFC 2866 «RADIUS Accounting». Протокол RADIUS используется для осуществления проверки подлинности, авторизации и учета. Клиент RADIUS (обычно сервер удаленного доступа, VPN-сервер или точка доступа к беспроводной сети) посылает учетные данные пользователя и параметры подключения в форме сообщения RADIUS на сервер RADIUS. Сервер RADIUS проверяет подлинность и авторизует запрос клиента RADIUS, а затем посылает обратно ответное сообщение RADIUS. Клиенты RADIUS посылают на серверы RADIUS также сообщения учета RADIUS. Кроме того стандарт RADIUS поддерживает использование прокси-серверов RADIUS. Прокси-сервер RADIUS — это компьютер, пересылающий сообщения RADIUS между компьютерами, поддерживающими протокол RADIUS.

Для передачи сообщений RADIUS используется протокол UDP (User Datagram Protocol). Для сообщений проверки подлинности RADIUS используется UDP-порт 1812, а для сообщений учета RADIUS — UDP-порт 1813. Некоторые серверы доступа к сети могут использовать UDP-порт 1645 для сообщений проверки подлинности RADIUS и UDP-порт 1646 для сообщений учета

RADIUS. В документах RFC 2865 и RFC 2866 определены следующие типы сообщений RADIUS.

- Access-Request (запрос доступа) Посылается клиентом RADIUS для запроса проверки подлинности и авторизации попытки подключения. Access-Accept (предоставление доступа) Посылается сервером RADIUS в ответ на сообщение запроса доступа. Это сообщение информирует клиента RADIUS о том, что для попытки подключения клиента была выполнена проверка подлинности и авторизация. Access-Reject (запрещение доступа) Посылается сервером RADIUS в ответ на сообщение запроса доступа. Это сообщение информирует клиента RADIUS о том, что попытка подключения клиента была отклонена. Сервер RADIUS посылает это сообщение в том случае, если недействительны учетные данные или не авторизована попытка подключения.
- Access-Challenge (запрос уточнения) Посылается сервером RADIUS в ответ на сообщение запроса доступа. Это сообщение является запросом дополнительной информации клиента RADIUS, который требует ответа. Accounting-Request (запрос учета) Посылается клиентом RADIUS для указания учетных сведений о разрешенном подключении. Accounting-Response (ответ учета) Посылается сервером RADIUS в ответ на сообщение запроса учета. Это сообщение подтверждает успешное получение и обработку сообщения запроса учета.

Сообщение RADIUS состоит только из заголовка RADIUS или из заголовка RADIUS и одного или нескольких атрибутов RADIUS. Каждый атрибут RADIUS содержит определенные сведения о попытке подключения. Например, имеются атрибуты RADIUS для имени пользователя, пароля пользователя, типа услуг, запрашиваемых пользователем, и IP-адреса сервера доступа. Атрибуты RADIUS используются для передачи информации между клиентами RADIUS, прокси-серверами RADIUS и серверами RADIUS. Например, список атрибутов в сообщении запроса доступа включает информацию об учетных данных пользователя и параметрах попытки подключения. В отличие от этого сообщение предоставления доступа содержит информацию о типе подключения, которое может быть осуществлено, ограничениях подключения и имеющихся особых атрибутах вендора (Vendor-Specific Attribute, VSA).

На сегодняшний день существует большое множество RADIUS серверов, реализованных как программно, так и аппаратно. Большинство из них – это коммерческие продукты. Для выбора более подходящего продукта сформулирую два основных критерия. Продукт должен иметь сертификат соответствия требованиям Гостехкомиссии России, в области зашиты информации от НСД. Продукт должен иметь как можно меньшую стоимостью, при этом обладать достаточной функциональностью.

Использование аппаратных RADIUS серверов для небольших сетей не оправдано из-за их высокой стоимости. Свободно распространяемые продукты не имеют сертификатов соответствия, их использование может быть не безопасным (программа может содержать вредоносный код, не

гарантируется конфиденциальность и криптографическая защита информации с которой взаимодействует программа). Подходящим вариантом является использование включенного в состав Windows server 2003 Enterprise Edition RADIUS – сервера (служба IAS). Операционная система имеет сертификат соответствия (№112-0938 выдан 23.10.06 центром безопасности связи ФСБ России) и может применятся в составе автоматизированных информационных систем, работающих с информацией не содержащей государственную тайну. Для различных решений могут быть созданы различные конфигурации службы Internet Authentication Service (IAS):

- - Беспроводной доступ.
- - Удаленный доступ организаций через коммутируемое подключение или виртуальную частную сеть (VPN).
- - Удаленный коммутируемый или беспроводной доступ через внешних поставщиков.
- - Доступ к Интернету.
- - Доступ с проверкой подлинности к ресурсам экстрасети для деловых партнеров

Я буду использовать службу IAS для авторизации клиентов беспроводной сети. Основные возможности службы. Поддерживаются разнообразные методы проверки подлинности. Поддерживаются протоколы PPP проверки подлинности с паролем, такие как протокол PAP (Password Authentication Protocol), протокол CHAP (Challenge Handshake Authentication Protocol), протокол MS-CHAP (Microsoft Challenge Handshake Authentication Protocol) и MS-CHAP версии 2 (MS-CHAP v2). Протокол EAP Инфраструктура, основанная на стандартах Интернета и разрешающая дополнительные произвольные методы проверки подлинности, такие как смарт-карты, сертификаты, одноразовые пароли и генераторы кода доступа. Способ проверки подлинности, в котором применяется инфраструктура EAP, является способом типа EAP. В службу IAS включена поддержка способов EAP-Message Digest 5 (MD5) и EAP-Transport Level Security (EAP-TLS).

1. Поддерживаются различные способы авторизации. Протокол DNIS (Dialed Number Identification Service). Авторизация попытки подключения на основе набираемого номера. Служба DNIS показывает набранный номер получателю вызова. Эта возможность предоставляется большинством обычных телефонных компаний. Протокол ANI/CLI (Automatic Number Identification/Calling Line Identification). Авторизация попытки подключения на основе номера телефона, с которого выполняется вызов. Служба ANI/CLI показывает получателю вызова номер телефона, с которого выполняется вызов. Эта возможность предоставляется большинством обычных телефонных компаний. Авторизация для гостей. Учетная запись гостя применяется для идентификации пользователя при установлении подключения без учетных данных пользователя (имени пользователя и пароля).

1. Неоднородные серверы доступа. Служба IAS поддерживает серверы доступа, реализованные на основе документов RADIUS RFC 2865 и 2866. Помимо серверов удаленного доступа служба IAS поддерживает следующие возможности. Точки доступа к беспроводной сети. Применение политик удаленного доступа и параметров порта Wireless-IEEE 802.11 позволяет использовать службу IAS в качестве сервера RADIUS для точек доступа к беспроводной сети, в которых проверка подлинности и авторизация для беспроводных узлов производится с помощью RADIUS.

Коммутаторы с проверкой подлинности. Применение политик удаленного доступа и параметров порта Ethernet позволяет использовать службу IAS в качестве сервера RADIUS для коммутаторов сети Ethernet, в которых проверка подлинности и авторизация производится с помощью RADIUS. Интеграция со службой маршрутизации и удаленного доступа. Службы IAS и маршрутизации и удаленного доступа используют общие политики удаленного доступа и возможности ведения файла журнала. Такая интеграция обеспечивает согласованную работу служб IAS и маршрутизации и удаленного доступа. Это позволяет развертывать службу маршрутизации и удаленного доступа на небольших узлах, не предъявляя требований к наличию отдельного централизованного IAS-сервера. Обеспечивается также возможность масштабирования модели централизованного управления удаленным доступом, когда в организации появятся несколько серверов маршрутизации и удаленного доступа. Служба IAS совместно с серверами маршрутизации и удаленного доступа используют одну точку администрирования для удаленного доступа к сети через внешнего поставщика, вызова по требованию и доступа через VPN. Политики службы IAS большого центрального сайта можно экспортировать на независимый сервер маршрутизации и удаленного доступа малого сайта.

Прокси-сервер RADIUS. Служба IAS позволяет пересылать входящие запросы RADIUS на другие RADIUS-серверы для проверки подлинности и авторизации или учета. Действуя в качестве прокси-сервера RADIUS, служба IAS может быть применена всякий раз когда возникает необходимость маршрутизации запроса RADIUS на другой RADIUS-сервер. Служба IAS позволяет пересылать запросы, основанные на имени пользователя, получать доступ к IP-адресу сервера, идентификатору сервера и другим параметр.

Обеспечение удаленного и беспроводного доступа в сеть через внешнего поставщика. При удаленном доступе через внешнего поставщика заключается договор между организацией (заказчиком) и поставщиком услуг Интернета (ISP). Поставщик услуг Интернета обеспечивает подключение сотрудников организации к своей сети перед установлением туннеля VPN в частную сеть организации. Когда сотрудник подключается к серверу NAS поставщика услуг Интернета, на сервер IAS, расположенный в организации, пересылаются записи проверки подлинности и использования. Сервер IAS позволяет организации управлять проверкой

подлинности пользователей, отслеживать использование сети поставщика услуг Интернета и управлять доступом сотрудников к ней.Преимущество доступа через внешнего поставщика заключается в потенциальной экономии. Использование маршрутизаторов, серверов сетевого доступа и доступа к каналам глобальной сети, предоставленных поставщиком услуг, вместо приобретения собственных, позволяет получить значительную экономию на затратах, связанных с оборудованием (инфраструктурой). Международные подключения через поставщика услуг Интернета позволяют существенно сократить счета организации за междугородние телефонные звонки. Благодаря перекладыванию на поставщика забот по поддержке сети исключаются расходы на ее администрирование.Кроме того, через внешнего поставщика можно осуществлять и беспроводной доступ. Поставщик может обеспечить беспроводной доступ с удаленной территории и, используя имя пользователя, пересылать запрос на подключение для проверки подлинности и авторизации на тот RADIUS-сервер, который находится под управлением организации. Хорошим примером служит доступ к Интернету в аэропортах.

Централизованная проверка подлинности и авторизация пользователей. При проверке подлинности запроса на подключение служба IAS сверяет учетные данные подключения с учетными записями пользователей в локальном диспетчере учетных записей безопасности (SAM) домена Microsoft® Windows NT® Server 4.0 или домена Active Directory®. Для домена Active Directory в службе IAS имеется поддержка использования основных имен пользователей (User Principal Name, UPN) Active Directory и универсальных групп. Для авторизации запроса на подключение в службе IAS применяются параметры входящих звонков для учетной записи пользователя, соответствующие как учетным данным подключения, так и политикам удаленного доступа. Управление разрешением удаленного доступа осуществляется относительно просто, однако такой подход не обеспечивает масштабирования по мере роста организации. Политики удаленного доступа обеспечивают более мощное и гибкое управление разрешениями удаленного доступа. Авторизация доступа в сеть может производиться на основе различных параметров, включая описанные далее. (Вхождение учетной записи пользователя в группу, Время суток или день недели, Тип устройства, с помощью которого производится подключение (например беспроводное устройство, коммутатор Ethernet, модем или туннель VPN, Номер вызываемого телефона, Сервер доступа, с которого был получен запрос, Интервал времени бездействия, Максимальная продолжительность одного сеанса, Выбор применяемых способов проверки подлинности, Применение шифрования и степень его стойкости).

Централизованное администрирование всех серверов доступа организации. Поддержка стандарта RADIUS позволяет службе IAS управлять параметрами подключения для любого сервера NAS, использующего стандарт RADIUS. Стандарт RADIUS также позволяет отдельным поставщикам удаленного доступа создавать собственные расширения, называемые

особыми атрибутами вендора (Vendor-Specific Attribute, VSA). Служба IAS объединяет расширения, предоставленные несколькими поставщиками, в один словарь. Дополнительные атрибуты VSA могут быть внесены в профиль отдельных политик удаленного доступа.

Централизованный аудит и учет использования. Поддержка стандарта RADIUS позволяет службе IAS централизованно собирать записи об использовании (записи учета), отправленные всеми серверами доступа. Служба IAS хранит сведения аудита (например, успехи проверки подлинности и отказы) и использования (например, подключения и отключения) в файлах журналов. Служба IAS поддерживает формат файла журнала, допускающий непосредственный импорт в базу данных. Последующий анализ данных может быть выполнен с помощью любого обычного пакета анализа.

**IAS в качестве RADIUS-сервера**

В данной работе служба Internet Authentication Service будет использоваться в качестве RADIUS – сервера. Сервер RADIUS будет выполнять проверки подлинности, авторизацию и учет клиентов RADIUS. В моем случае клиентом радиус клиентами RADIUS будут точки доступа. Для авторизации подключения IAS-сервер применяет параметры входящих звонков учетной записи пользователя и политику удаленного доступа, запросы учета будут сохранятся для анализа в локальном файле журнала. На рисунке 4.39 показан IAS-сервер в качестве сервера RADIUS для клиентов беспроводного доступа. Сервер IAS использует домен Active Directory для проверки подлинности учетных данных пользователя в поступающих сообщениях запросов доступа RADIUS.

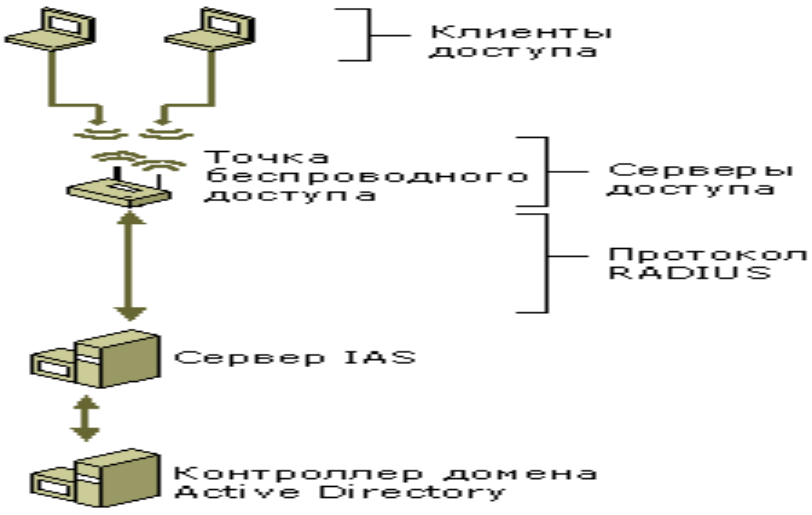



Рис. 39. Использование IAS в качестве RADIUS-сервера

Если IAS-сервер используется как сервер RADIUS, сообщения RADIUS обеспечивают проверку подлинности, авторизацию и учет подключений к сети следующим образом. Серверы доступа, например серверы удаленного доступа к сети, VPN-серверы и точки доступа к

беспроводной сети, получают запросы подключения от клиентов доступа.

1. Сервер доступа, настроенный для использования RADIUS в качестве протокола проверки подлинности, авторизации и учета, создает сообщение запроса доступа и посылает его на IAS-сервер. Сервер IAS оценивает сообщение запроса доступа. При необходимости IAS-сервер посылает запрос уточнения на сервер доступа. Сервер доступа обрабатывает запрос уточнения и посылает обновленный запрос доступа на IAS-сервер.

2. Производится проверка учетных данных пользователя, а также получение параметров входящих звонков учетной записи пользователя через безопасное соединение с контроллером домена. Попытка подключения авторизуется с учетом параметров входящих звонков учетной записи пользователя и политики удаленного доступа. Если для попытки подключения проверка подлинности и авторизация выполнена, IAS-сервер посылает сообщение предоставления доступа на сервер доступа. Если попытка подключения не прошла проверку подлинности или авторизацию, IAS-сервер посылает сообщение запрещения доступа на сервер доступа. Сервер доступа завершает процесс подключения с клиентом доступа и посылает сообщение запроса учета на IAS-сервер, на котором сообщение записывается в журнал. Сервер IAS посылает ответ учета на сервер доступа

**Выбор оборудования для проектируемой сети**

Проектируемая сеть строится на основе беспроводного коммутатора Netgear ProSafe Smart WFS709TP. Его описание приведено в таблице 4.12. Коммутатор способен работать с точками доступа следующих моделей: NETGEAR ProSafe 802.11a/g Dual Band Light Wireless Access Point (WAGL102); NETGEAR ProSafe 802.11g Light Wireless Access Point (WGL102); и NETGEAR WG102 и WAG102. Модели WG102 и WGL102 имеют одинаковые физические характеристики и отличаются лишь программным обеспечением функционирующим на них. Модели WAGL102 и WAG102 также имеют одинаковые физические характеристики. Точки WG102 и WAG102 выпущены раньше беспроводного коммутатора и в своей первоначальной конфигурации не могут взаимодействовать с беспроводным коммутатором, однако производители выпустили свежую прошивку. Ее можно свободно скачать с сайта компании NETGEAR. Выбор будем производить из двух моделей WG102 и WAG102, более новые модели не рассматриваются так как при одинаковых физических характеристиках с более старыми точками их цена превышает последние более чем на 1000 рублей. Характеристики точек приведены в таблицах 4.13 и 4.14 соответственно. Из ходя из приведенных в таблицах данных было решено что для решаемой задачи наиболее подходящей является модель NETGEAR WG102. WG102 поддерживает технологию Power over Ethernet (POE), следовательно отпадает необходимость в прокладке электрической сети в места установки точек. Еще один не мало важный плюс этой технологии

является возможность управлять питанием включать/выключать точки доступа с помощью беспроводного коммутатора (если точка доступа по каким то причинам повиснет администратор сможет перезагрузить ее не вставая с рабочего мета). Точки доступа WG102 полностью соответствую стандарту 802.11g.

### 3. Порядок выполнения работы

#### Настройка точек доступа

Для того чтобы перейти к настройке точки доступа необходимо подключить ее к ПК по средствам Ethernet и подключится к ней по используя telnet или WEB – интерфейс. Я буду использовать WEB – интерфейс, он более прост и нагляден. По умолчанию точки доступа D-Link Dir 300, имеют IP – адрес 192.168.0.1, имя пользователя “admin” и пароль “password”.

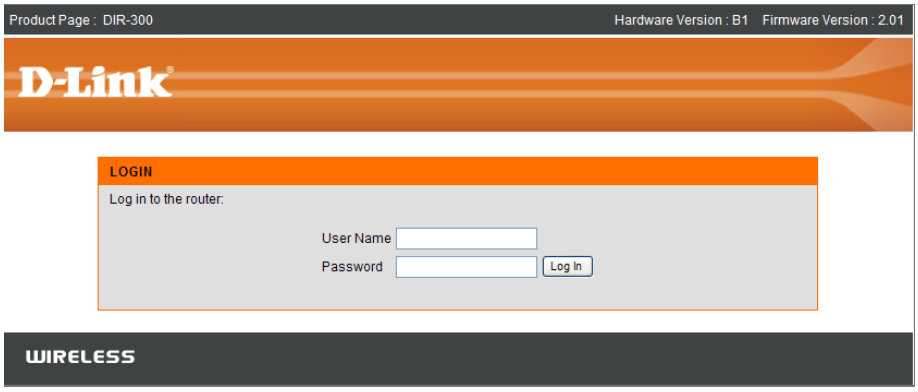



Рис. 40. Начало настройки маршрутизатора

Необходимо настроить точку доступа. Для этого заходим на закладку Setup – Internet Setup.

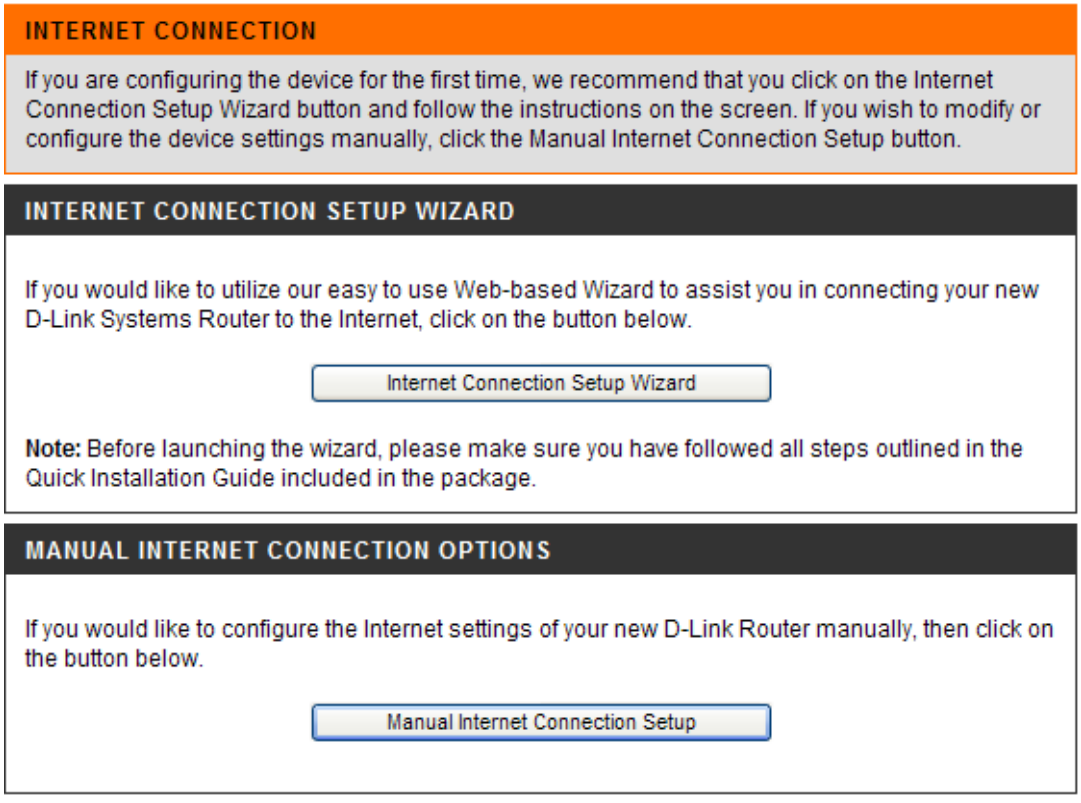



Рис. 41. Настройка Internet.

Для настройки Internet необходимо выбрать одну из предлагаемых функций: Internet connection Setup Wizard (автоматическая настройка) или Manual Internet Connection Setup (ручная настройка). Будем использовать Internet connection Setup Wizard.

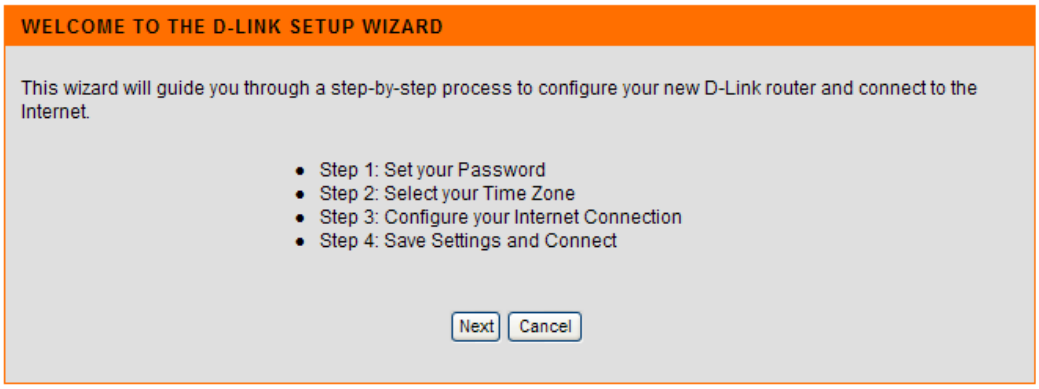



Рис. 42. Первый шаг

Необходимо будет пройти 4 шага настройки. Т.к. Интерфейс настройки маршрутизатора достаточно понятен, то настройка маршрутизатора не представляет особых затруднений.


Рис. 43. Второй шаг

Необходимо ввести пароль.

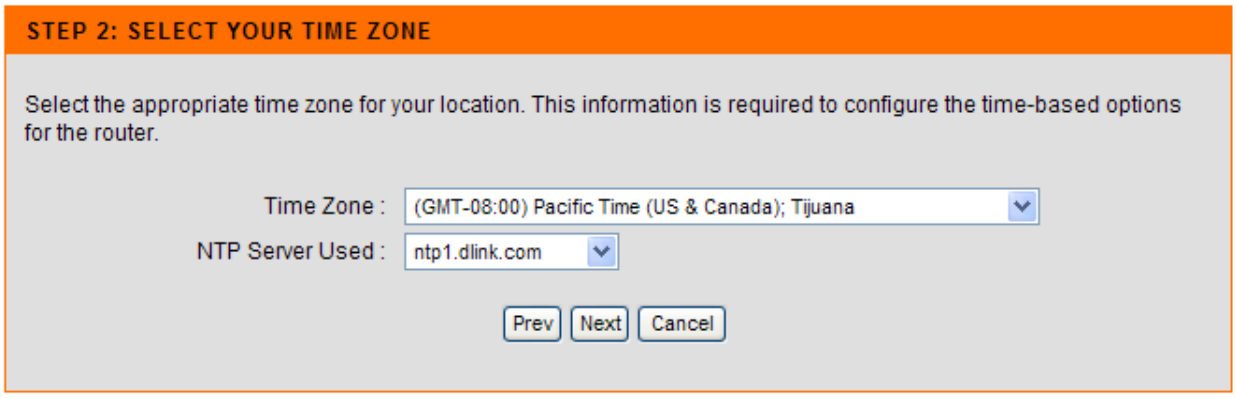



Рис. 44. Третий шаг

Затем выбрать соответствующий часовой пояс.

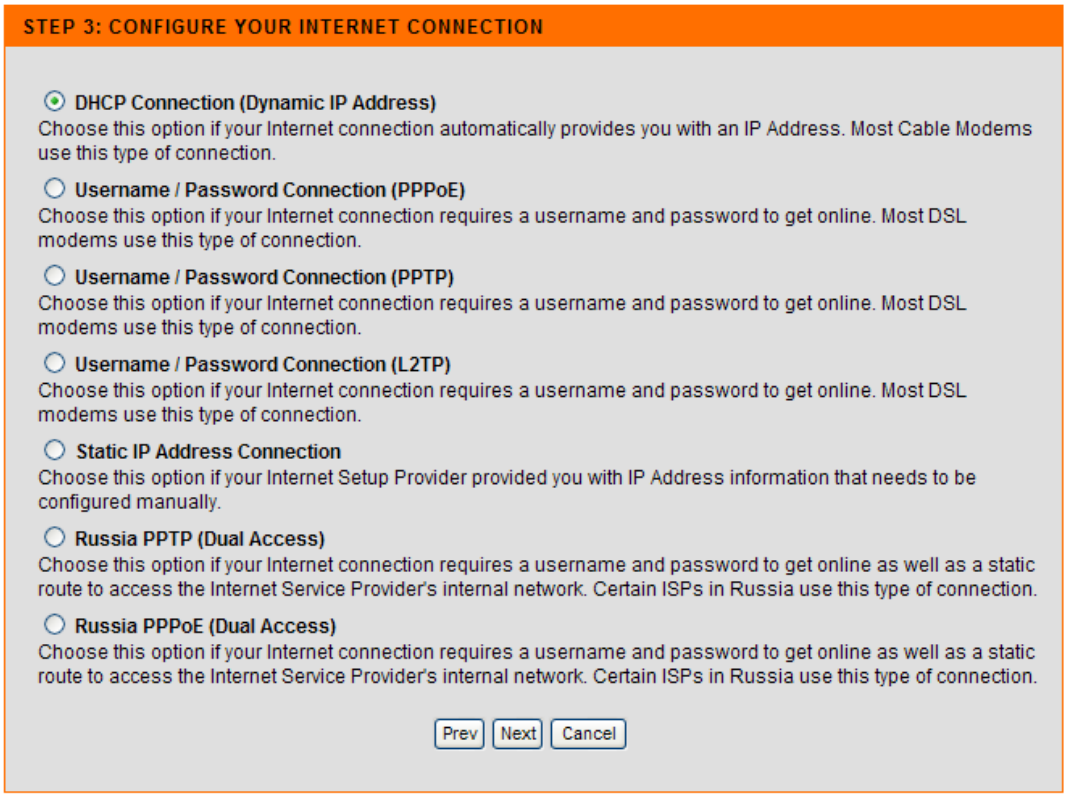



Рис. 45. Четвертый шаг

Последним этапом настройки является выбор интернет соединения. В нашем случает это DHCP Connection (Dynamic IP Address).

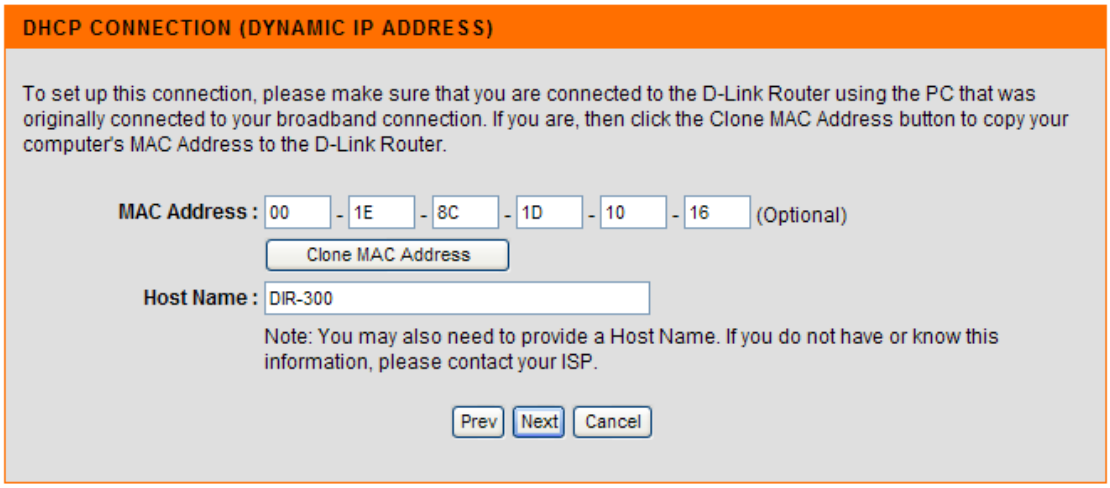



Рис. 46. Проверка MAC адреса

Далее будет предложено проверить мак адрес соединения и ввести Host Name.

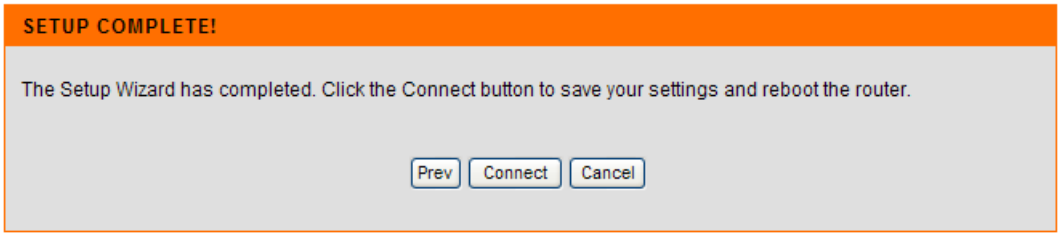



Рис. 47. Завершение настройки

Поле нажатия Connect будет установлено соединения.

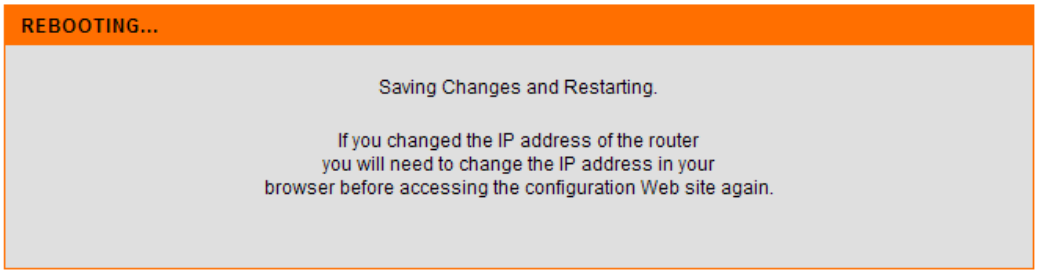



Рис. 48. Сохранение и перезапуск маршрутизатора

Далее необходимо сохранить изменения и перезапустить точку доступа.

Далее необходимо настроить беспроводное соединение. Для этого надо зайти на вкладку Setup – Wireless Setup.

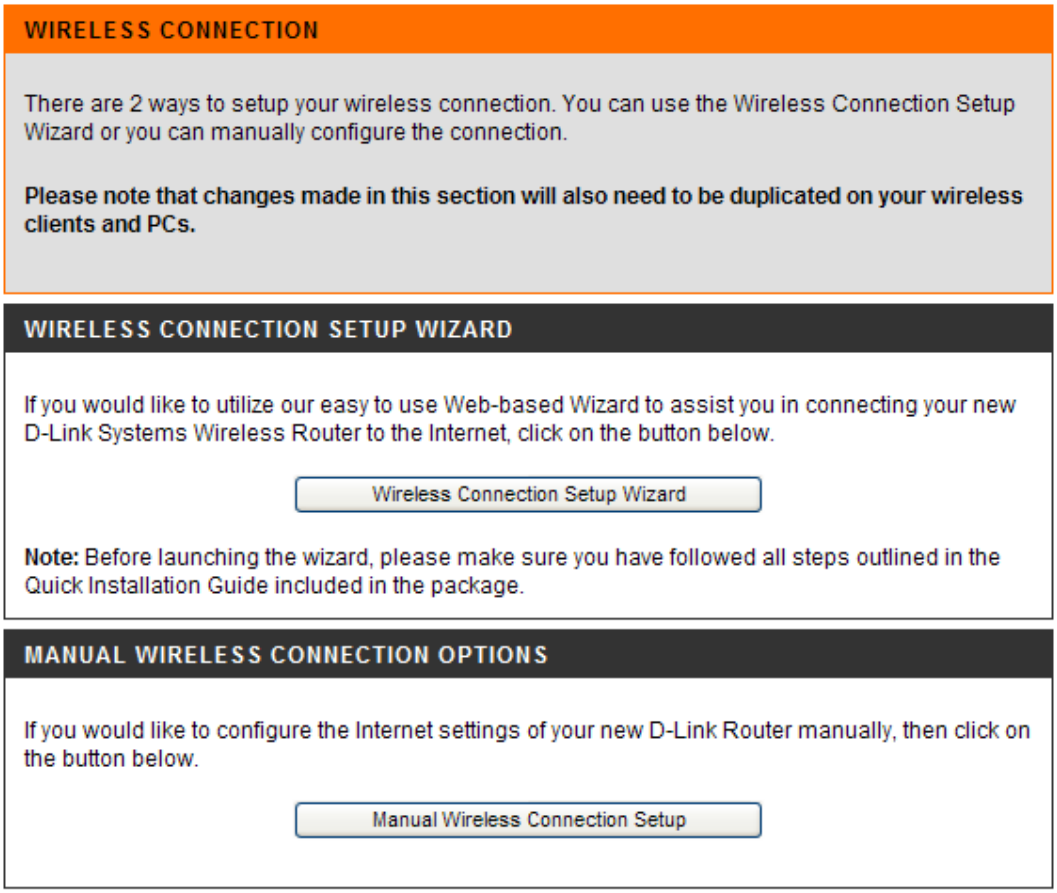



Рис. 49. Настройка беспроводной сети

Здесь также предлагается два типа настройки Internet connection Setup Wizard или Manual Internet Connection Setup. В этот раз выберем Manual Internet Connection Setup .

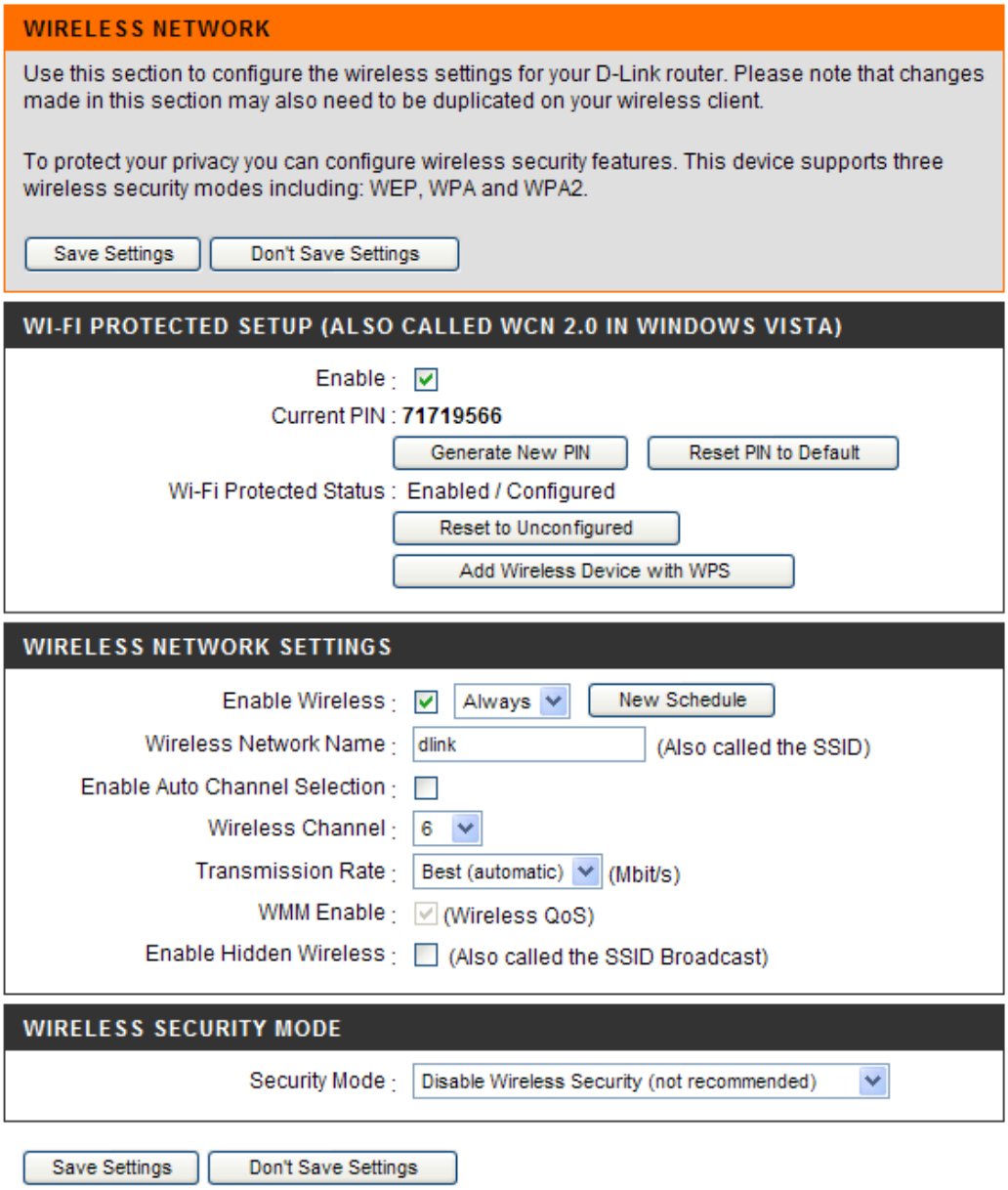



Рис. 50. Вкладка настроек

В строке Wireless Network Name вводим имя создаваемой беспроводной сети. В строке Wireless Channel предлагается выбрать канал, используемый для передачи данных. По умолчания выбран 6 канал, но при необходимости можно выбрать любой из предложенных (если только на таком этом канале не работает другая точка доступа).

В пункте Wireless security mode выбирается метод шифрования данных. По умолчанию эта функция отключена. В ходе проведения лабораторной работы придется меня метод шифрования. Это делается следующим образом.

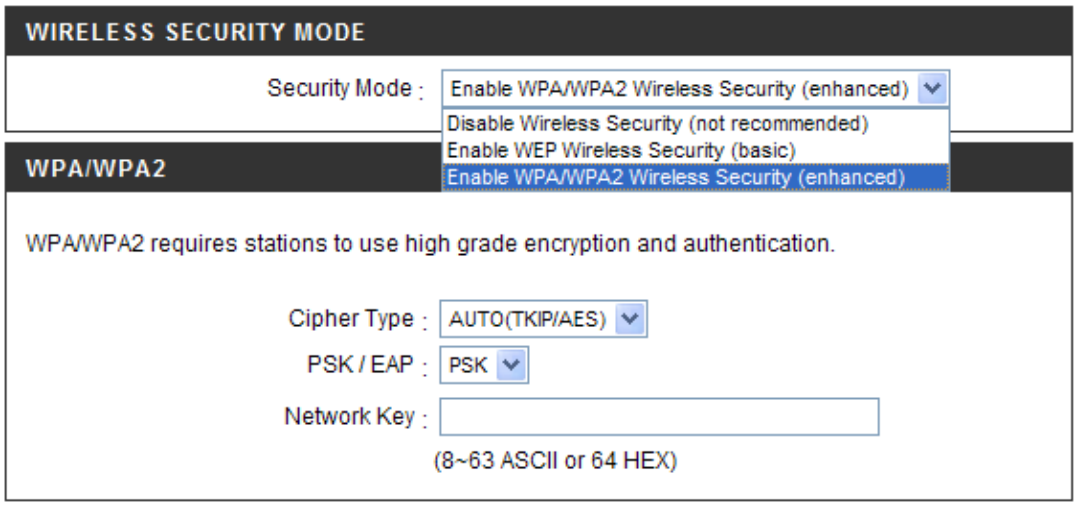



Рис. 51. Настройка режима шифрования

Из выпадающего списка выбирается необходимый метод шифрования. Затем в строке Network Key вводится ключ шифрования. При установки соединения с адаптером вводится этот ключ.

**Проведения испытаний**

**Оценка производительности точек доступа**

Данный тест направлен на оценку производительности используемых в работе точек доступа D-link DIR-300. Под производительностью в данном случае понимается скорость передачи между LAN и WAN (внутренним и внешним) портами устройства, т.е. на сколько быстро микропроцессор точки доступа может обрабатывать поток данных, проходящий сквозь него.

Не смотря на то, что все выпускаемое оборудование соответствует стандарту 802.11g, реальная пропускная способность при работе точки доступа с различным клиентским оборудованием оказывается различной. Проектируемая сеть будет работать с большим числом клиентских адаптеров, выпушенных различными производителями, по этому целесообразно провести тестирование только точек доступа. Именно точки доступа являются связующим звеном между проводной и беспроводной сетью, и по этому, даже если клиентское оборудование может обеспечить большую скорость передачи, максимальная скорость передачи будет ограничена именно возможностями точки доступа.

Для тестирования будет применятся программный пакет NetIQ Chariot. Пакет представляет собой консоль управления (которая может находиться на любом компьютере) и набор сенсоров. Последние являются программами, которые устанавливаются на хостах-генераторах и осуществляют генерацию и мониторинг трафика. Сенсоры существуют под множество ОС, из которых нас интересует Windows XP SP3. Схема тестирования приведена на рисунке 6.13. В помещении, где проводится тестирование, нет оборудования работающего в диапазоне 2.4 ГГц.

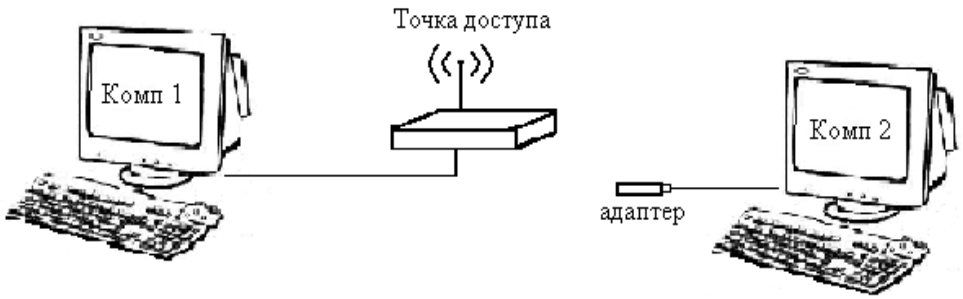



Рис. 52. Тестовый стенд для определения максимальной пропускной способности.

**Методика тестирования**

Осуществляется передача трафика, сгенерированного программой NetIQ Chariot, между узлами Комп1 и Комп2. В ходе тестирования направление передачи и количество потоков трафика будет меняться:

1. Передача трафика от узла Comp1 к узлу Comp2 с длинной пакета:
   a. Пакеты максимального размера (байт);
   b. Пакеты размера 512 байт;
   c. Пакеты размера 64 байта;

Проведем настройку программы NetIQ Chariot. На рис. 53 представлен интерфейс программы.

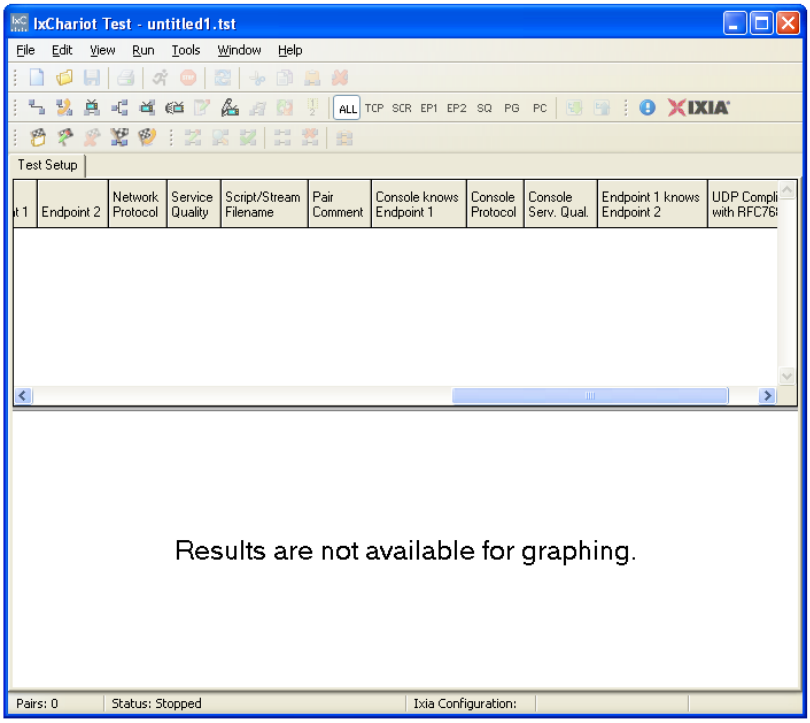



Рис. 53. Интерфейс IXChariot

Перед началом измерений необходимо убедиться , что на компьютере запущена служба «Ixia Perfomance Endpoint» (Пуск -> Настройка -> Панель Управления -> Администрирование -> Службы). Затем зайдите в программу IxChariot и открыть окно Add an Endpoint Pair.

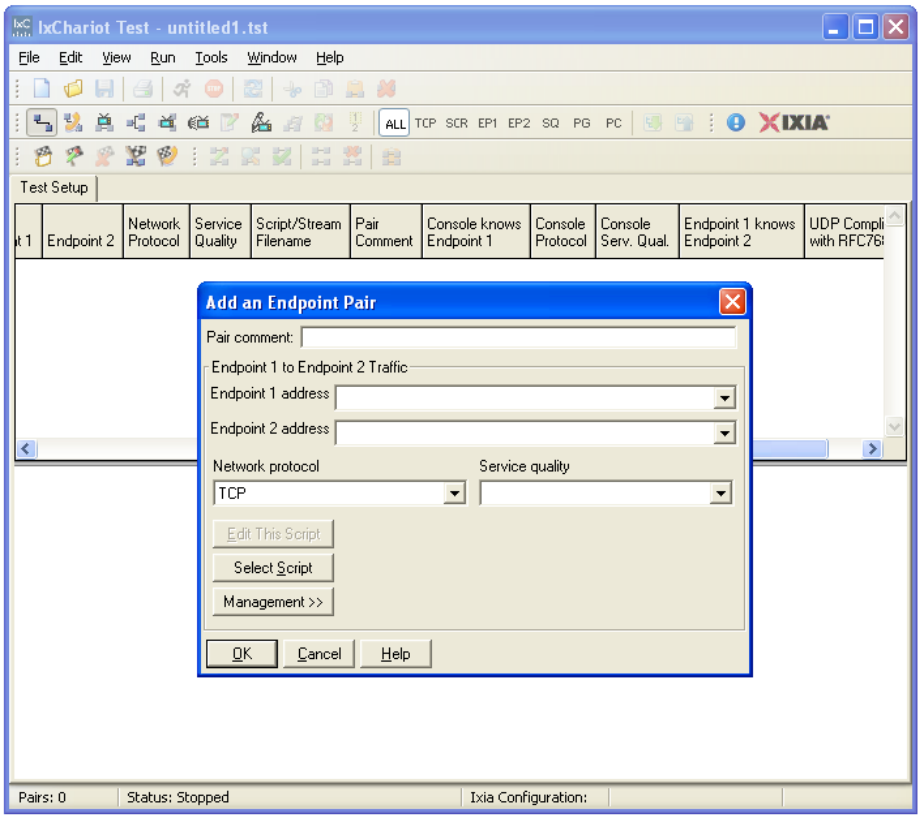



Рис. 54. Окно Add an Endpoint Pair

В строке Endpoint 1 вводим IP адрес копьютера с которого буду проводиться измерения, в строке Endpoint 2 вводится IP адрес Комп 2.

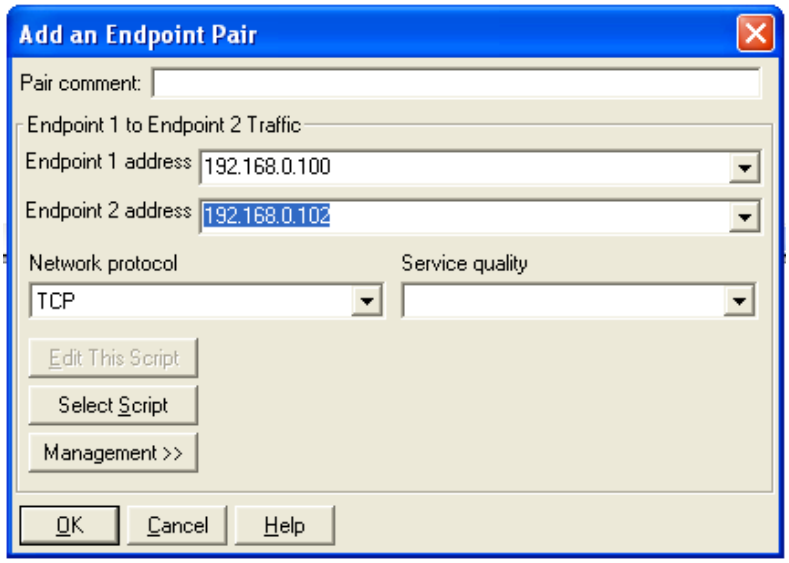



Рис. 55. – Ввод IP адресов тестируемых устройств

Далее выбираем Select Script и выбираем throughput.

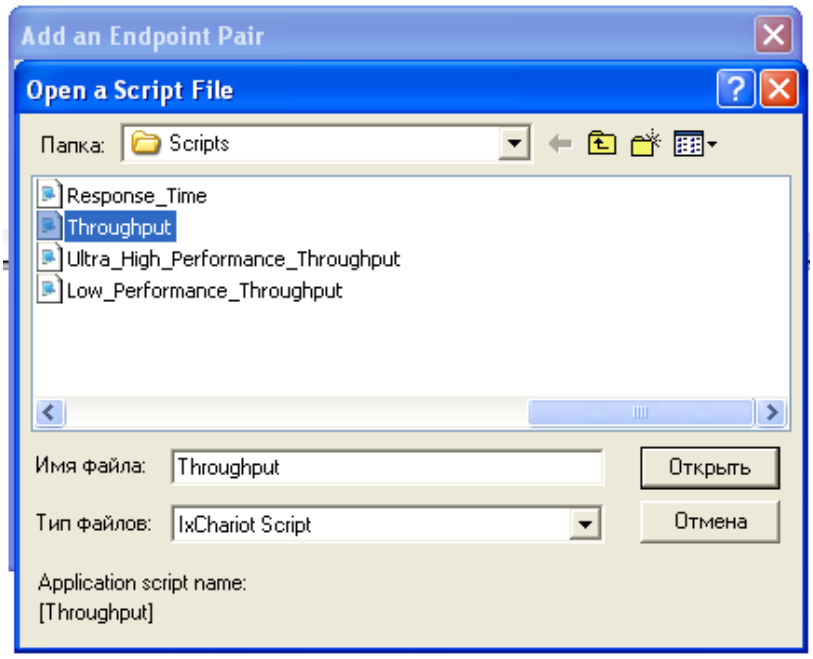



Рис. 56. Выбор скрипта

Произведем настройку скрипта для проведения измерений с различной длиной пакета. Для этого в поле size_file указываем нужное число.

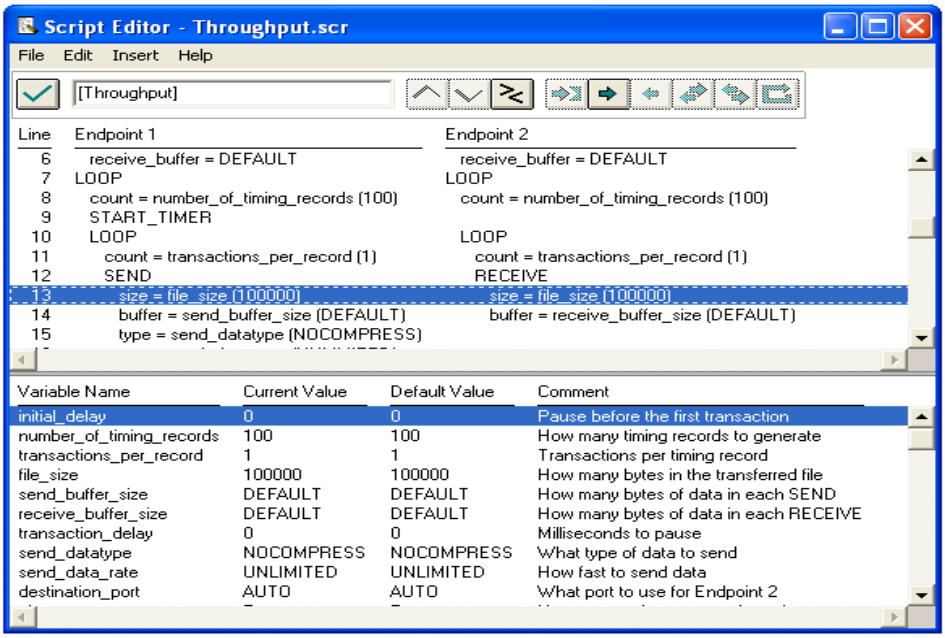



Рис. 57. Настройка скрипта

Результаты измерений.

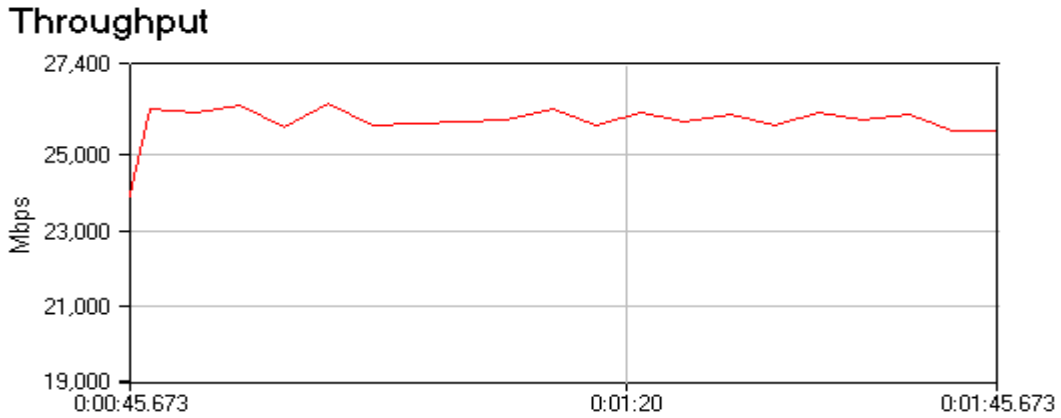



Рис. 58. Размер пакета 1500 байт.


Рис. 59. Размер пакета 512 байт.

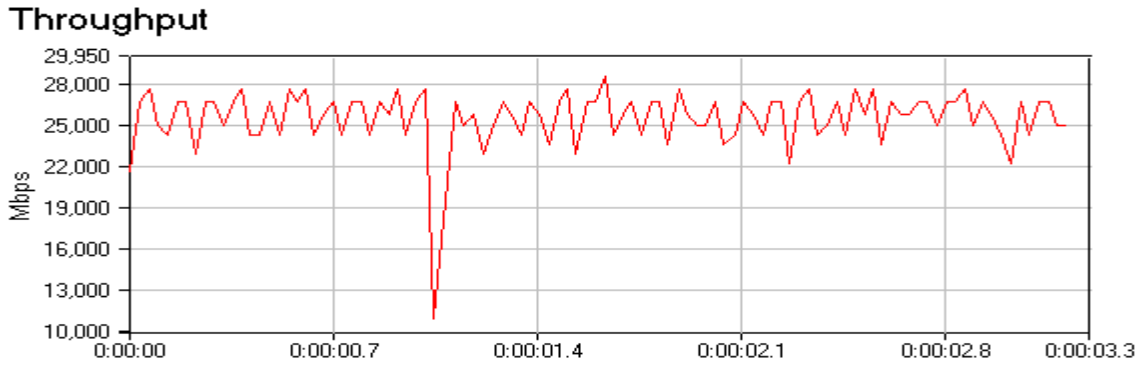



Рис. 60. Размер пакета 64 байта.

При проведении всех тестов измерялось среднее время отклика, для этого в течении всего времени тестирования с помощью команды ping от к comp1 к comp2 посылались запросы. Среднее время откликов для каждого из проведенных тестов приведено в таблице 9.

Таблица 9. Результаты измерения времени отклика

| № теста | Время отклика, мс |
|---|---|
| 1 | 17 |
| 2 | 16 |
| 3 | 9 |

**Оценка накладных расходов связанных с шифрованием**

Шифрование как известно, требует значительных вычислений, в результате падает пропускная способность и увеличивается задержки при передаче пакетов, данный тест будет направлен на оценку пропускной способности точки доступа при использовании различных алгоритмов шифрования (WEP, TKIP и AES).

**Методика тестирования**

Как и в предыдущем случае между конечными точками будет пересылаться сгенерированный программой NetIQ Chariot трафик, будет измеряться скорость передачи и среднее время отклика. При проведении тестирования будем использовать тестовый стенд изображенный на рисунке 6.13. Чтобы провести сравнительный анализ влияния шифрования на пропускную способность как и в предыдущем тесте будем пересылать пакеты с размером 1500 и  используя для генерации скрипт throughput.scr. Измерение скорости производится в течении 2 минут.

**Настройка оборудования**

Оставляем все настройки сделанные для проведения первого теста. Для настройки точки доступа заходим на вкладку Wireless Setup и изменяем метод шифрования.

Без шифрования

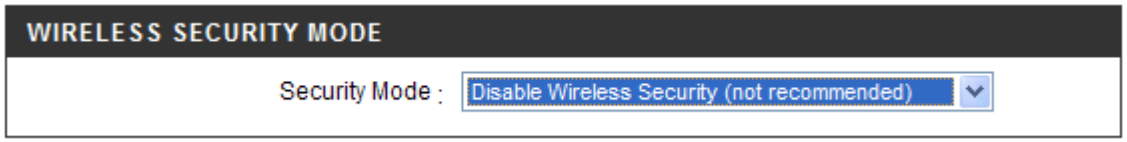



Рис. 61. Настройка маршрутизатора для проведения измерений

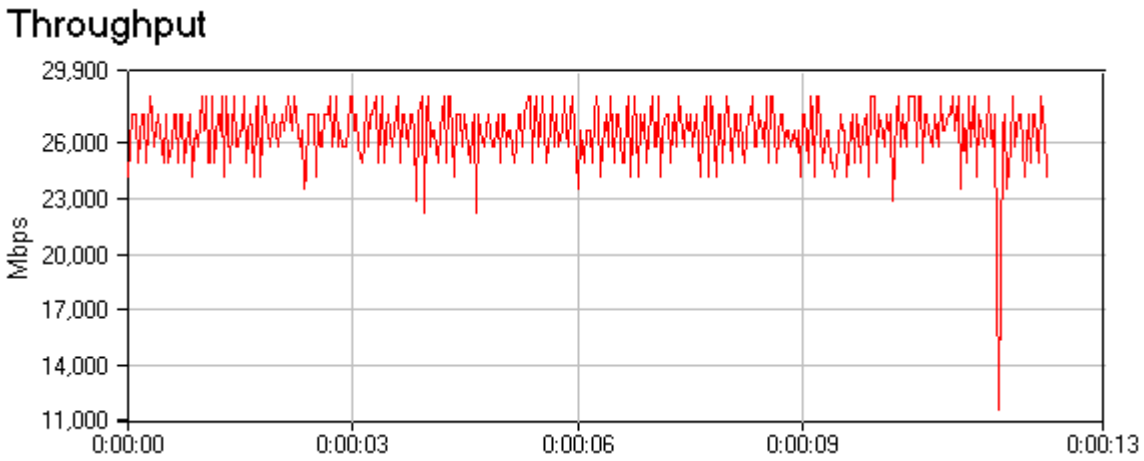



Рис. 62. Результаты измерений в режиме без шифрования

WPA/WPA 2 PSK

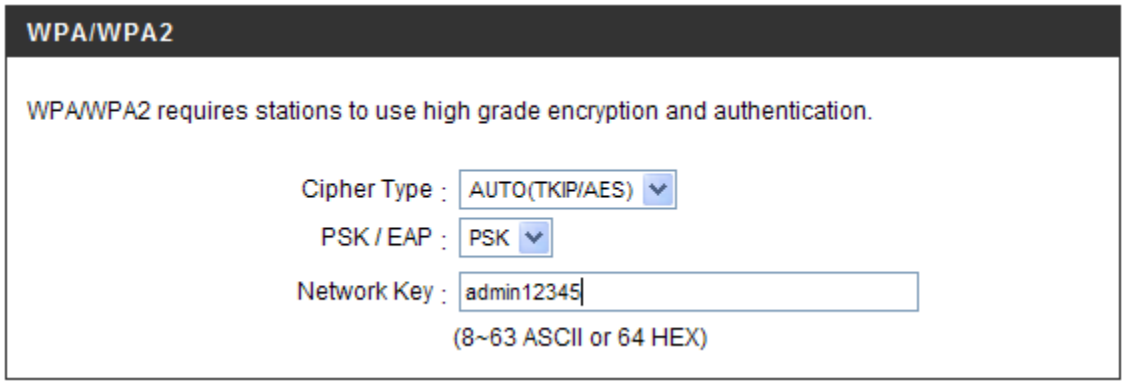



Рис. 63. Настройка маршрутизатора для режима шифрования WPA/WPA 2 PSK

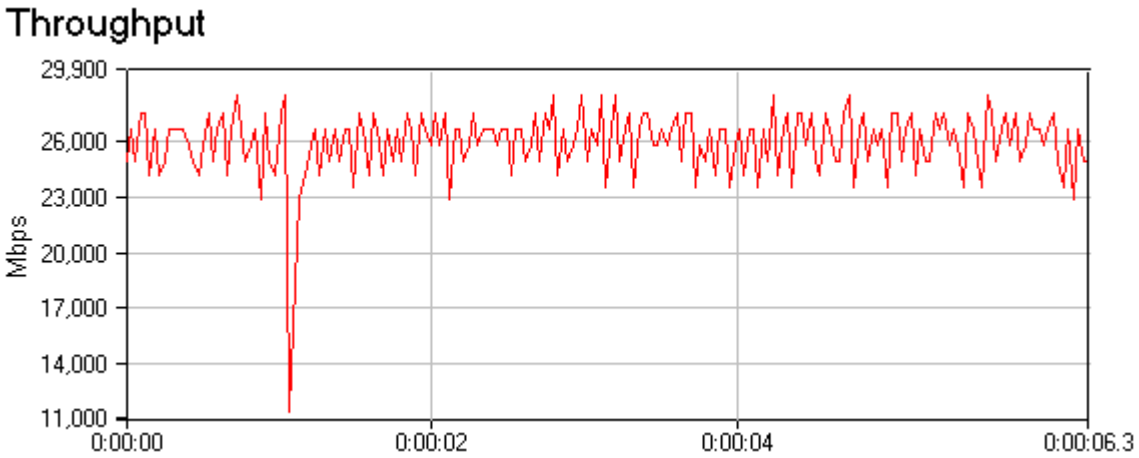



Рис. 64. Результаты измерений режима WPA/WPA 2 PSK

**AES**

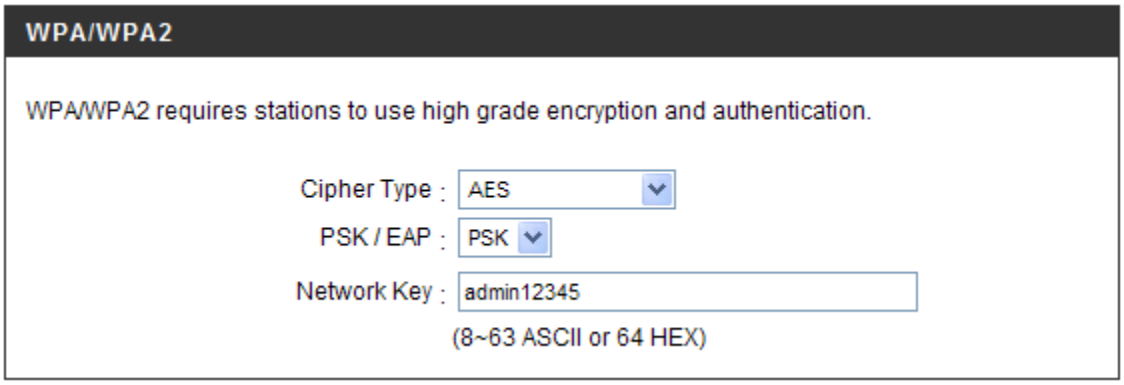



Рис. 65. Настройка маршрутизатора для режима шифрования AES

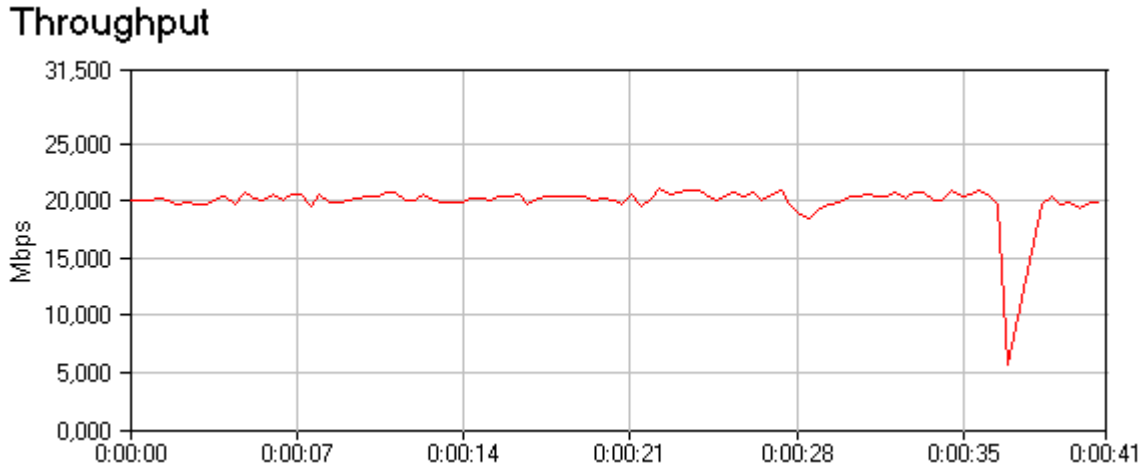



Рис. 66. Результаты измерений в режиме AES

Таблица 10. Результаты измерения времени отклика

| № теста | Время отклика, мсек |
|---|---|
| Без шифрования | 9 |
| TKIP | 10 |
| AES | 13 |

**Фрагментация фреймов**

Данный эксперимент направлен на определение зависимости скорости передачи от длины поля данных в передаваемом пакете.

**Методика тестирования**

Как и в предыдущих тестах, трафик сгенерированный программой NetIQ Chariot, пересылается между узлами Комп1 и Комп2 (рис. 52), при этом в настройках точки изменяется значение поля данных (Fragmentation) в диапазоне 1500 – 2346 бит. Измерение скорости производится в течении 2 минут, фиксируется среднее значение. По результатам тестирования строится график зависимости скорости передачи от длины поля данных

**Настройка оборудования**

Оставляем без изменения настройки ПК, выключаем шифрование на точках. Для настройки длины поля данных необходимо перейти на вкладку Advanced Wireless, в поле Fragmentation ввести соответствующее значение.

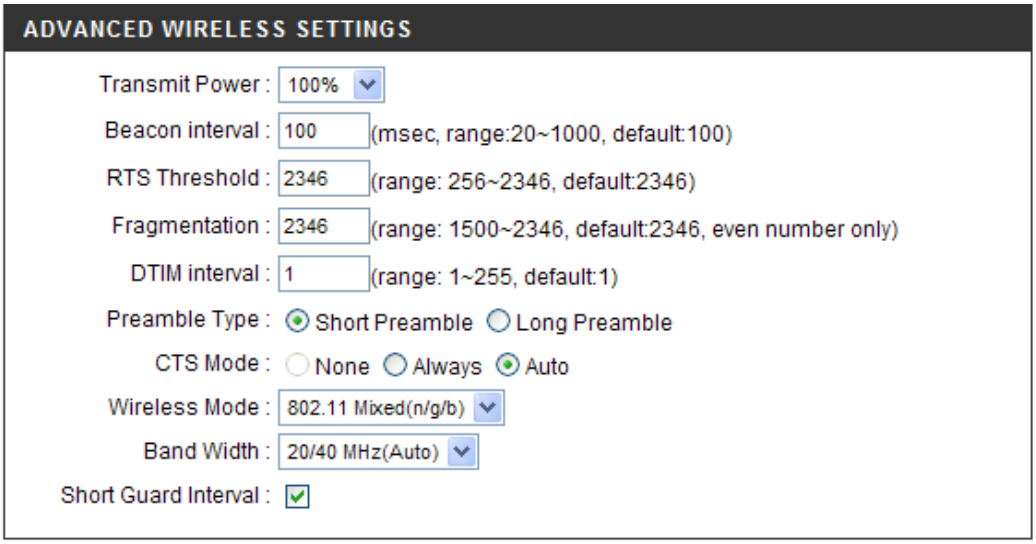



Рис. 67. Настройка длины поля данных передаваемого фрейма

Результаты тестирования

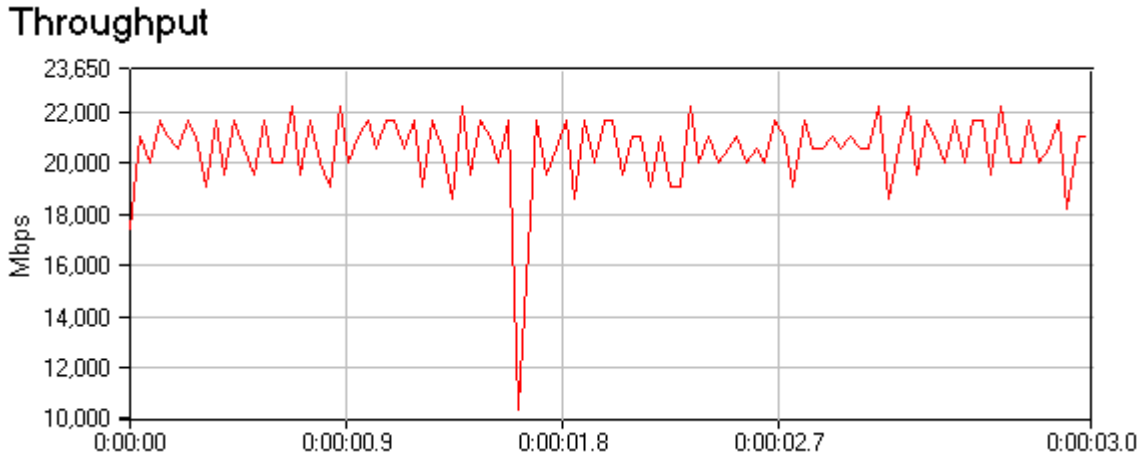



Рис. 68. Длина поля данных 1500 бит

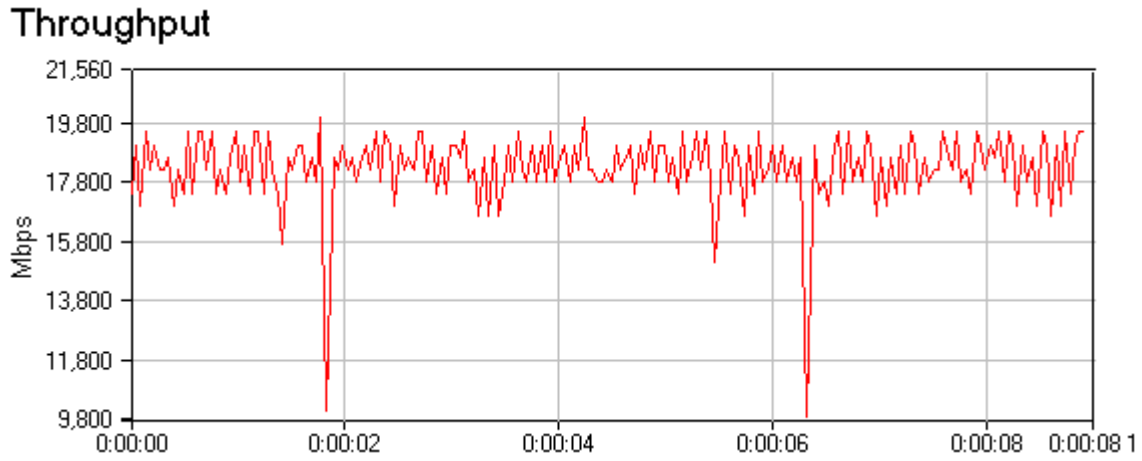



Рис. 69. длина поля данных 2000 бит

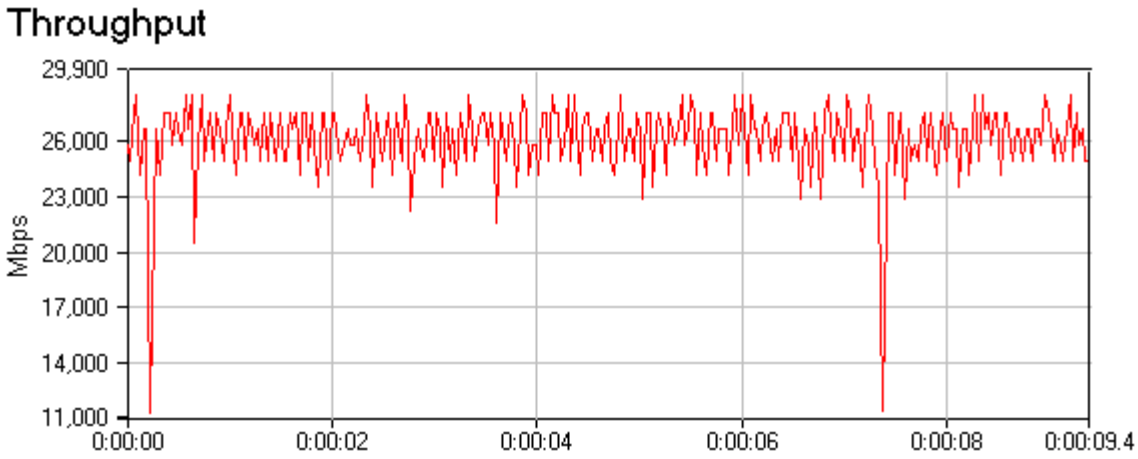



Рис. 70. длина поля данных 2346 бит

**Оценка взаимного влияния точек работающих на одном канале**

Оценка взаимного влияния точек работающих на одном канале. Тестовый стенд изображен на Рис.2. Точки доступа переводятся на один частотный канал, в первый случае. Между узлами comp1 и comp2, comp3 и comp4 осуществляется передача трафика сгененрированого программой NetIQ Chariot. При тестировании расстояние между точкой 1 и точкой 2 изменяется в пределах от 1 до 30 метров. Для каждого из выбранных значений расстояния L, для пары узлов comp1 и comp2 измеряется среднее значение скорости передачи, времени отклика, количество потерянных пакетов в течении 5 минут.

Настройка DSL-2640U на работу в режиме Bridging (режим прозрачного моста).

1. В разделе «Advanced Setup» выберите пункт «WAN», и нажмите кнопку «Add» для создания нового соединения.

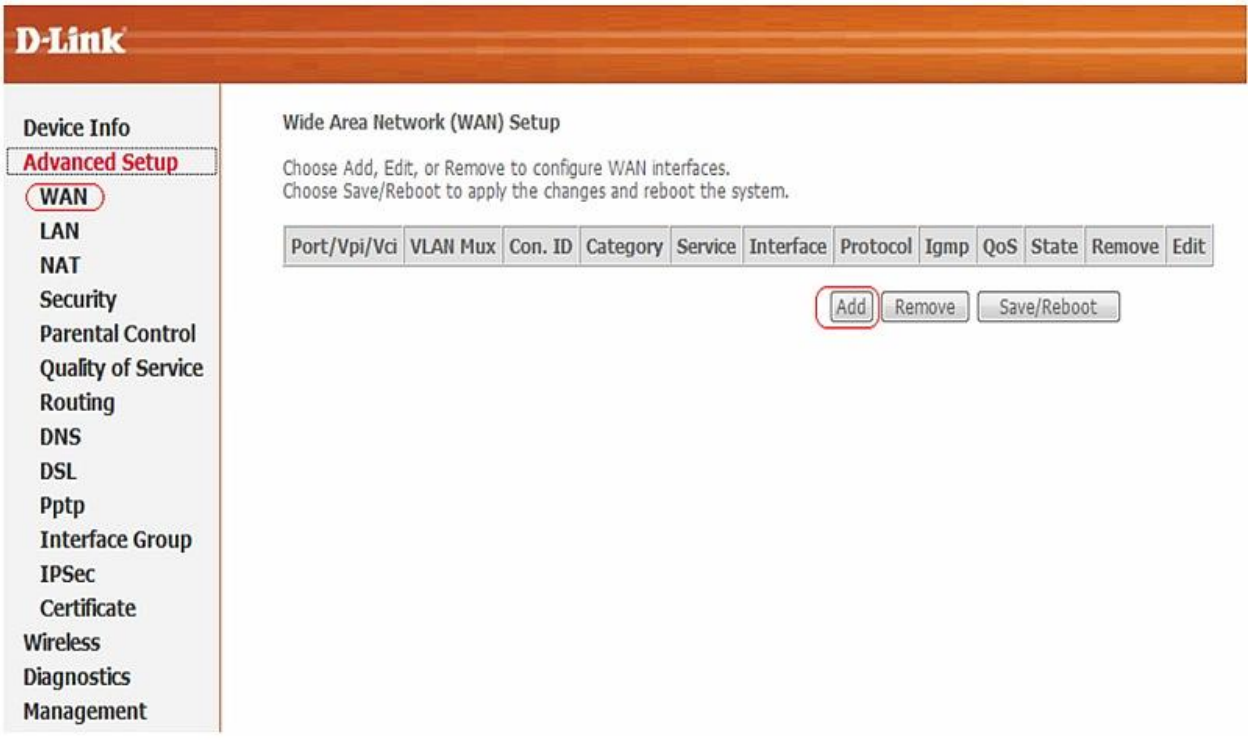


Рис. 71. Создание нового соединения

2. На появившейся странице укажите значения параметров VPI и VCI (значения данных параметров предоставляются провайдером) и нажмите кнопку «NEXT».

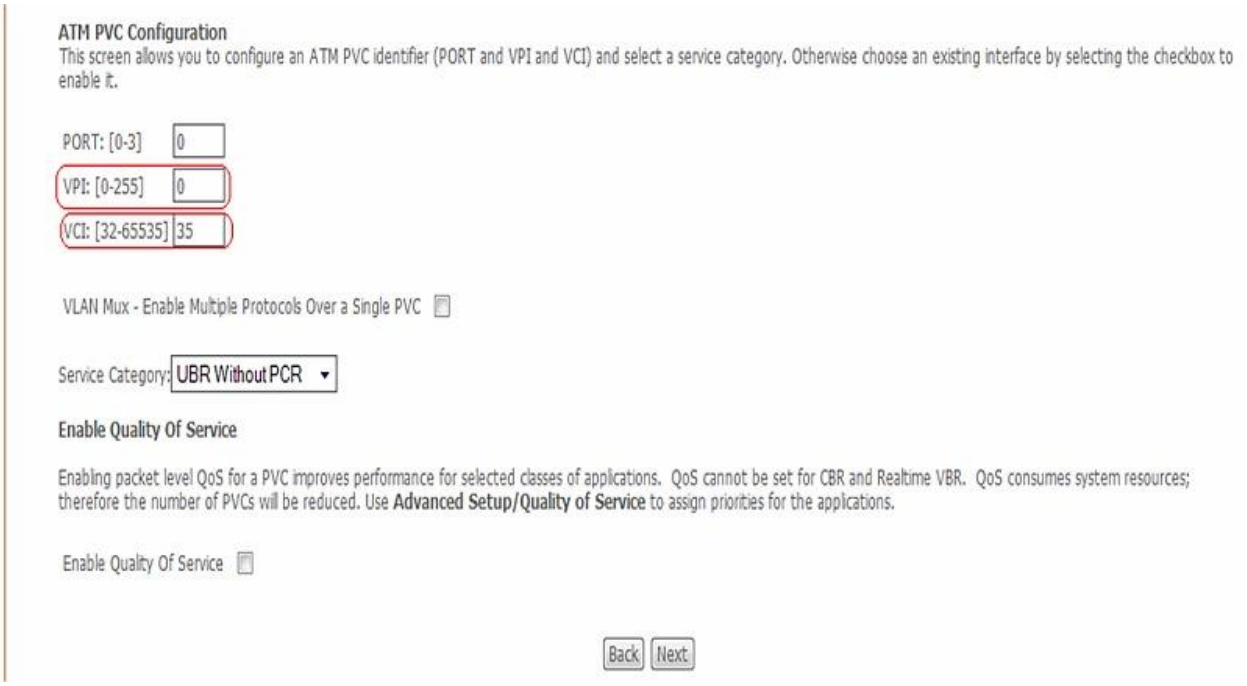



Рис. 72. Значение VPI и VCI

3. На следующей странице в разделе Connection Type установите «Bridging» и нажмите кнопку «NEXT».

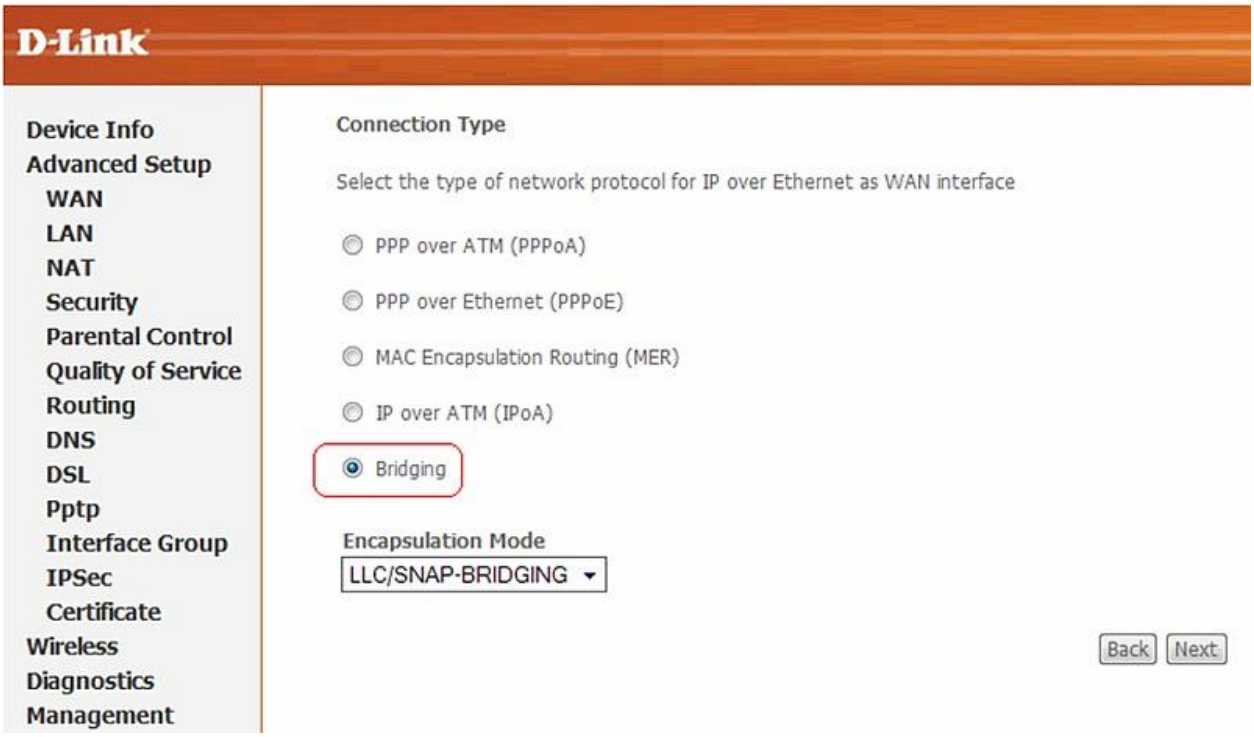



Рис. 73. Установка режим моста.

4. На следующей странице оставьте все настройки по умолчанию и нажмите кнопку «NEXT».

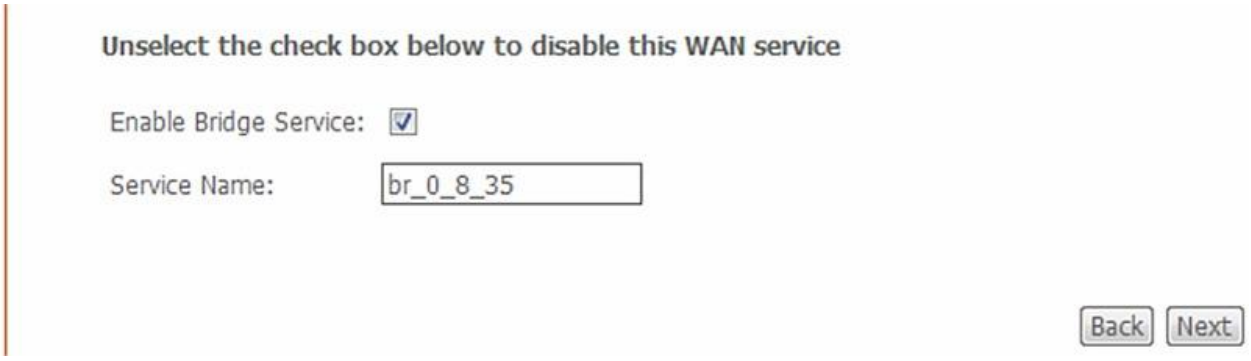



Рис. 74. Создаем имя моста

5. На следующей странице нажмите кнопку «Save».

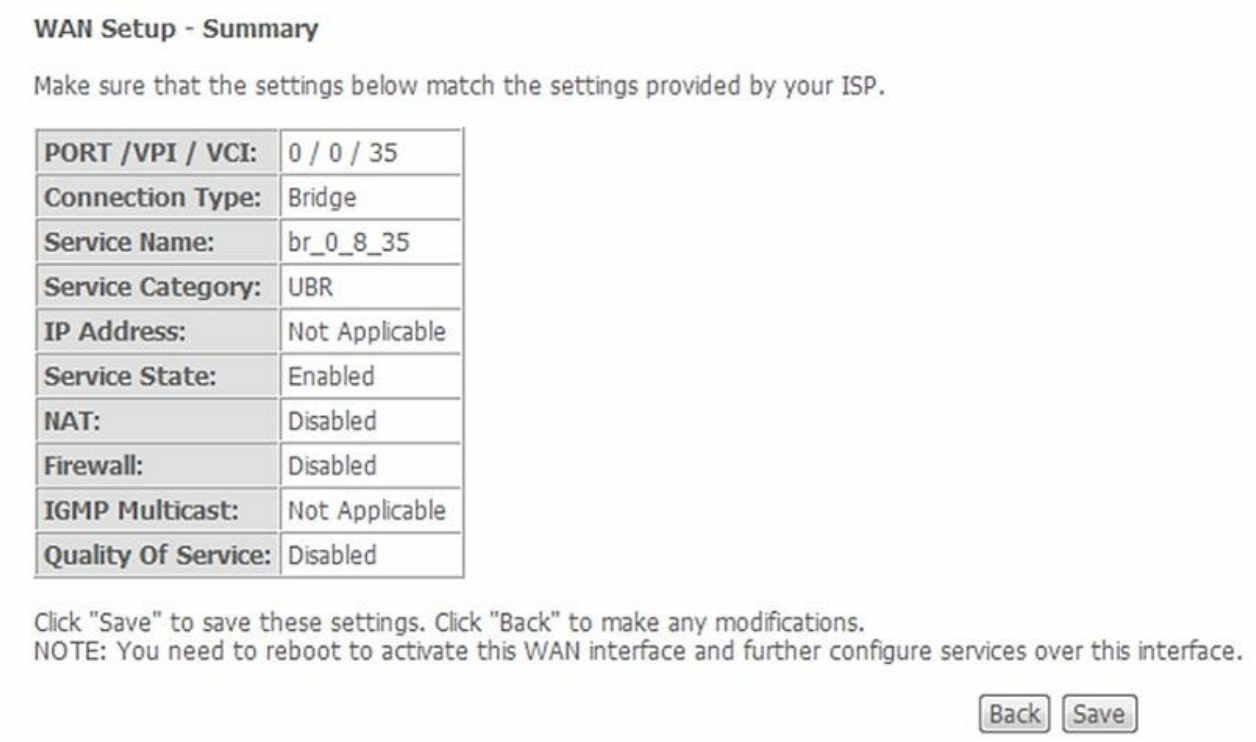



Рис. 75. Проверка настроек

6. После нажатия кнопки «Save» перейдите на страницу «Advanced Setup» > «WAN», где увидите созданное Bridge соединение. Нажмите кнопку «Save/Reboot» для применения параметров и перезагрузки устройства.

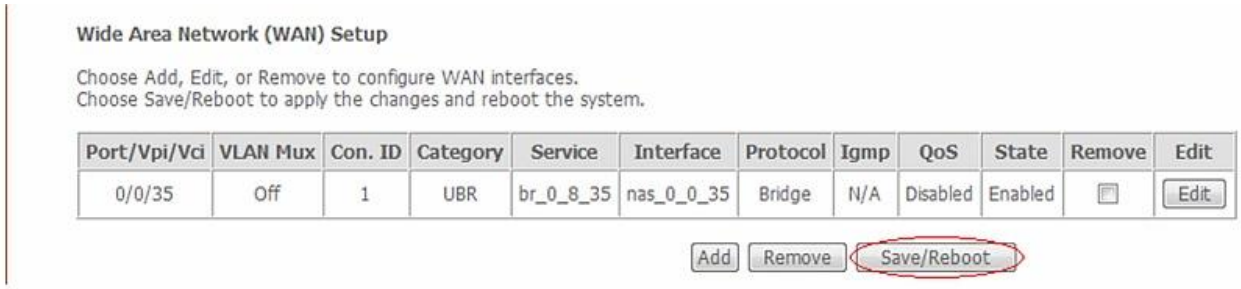



Рис. 76. Перезагрузка устройства

7. Перезагрузка устройства


Рис. 77. Окончание настройки

На этом настройка устройства закончена.

На обеих точках выключается шифрование трафика. Точки переводятся на работу в первый частотный канал. Точкам назначаются разные SIDD, точка один имеет SIDD «dlink», точка 2 «dlink2». Узлам comp1 и comp2, comp3 и comp4 назначаются адреса из одной подсети, конфигурируется тест, по аналогии с предыдущими тестами для генерации трафика используется скрипт throughput.scr, размер пакета максимален. Изначально точки удаленны друг от друга на расстояние 30 метров, с помощью программы Netstumbler 4.0, установленной на узле comp2 осуществляется контроль за уровнем сигнала.

Результаты тестирования

Таблица 11. Результаты измерения

| Расстояние между точками L, м | Скорость передачи Мбит/с | Среднее время отклика, мс | Количество потерянных пакетов, % |
|---|---|---|---|
| Точка №2 выключена | 45 | 12 | 0 |
| 30 | 43 | 12 | 0 |
| 20 | 36 | 13 | 0 |
| 15 | 32 | 13 | 0.01 |
| 10 | 31 | 14 | 0.05 |
| 8 | 30.5 | 15 | 0.1 |
| 5 | 30.5 | 15 | 0.6 |
| 3 | 29.5 | 18 | 1.5 |
| 1 | 30 | 23 | 3 |

Как и ожидалось обе точки сохранили работоспособность, не смотря на то что находились в непосредственной близости друг от друга. Используемый для предотвращения коллизий механизм распределенной координации заставляет точки конкурировать за среду, предотвращая тем самым одновременную передачу фреймов обоими точками.

Перед проведением эксперимента я полагал что скорость передачи должна была снизится более чем на 50% при размещении точек в непосредственной близости. Однако наблюдалось уменьшение скорости всего на 30%. При этом скорость передачи между узлами comp3 и comp4 равнялась 28-30 Мбит/с. Суммарная скорость двух систем работающих на одном канале оказалась равной 58-60 Мбит/с, чего в принципе не могло быть. Чтобы объяснить происходящее был детально исследован процесс включения точек. При включении второй точки (первая работала) скорость передачи между узлами comp3 и comp4 составляла около 5-8 Мбит/с, через 8-10 секунд скорость возрастала до 28-30 Мбит/с. При запуске сетевого сканера Netstumbler 4.0 оказалась что точка номер два использует по переменно несколько каналов рисунок 15.19. В точки D-Link Dir - 320 встроена утилита AutoCell которая способна автоматически выбирать не занятые каналы подстраивать мощность передатчика, она отключена, но при конфликтах самостоятельно активируется.

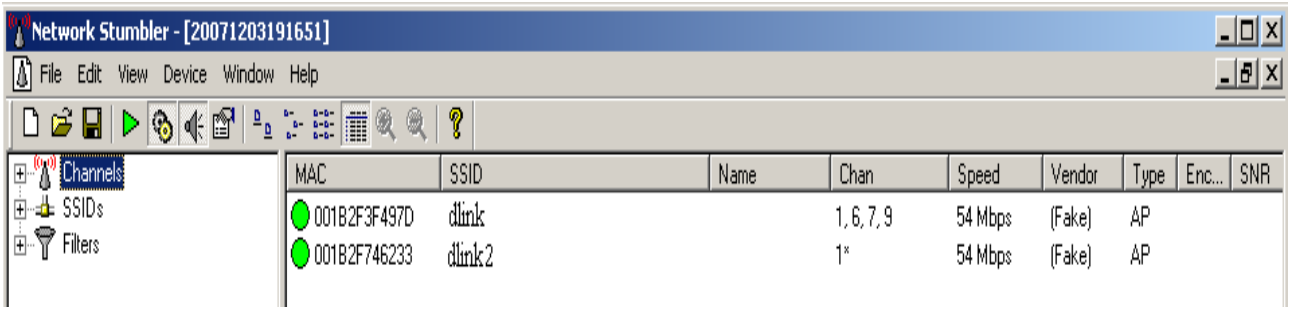



Рис. 78. Влияние точек доступа

**Взлом ключей шифрования для стандарта IEEE 802.11**

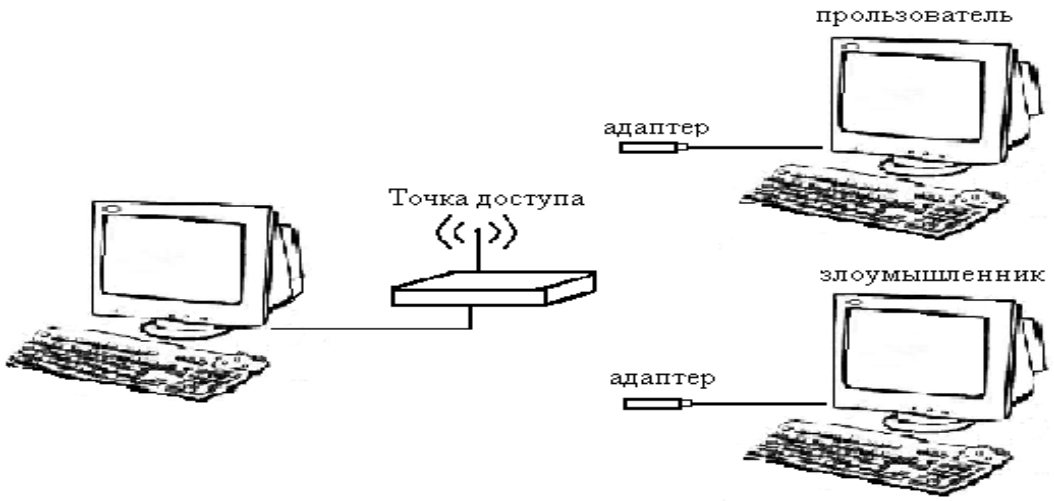



Рис. 79. Тестовый стенд для проверки методов шифрования

Настроим точку доступа на режим шифрования как показано в пункте 7. Затем произведем подключение адаптера к нашему компьютеру.

1. Получения ключа WEP шифрования. Для проведения данного рода атаки необходимо:

a. Перевести адаптер в режим мониторинга

```
Interface       Chipset         Driver

wlan0           Broadcom        b43 - [phy0]
                                (monitor mode enabled on mon1)
mon0            Broadcom        b43 - [phy0]
```

Рис. 80. Перевод адаптера в режим мониторинга

b. Заменить MAC-адрес адаптера (это делается для того чтобы показать что данная схема защиты не является эффективной)

```
root@dlink-01:~# macchanger --mac 00:11:22:33:44:55 wlan0
Current MAC: 00:11:22:33:44:55 (Cimsys Inc)
Faked MAC:   00:11:22:33:44:55 (Cimsys Inc)
It's the same MAC!!
```

Рис. 81. Замена MAC адреса

Затем поменяем MAC-адрес нашего адаптера. Нужно это для того, что бы показать, что данная схема защиты, т.е привязка по MAC-адресу уже не является функцией защиты.

c. Произвести поиск сети с шифрование данных WEP

После того как мы проделали данную работу можно приступить к поиску сети с шифрованием данных WEP. Для этого в операционной системе.

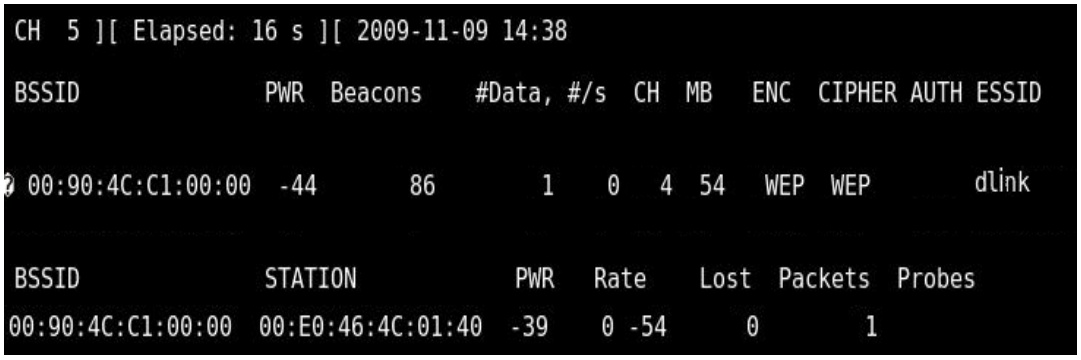



Рис. 82. Поиск сети

d. Произвести набор пакетов от 10000 до 25000 (это необходимо для дальнейшего анализа пакетов и получения ключа) и при помощи программы aircrack-ng произвести подбор ключа

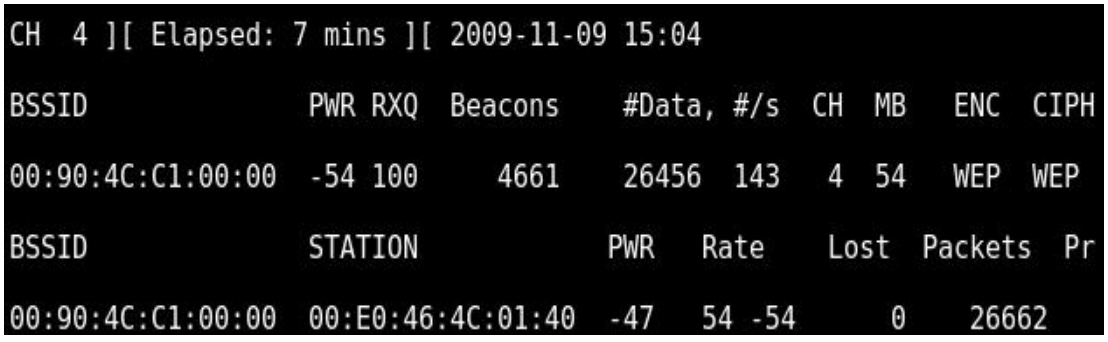



Рис. 83. Сбор пакетов

Для осуществления подбора ключа нам достаточно набрать от 10 000 до 25 000 пакетов. Дождавшись нужного количества пакетов, можно приостановить запись и приступить к перебору пароля. Программа aircrack-ng предназначенная для взлома ключей шифрования, которая перебирает комбинации до того момента, пока конечная сумма не совпадет. Так же она использует еще один метод, это подбор по словарю, но первый метод считается наиболее эффективным и быстрым.

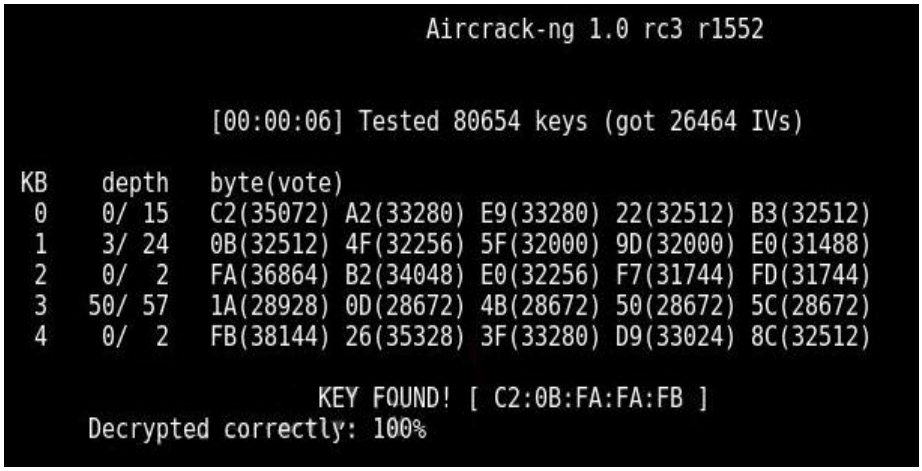



Рис. 84. Нахождение ключа

Подбор ключа занял 15 минут. Т.е. злоумышленнику не составит труда проникнуть в беспроводную сеть.

При изучении программного кода программы aircrack-ng было замечена незначительная ошибка в проверке пакетов, полученных при сборе из эфира. То есть в программе не была описана проверка пакетов на их точное шифрование, т.е если в начале программа проверяла, что пакеты именно ARP пакеты и записывала их в отдельный файл, то при дальнейшей работы программа не проверяла ни длину пакета ни его содержимое, а просто записывала их в отдельный файл. Что бы защитить сеть на WEP шифровании, надо внедрить в эфир пакеты с WPA шифрованием. Так сказать запутать программу, что бы злоумышленник применял методы атак для другого метода шифрования. Для этого нам понадобится еще один компьютер с wi-fi адаптером, который бы выкидывал “мусорный трафик” под точно таким же MAC-адресом как у точки, как было описано раньше, подделать MAC-адрес не так уж и сложно.

Для получения ключа WPA/WPA2 шифрования, пойдет упор на лобовой метод атаки, то есть перебор всех возможных вариантов ключа. Но мы же не знаем где начало пакетов, я имею ввиду тот счетчик который отправляет, пакеты по очередности. Что бы скинуть счетчик, непосредственно нужно провести атаку на пользователя, тогда же точке придется повторно авторизировать пользователя методом 4 этапного рукопожатия.

Нам не надо собирать множество пакетов из эфира - достаточно поймать первый кадр в котором передана информация о том, что пользователь авторизировался правильным ключом и может работать, принимая и расшифровывая пакеты. В первом же пакете и собранна вся информация о ключе. Тогда и проводить атаку мы будем непосредственно на пойманный пакет

2. Получение ключа WPA/WPA2 шифрования. Для проведения данного рода атак необходимо:

a. Задать самостоятельно ключ шифрования в настройках точки доступа

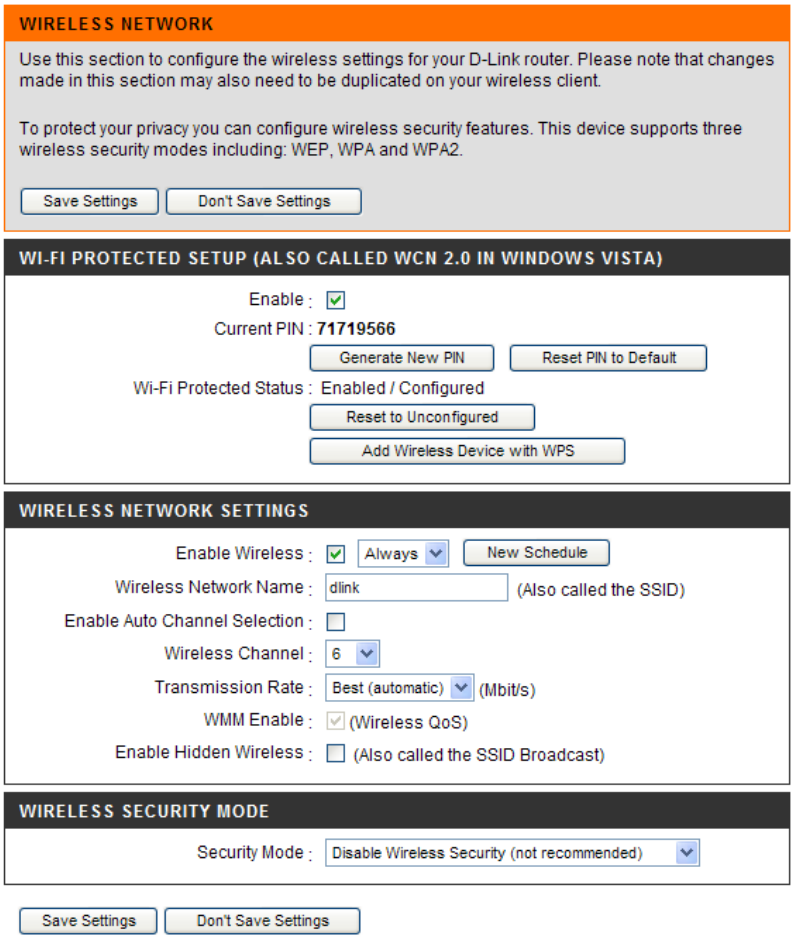



Рис. 85. Настройка точки доступа

b. Перевести адаптер в режим мониторинга

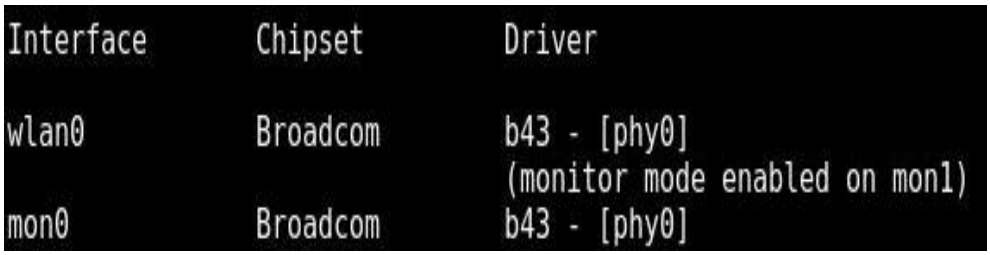



Рис. 86. Перевод адаптера в режим мониторинга

c. Выбрать пользователя для атаки и посылать покаты к точке доступа под MAC – адреса пользователя (это необходимо чтобы точка доступа отключила пользователя и он

начал авторизоваться снова)

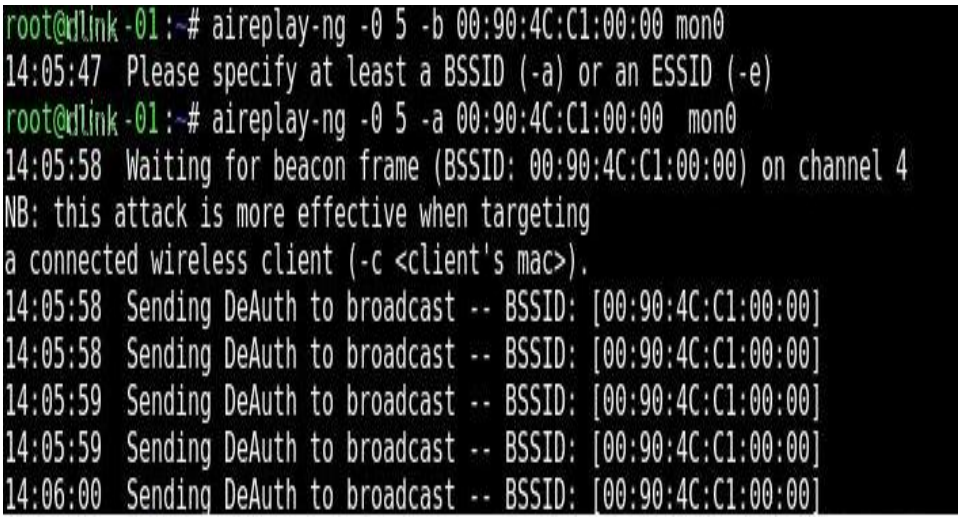



Рис. 87. Деавторизация пользователя


Рис. 88. Отключение пользователя от точки доступа

Пользователь которого мы усиленно отключим от точки доступа будет переключатся заново, то есть проходить авторизацию еще раз. Пакеты авторизации нам и нужны. Поймав эти пакеты, мы начнем перебор. Если пароль легкий то времени займет от 5 минут до 1 дня.

d. Перехватить пакеты авторизации

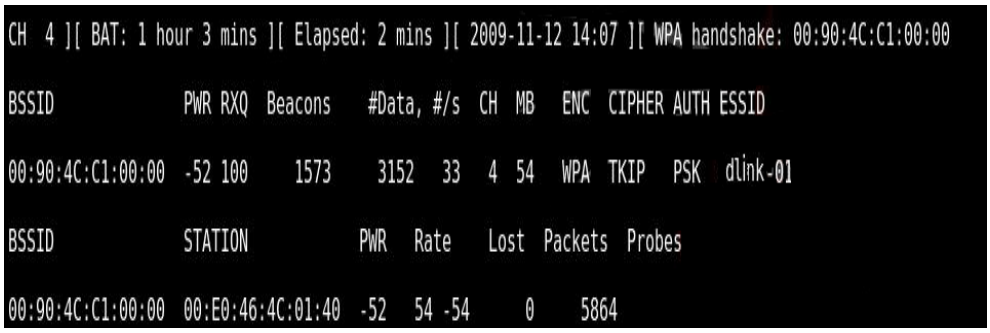



Рис. 89. перехват пакетов

e. При помощи программы aircrack-ng произвести подбор ключа.

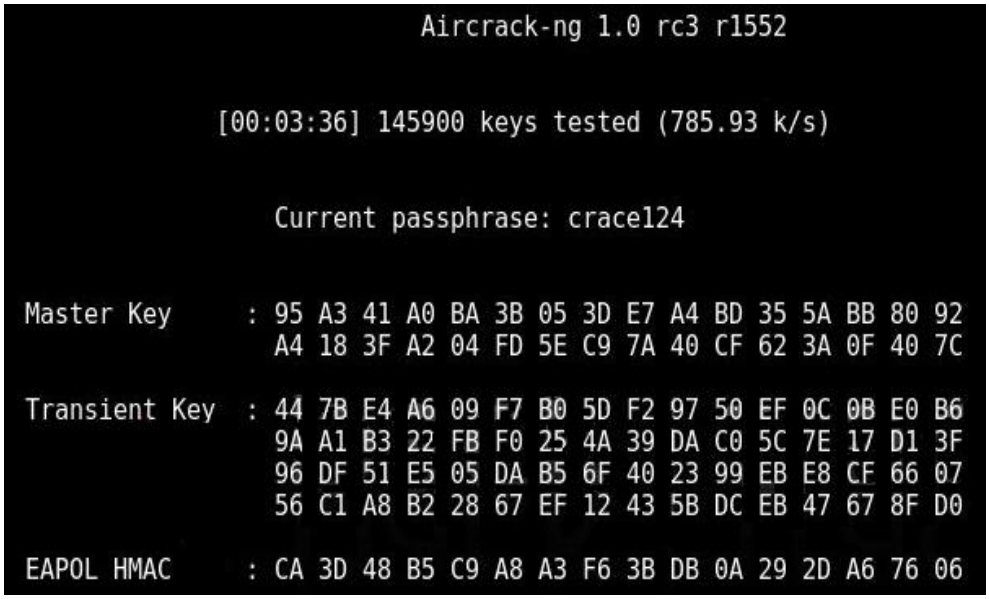



Рис. 90. Нахождение ключа

Для демонстрации устойчивости шифра к перебору, мы взяли простой пароль. Но заметно, что на эксперимент потребовалось 22 часа. Что позволяет сказать о том, что пароль будет сильнее и дольше перебираться, если его содержимое будет составлять Буквы нижних и верхних регистров, чисел и спецзнаков.

**Защита беспроводных сетей.**

Большинство беспроводных сетей никак не защищены от проникновения злоумышленника. Для обеспечения защиты беспроводного соединения необходимо учитывать множество факторов. Поскольку оборудования для беспроводных соединений постепенно дешевеет, то для большего числа пользователей становится возможным подключение к этой сети.

1. Максимальный уровень безопасности обеспечит применение VPN — используйте эту технологию в корпоративных сетях.
2. Если есть возможность использовать 802.1X (например, точка доступа поддерживает, имеется RADIUS-сервер) — воспользуйтесь ей (впрочем, уязвимости есть и у 802.1X).
3. Перед покупкой сетевого устройства внимательно ознакомьтесь с документацией. Узнайте, какие протоколы или технологии шифрования ими поддерживаются. Проверьте, поддерживает ли эти технологии шифрования ваша ОС. Если нет, то скачайте апдейты на сайте разработчика. Если ряд технологий не поддерживается со стороны ОС, то это должно поддерживаться на уровне драйверов.
4. Обязательно включать шифрование трафика.

5. Управлять доступом клиентов по MAC-адресам (Media Access Control, в настройках может называться Access List). Хотя MAC-адрес и можно подменить, тем не менее это дополнительный барьер на пути злоумышленника.

6. Запретить трансляцию в эфир идентификатора SSID, используйте эту возможность (опция может называться “closed network”), но и в этом случае SSID может быть перехвачен при подключении легитимного клиента.

7. Располагать антенну как можно дальше от окна, внешней стены здания, а также ограничивайте мощность радиоизлучения, чтобы снизить вероятность подключения «с улицы». Используйте направленные антенны, не используйте радиоканал по умолчанию.

8. При установке драйверов сетевых устройств предлагается выбор между технологиями шифрования WEP, WEP/WPA (средний вариант), WPA, выбирайте WPA (в малых сетях можно использовать режим Pre-Shared Key (PSK)).

9. Всегда используйте максимально длинные ключи. 128-бит — это минимум (но если в сети есть карты 40/64 бит, то в этом случае с ними вы не сможете соединиться). Никогда не прописывайте в настройках простые, «дефолтные» или очевидные ключи и пароли (день рождения, 12345), периодически их меняйте (в настройках обычно имеется удобный выбор из четырёх заранее заданных ключей — сообщите клиентам о том, в какой день недели какой ключ используется).

10. Не давайте никому информации о том, каким образом и с какими паролями вы подключаетесь (если используются пароли). Искажение данных или их воровство, а также прослушивание траффика путем внедрения в передаваемый поток — очень трудоемкая задача при условиях, что применяются длинные динамически изменяющиеся ключи. Поэтому хакерам проще использовать человеческий фактор.

11. Если вы используете статические ключи и пароли, позаботьтесь об их частой смене. Делать это лучше одному человеку — администратору.

12. Обязательно используйте сложный пароль для доступа к настройкам точки доступа.

13. По возможности не используйте в беспроводных сетях протокол TCP/IP для организации папок, файлов и принтеров общего доступа. Организация разделяемых ресурсов средствами NetBEUI в данном случае безопаснее. Не разрешайте гостевой доступ к ресурсам общего доступа, используйте длинные сложные пароли.

14. По возможности не используйте в беспроводной сети DHCP — вручную распределить статические IP-адреса между легитимными клиентами безопаснее.

15. На всех ПК внутри беспроводной сети установите файерволлы, старайтесь не устанавливать точку доступа вне брандмауэра, используйте минимум протоколов внутри WLAN (например, только HTTP и SMTP). Дело в том, что в корпоративных сетях файерволл

стоит обычно один — на выходе в интернет, взломщик же, получивший доступ через Wi-Fi, может попасть в LAN, минуя корпоративный файерволл.

16. Регулярно исследуйте уязвимости своей сети с помощью специализированных сканеров безопасности (в том числе хакерских типа NetStumbler), обновляйте прошивки и драйвера устройств, устанавливайте заплатки для Windows.

RADIUS-протокол предназначен для работы в связке с сервером аутентификации, в качестве которого обычно выступает RADIUS-сервер. В этом случае беспроводные точки доступа работают в enterprise-режиме.

Если в сети отсутствует RADIUS-сервер, то роль сервера аутентификации выполняет сама точка доступа - так называемый режим WPA-PSK (pre-shared key, общий ключ). В этом режиме в настройках всех точек доступа заранее прописывается общий ключ. Он же прописывается и на клиентских беспроводных устройствах. Такой метод защиты тоже довольно секьюрен (относительно WEP), очень не удобен с точки зрения управления. PSK-ключ требуется прописывать на всех беспроводных устройствах, пользователи беспроводных устройств его могут видеть. Если потребуется заблокировать доступ какому-то клиенту в сеть, придется заново прописывать новый PSK на всех устройствах сети и так далее. Другими словами, режим WPA-PSK подходит для домашней сети и, возможно, небольшого офиса, но не более того.

Для того, чтобы пользователи проектируемой сети имели разграниченный доступ (в зависимости от логина и пароля), а также для того, чтобы избежать атак извне, необходимо иметь отдельный сервер авторизации (AAA-сервер).

В качестве такого сервера, в нашей сети будет выступать RADIUS сервер.

**3. Порядок выполнения работы**

1. Ознакомится с теорией по беспроводным сетям стандарта IEEE 802.11

2. Взять у преподавателя ключа шифрования для точки доступа;

3. Исследование производительности точки доступа:

3.1. Запустить программу NetIQ Chariot.

3.2. Открыть окно Add an Endpoint Pair.

3.3 В окне Add an Endpoint Pair в строках Endpoint 1 и Endpoint 2 написать MAC адреса компьютеров производящих измерения.

3.3. Выбрать скрипт throughput.

3.4. В настройках скрпита выбираем поле size_file и изменяем его значение согласно заданию.

3.5. Произвести измерения с различными значениями size_file и записать их в таблицу.

| | | | | |
|---|---|---|---|---|
| Размер поля size_file | | | | |
| Скорость передачи данных | | | | |
| Время отклика | | | | |

3.6. Построить графики зависимости скорости передачи данных от величины передаваемого пакета.

3.7. Сделать выводы.

4.Шифрование:

4.1. Запустить программу NetIQ Chariot.

4.2. Сделать размер отправляемого файла 1500 бит.

4.3. Зайти в настройки точки доступа.

4.4. Включит режим шифрования в соответствии с заданием.

4.5. Произвести измерения.

4.6. Поменять режим шифрования.

4.7. Повторить пункты 4.4-4.6 в соответствии с заданием

4.8. По полученным результатам заполнить таблицу:

| | | | | |
|---|---|---|---|---|
| Режим шифрования | | | | |
| Скорость передачи данных | | | | |
| Время отклика | | | | |

4.10. Построить на одном графике скорости передачи данных для различных режимов шифрования.

4.11. Сделать выводы.

5. Фрагментация фреймов:

5.1. Открыть настройки точки доступа.

5.2. Перейти на вкладку Advanced Wireless, в поле Fragmentation ввести соответствующее значение.

5.3. По полученным результатами заполнить таблицу:

| | | | | |
|---|---|---|---|---|
| Размер фрейма | | | | |
| Скорость передачи | | | | |

| | | | | |
|---|---|---|---|---|
| данных | | | | |
| Время отклика | | | | |

5.4 Построить график зависимости скорости передачи данных от размера фрейм.

5.5 Сделать выводы.

6. Взлом ключа шифрования WEP:

6.1. Ввести в настройках точки доступа ключ шифрования.

6.2. Открыть программу aircrack-ng.

6.3. Перевести адаптер в режим мониторинга.

6.6. Заменить MAC-адрес адаптера.

6.7. Произвести поиск сети с шифрование данных WEP .

6.8. Произвести набор пакетов от 10000 до 25000.

6.9. Произвести подбор ключа.

6.10. Произвести анализ полученных данных

7 Взлом ключа шифрования WPA/WPA2:

7.1. Перевести адаптер в режим мониторинга.

7.2. Выбрать пользователя для атаки и посылать пакеты к точке доступа под MAC – адреса пользователя

7.3. Перехватить покаты авторизации

7.4. При помощи программы aircrack-ng произвести подбор ключа.

7.5. Произвести анализ полученных данных

**Лабораторная работа 2. Исследование и администрирование средств обеспечения информационной безопасности Web-сервера Microsoft IIS Server**

**1. Цель работы**

Изучение, установка, настройка и администрирование Web-сервера IIS 7.0 на Windows Server 2008 R2, создание на основе IIS 7.0 хостинга, специально оптимизированного для размещения сайтов в Интернете.

**2. Краткие теоретические сведения**

Веб-сервером (от англ. Web-Server) называют как программное обеспечение, выполняющее функции веб-сервера, так и компьютер, на котором это программное обеспечение работает. Таким образом, веб-сервер – это компьютер, специально оптимизированный для размещения сайтов в Интернете (со специальным программным обеспечением), и сервер, принимающий HTTP - запросы от клиентов, обычно веб-браузеров, и выдающий им HTTP-ответы, обычно вместе с HTML-страницей, изображением, файлом, медиапотоком или другими данными. Веб-серверы — основа Всемирной паутины. Клиенты

получают доступ к веб-серверу по URL адресу нужной им веб-страницы или другого ресурса.

У веб-сервера одна задача: получить по сети запрос и послать на него ответ. Формально, запрос – это указание веб-серверу, какой ресурс вы бы хотели получить. Под ресурсом подразумевается документ HTML. Итак, набирая в адресной строке браузера какой-либо адрес на самом деле формируете запрос веб-серверу. Веб-сервер должен принять запрос. Понять его и обработать. Обработка означает передачу запрошенного ресурса или объяснение, почему ресурс не может быть предоставлен. Если вы не ошиблись в запросе и таковой ресурс имеются вналичии и вы его можете получить, тогда веб-сервер выбирает нужный документ HTML и передает его по сети вам. Причем, передает он его без каких-либо модификаций.

**Internet Information Services 7.0**

Internet Information Services 7.0 (IIS 7.0) – это последняя версия веб-сервера компании Microsoft. IIS был включен в состав семейства операционных систем Windows Server начиная с операционной системы Windows 2000 Server в качестве компонента Windows Component, а также для Windows NT в качестве дополнения. IIS 7.0 входит в состав операционных систем Windows Vista и Windows Server 2008, которые были выпущены в первой четверти 2008. IIS 7.0 претерпел множество изменений и новый дизайн был написан с нуля. Это было сделано для того, чтобы сделать его самой гибкой и безопасной платформой для размещения веб-приложений.

IIS 7.0 был спроектирован, чтобы быть самой безопасной и гибкой платформой для веб-приложений от компании Microsoft. Microsoft полностью переделала дизайн IIS, и во время этого процесса команда разработчиков IIS сфокусировалась на 5 основных областях:

- Безопасность
- Расширяемость
- Конфигурация и установка
- Администрирование и диагностика
- Производительность

Компания Microsoft сфокусировалась на модульности при создании IIS 7.0, что означает, что для установки необходимы лишь бинарные файлы, что минимизирует пространство для атак на веб-сервер. Операционная система Windows Server 2008 включает в себя все возможности IIS, необходимые для поддержки и размещения веб содержимого в промышленных средах.

**Роль веб-сервера (IIS)**

Основные характеристики служб IIS 7.0:

- гибкая модель расширения для эффективной настройки;
- эффективные средства диагностики, а также поиска и устранения неполадок;
- делегированное администрирование;
- улучшенная защита и ограничение уязвимости для атак путем настройки;
- реальное развертывание приложений с помощью команды xcopy;
- интегрированные средства управления приложениями и работоспособностью для служб Windows Communication Foundation (WCF);
- усовершенствованные средства администрирования.

Благодаря этим преимуществам службы IIS 7.0 обеспечивают единую согласованную модель разработки и администрирования интернет решений.

**Гибкая модель расширения для эффективной настройки**

Службы IIS 7.0 поддерживают новые более эффективные способы расширения функциональности в соответствии с конкретными требованиями. Модель расширения IIS 7.0 включает новые прикладные программные интерфейсы основных компонентов сервера, позволяющие разрабатывать функциональные модули как в машинном коде (C/C++), так и в управляемом коде (языки, использующие .NET Framework, такие как C# и Visual Basic 2005).

IIS 7.0 также поддерживают наборы расширений настройки, сценариев, регистрации событий и средств администрирования, предоставляя разработчикам программного обеспечения полную серверную платформу для создания расширений веб-сервера.

**Эффективные средства диагностики, а также поиска и устранения неполадок**

Службы IIS 7.0 облегчают поиск и устранение неполадок в работе веб-узлов и приложений. Они обеспечивают ясное представление внутренних диагностических сведений о работе IIS, а также собирает и позволяет изучать события диагностики, помогая устранять неполадки в работе проблемных серверов.

**Делегированное администрирование**

Службы IIS 7.0 позволяют при размещении или администрировании веб-узлов или служб WCF делегировать администрирование разработчикам или владельцам содержимого, что сокращает стоимость владения системой и снижает нагрузку на администратора. Для использования этих функций делегирования предоставляются новые средства администрирования.

**Улучшенная защита и ограничение уязвимости для атак**

**путем настройки**

Компоненты, устанавливаемые и выполняемые на веб-сервере, можно выбирать. Службы IIS 7.0 включают более 40 отдельных функциональных модулей. Каждый из них

можно установить на сервере независимо от других для уменьшения числа возможных направлений атаки на сервер и сокращения нагрузки на администратора.

**Развертывание приложений с помощью команды хсору**

Службы IIS 7.0 позволяют хранить параметры конфигурации IIS в файлах web.config, что значительно облегчает использование команды хсору для копирования приложений между интерфейсными веб-серверами, позволяя обходиться без дорогостоящих и подверженных ошибкам процедур репликации и избегать проблем, возникающих при синхронизации вручную.

**Управление приложениями и работоспособностью для служб WCF**

Для повышения эффективности разработки и размещения служб WCF с использованием различных протоколов в Windows Server 2008 включена служба активации Windows (WAS), поддерживающая модульную активацию произвольных прослушивателей протоколов. Служба WAS предоставляет доступ к различным приложениям, активируемым сообщениями, с интеллектуальным управлением ресурсами, активацией процессов по запросу, наблюдением за работоспособностью, а также автоматическим обнаружением сбоев и перезапуском процессов. Служба WAS основана на модели обработки запросов IIS 6.0.

**Усовершенствованные средства администрирования**

В IIS 7.0 реализован новый пользовательский интерфейс, ориентированный на выполнение задач, и новое средство командной строки для администрирования веб-серверов, веб-узлов и веб-приложений. Дополнительные сведения см. ниже, в подразделе "Средства администрирования" раздела.

**Архитектура**

В основе использовался модульный дизайн. Модульный дизайн обеспечивает больше гибкости и безопасности для IIS 7.0, по сравнению с предыдущими версиями IIS.

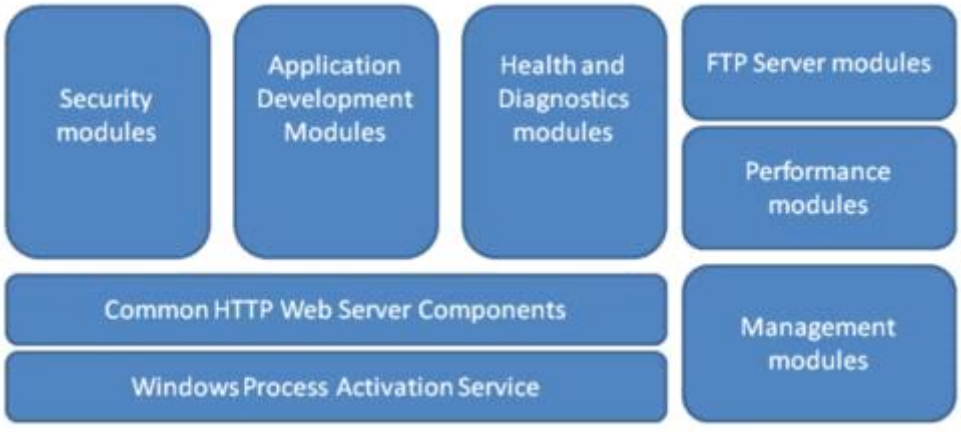



Рис. 1. Обзор основных модулей и компонентов IIS 7.0

Основное преимущество нового модульного дизайна заключается в том, что он

помогает снизить опорную поверхность, что обеспечивает большую безопасность платформы для веб-сервера, т.к. в этом случае минимизируется поверхность для атак.

IIS 7.0 снабжен новым собственным корневым API, который заменил фильтр ISAPI filter, используемый в предыдущих версиях IIS. Благодаря новому API появилась возможность для расширения IIS с помощью новых модулей, или даже замены любых встроенных модулей собственными модулями.

**Администрирование**

Существует несколько способов для администрирования IIS 7.0.

- Графический интерфейс GUI с помощью менеджера IIS Manager
- Инструмент командной строки APPCMD
- Удаленное администрирование (Remote administration) с помощью IIS Manager
- Написание сценариев с помощью Windows PowerShell
- Интерфейс Microsoft.Web.Administration API interface

Графический интерфейс для управления GUI Management был также изменен, новый менеджер IIS Manager теперь более ориентирован на выполнение задач.

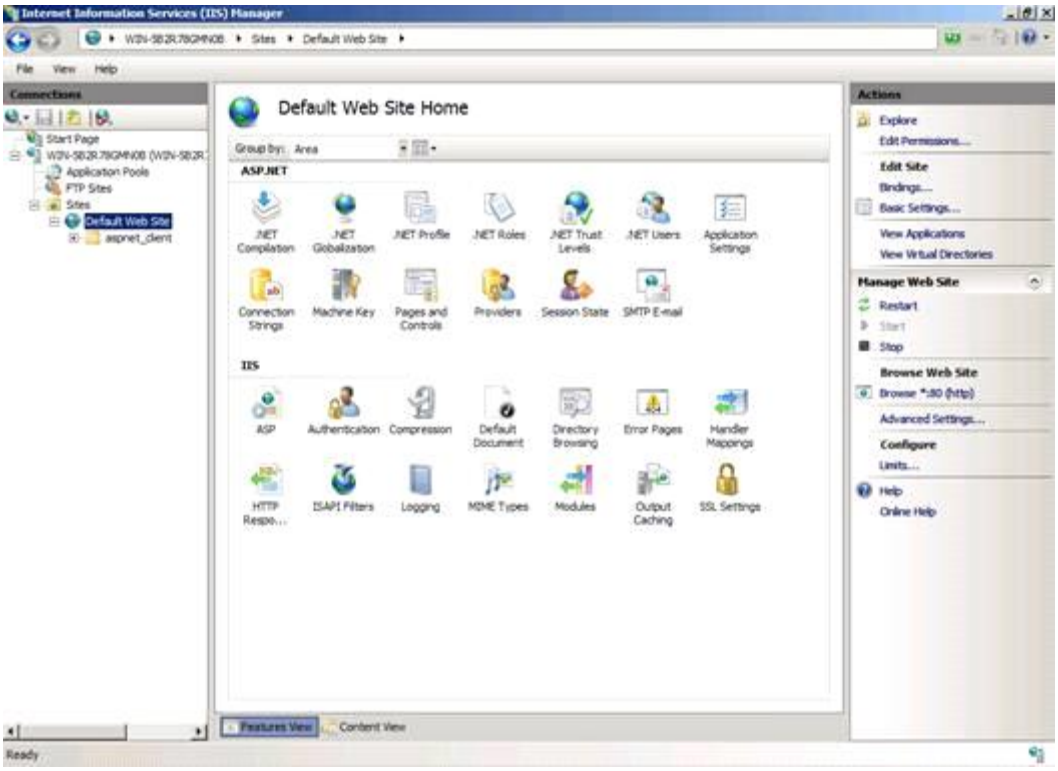



Рис. 2. Окно менеджера IIS Manager

Менеджер IIS Manager можно использовать для настройки параметров IIS и ASP.NET, конфигурационные параметры записываются в конфигурационные файлы в формате xml. Информация о состоянии и диагностика теперь доступна напрямую из менеджера IIS Manager, и теперь является частью IIS 7.0.

APPCMD – это новый инструмент общего назначения для IIS 7.0, работающий из командной строки, который используется для администрирования и настройки IIS. APPCMD – это новая улучшенная версия старого модуля adsutil.vbs.

Удаленное администрирование (Remote Administration) было также улучшено, и теперь появилась возможность использование менеджера IIS Manager, при безопасном взаимодействии по https с веб-сервером.

Существует также возможность написания сценариев для управления IIS. Это делается с помощью Windows PowerShell, который является новым языком для написания сценариев от компании Microsoft. Это простой и эффективный способ для администрирования IIS на вашем веб-сервере, которое особенно полезно, если вы управляете несколькими веб-серверами или большими веб фермами. Windows PowerShell может напрямую использоваться для интерфейса WMI IIS или использоваться для чтения или записи в конфигурационные файлы IIS 7.0 XML.

IIS 7.0 обладает обратной совместимостью с метабазой IIS 6.0 metabase и ADSI, а также интерфейсом для написания сценариев WMI scripting interface, известный с версии IIS 6.0, что означает, что все ваши сценарии, написанные для версии IIS 6.0 будут работать и для версии IIS 7.0.

Microsoft.Web.Administration API – это интерфейс для разработчиков, которые хотят писать свои собственные программы или сценарии для управления IIS 7.0.

В IIS 7.0 существует возможность передачи управления над IIS и веб- сайтами. Вы можете передать полный административный доступ владельцам веб-сайта. Владельцы веб-сайта могут контролировать и управлять всеми настройками веб-сайта с помощью менеджера IIS Manager, при этом безопасность сервера не будет страдать. Все настройки, которые меняют владельцы сайтов, записываются в файл в формате xml под названием web.config на их веб сайте.

**Конфигурация**

Конфигурация значительно упростилась, и теперь она основана на распределенных XML файлах, которые содержат конфигурационные параметры для всего IIS и ASP.NET.

Конфигурационные параметры могут быть настроены глобально для всего веб-сервера или для определенных веб-сайтов, с помощью XML файлов, или с помощью графического интерфейса управления (GUI Management interface). Графический интерфейс лишь записывает конфигурационные параметры в то те же самые XML файлы. Основные конфигурационные файлы xml в IIS 7.0 это:

- Applicationhost.config
- Global web.config

- Machine.config
- Site web.config
- App web.config

Благодаря использованию конфигурационных файлов в формате xml, установка и масштабирование в больших средах значительно оптимизировалась. Теперь достаточно просто скопировать конфигурацию IIS на новый сервер и просто запустить его.

Выполнение репликации конфигурации веб-сервера также значительно упростилось для IIS 7.0 по сравнению с IIS 6.0, благодаря использованию конфигурационных файлов в формате xml. Благодаря этому очень просто скопировать и установить конфигурацию в крупных средах.

Общая конфигурация (Shared Configuration) – это новая возможность в IIS 7.0, которая была разработана для веб ферм (web farm). С помощью общей конфигурации (Shared Configuration) теперь появилась возможность для нескольких веб-серверов использовать один конфигурационный файл (applicationhost.config). Главный файл размещается по общему пути UNC. Возможность использования общей конфигурации (Shared Configuration) – это великолепная альтернатива перспективе копирования настроек IIS.

Файл в формате xml под названием Applicationhost.config является основным конфигурационным файлом IIS 7.0, этот конфигурационный файл содержит всю информацию о сайтах, виртуальных директориях, приложениях, пулах приложений и глобальных настройках для веб-сервера.

Репликация содержимого может быть легко выполнена с помощью команды x-copy или robocopy, точно также как и особые настройки веб-сайта, которые хранятся в файле web.config в формате xml внутри сайта.

Благодаря изменению дизайна IIS, компания Microsoft сделала IIS 7.0 лучшим веб-сервером для всех, начиная со специалистов по информационным технологиям IT и разработчиков до Web Hosters. IIS 7.0 является очень мощным продуктом:

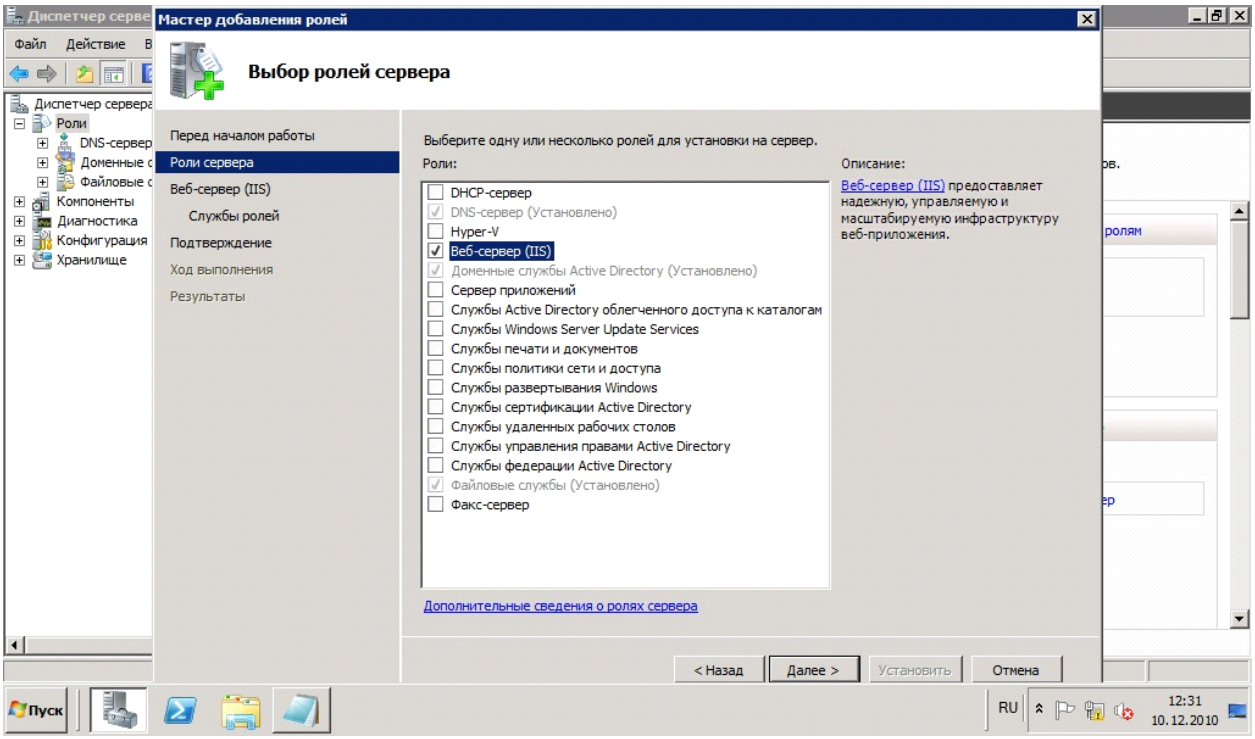
- Продукт стал более безопасным – можно устанавливать только бинарные файлы
- Он расширяем и гибок благодаря использованию новой модульной архитектуры
- Он стал более масштабируемым благодаря упрощению настройки, для которой теперь используются файлы в формате xml
- Улучшение производительности благодаря улучшениям в ядре IIS (http.sys)

**3. Порядок выполнения работы**

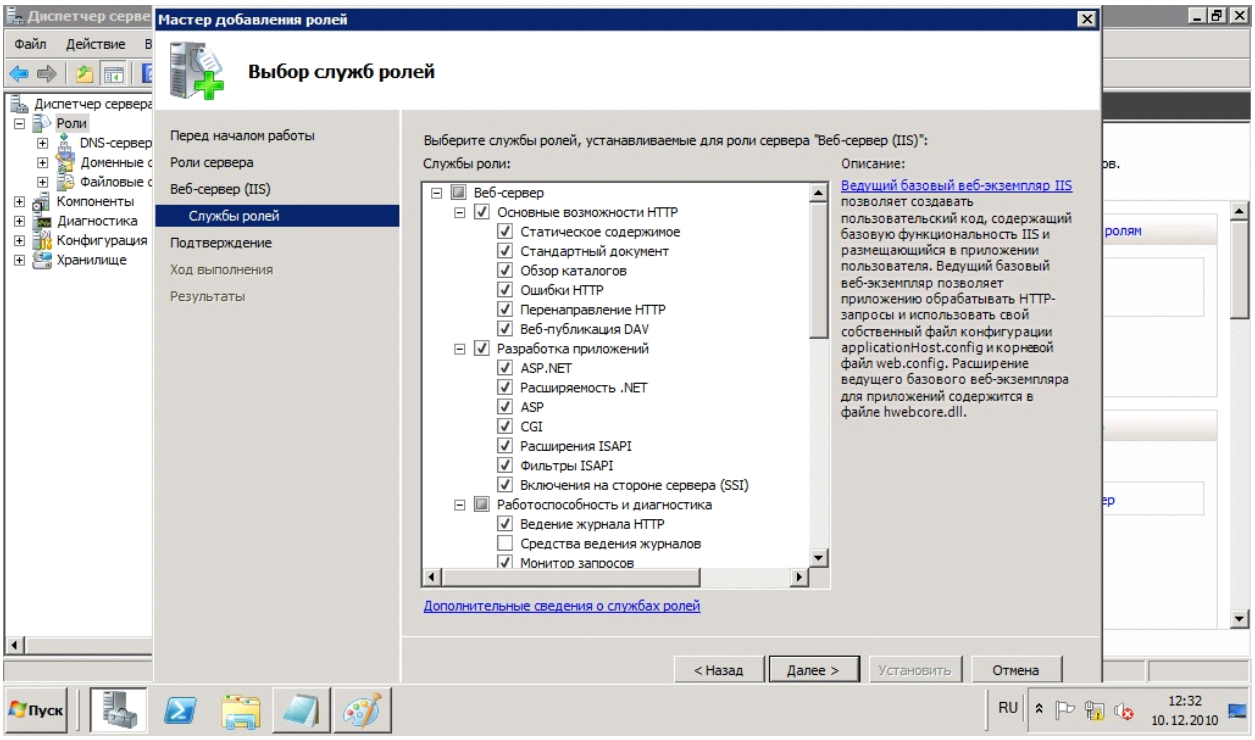
**Установка и настройка IIS на Windows Server 2008 R2, а так же установка**

**различных cms (на конкретном примере - drupal)**

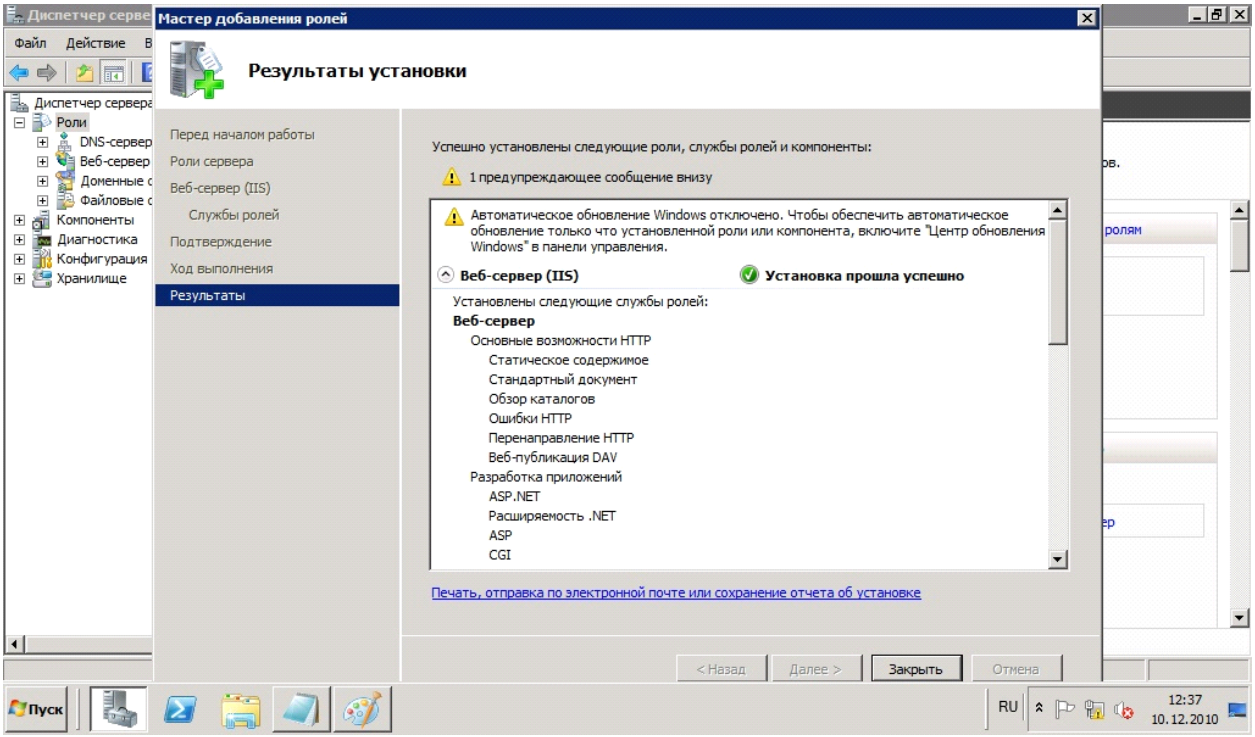
1) Включаем роль IIS. Для этого заходим в пуск - администрирование - диспетчер сервера - вкладка роли. Кликаем - добавить роли и в ролях отмечаем веб-сервер iis для установки.




Выбираем службы ролей, которые потребуются в дальнейшем использовании



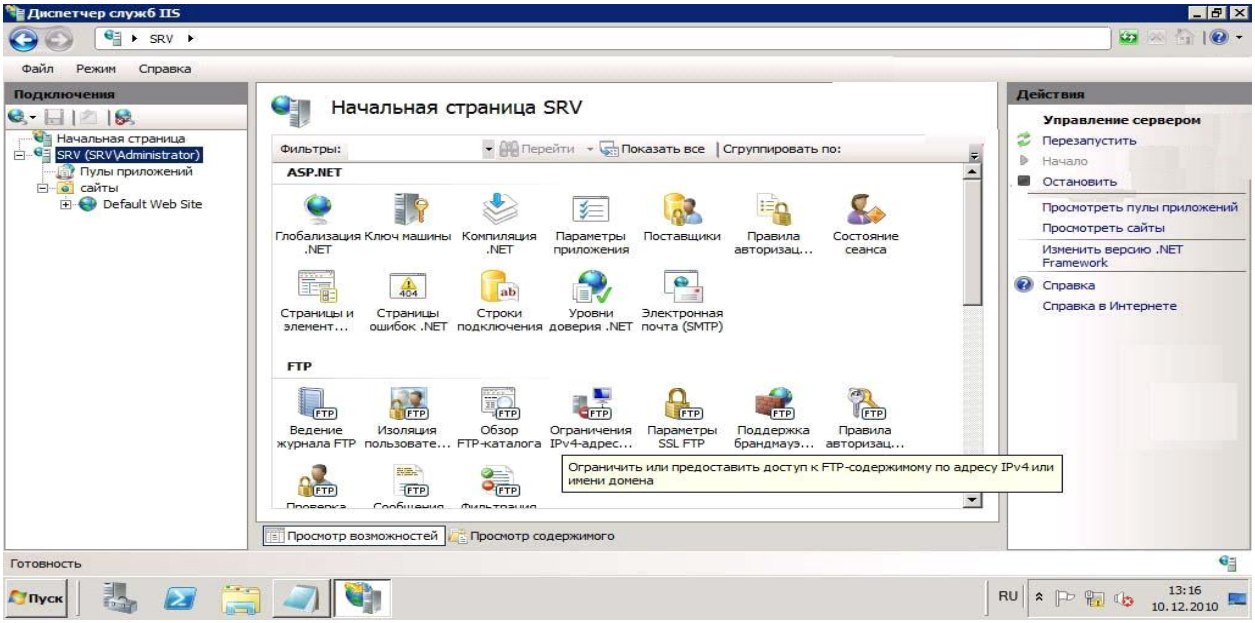
Затем выводятся результаты об установке




На этом этапе установка заканчивается.

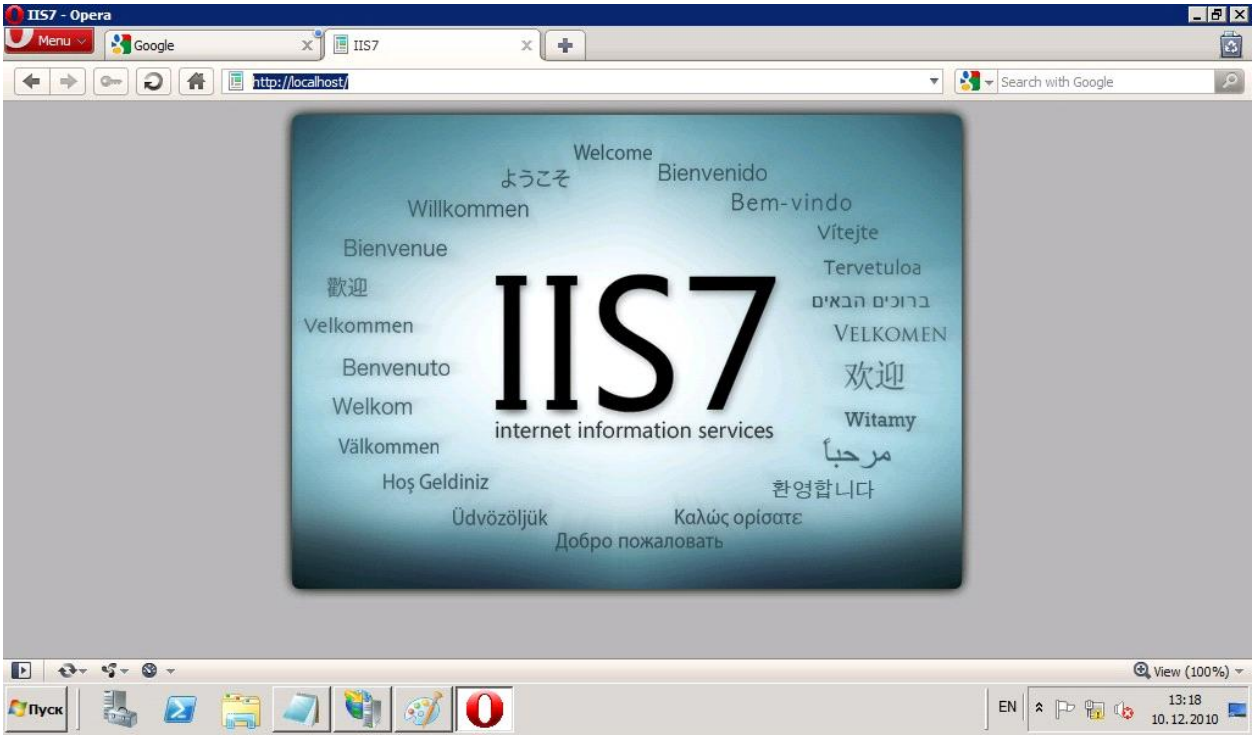
2) Настройка IIS сервера

Идем по адресу пуск - администрирование - диспетчер служб iis. Жмем кнопку начало, тем самым запускаем сервер.




для теста идем на localhost. (в браузере вводим строку http://localhost/) Если приветствие отобразилось, значит все действия выполнены верно и можно продолжать

работу.



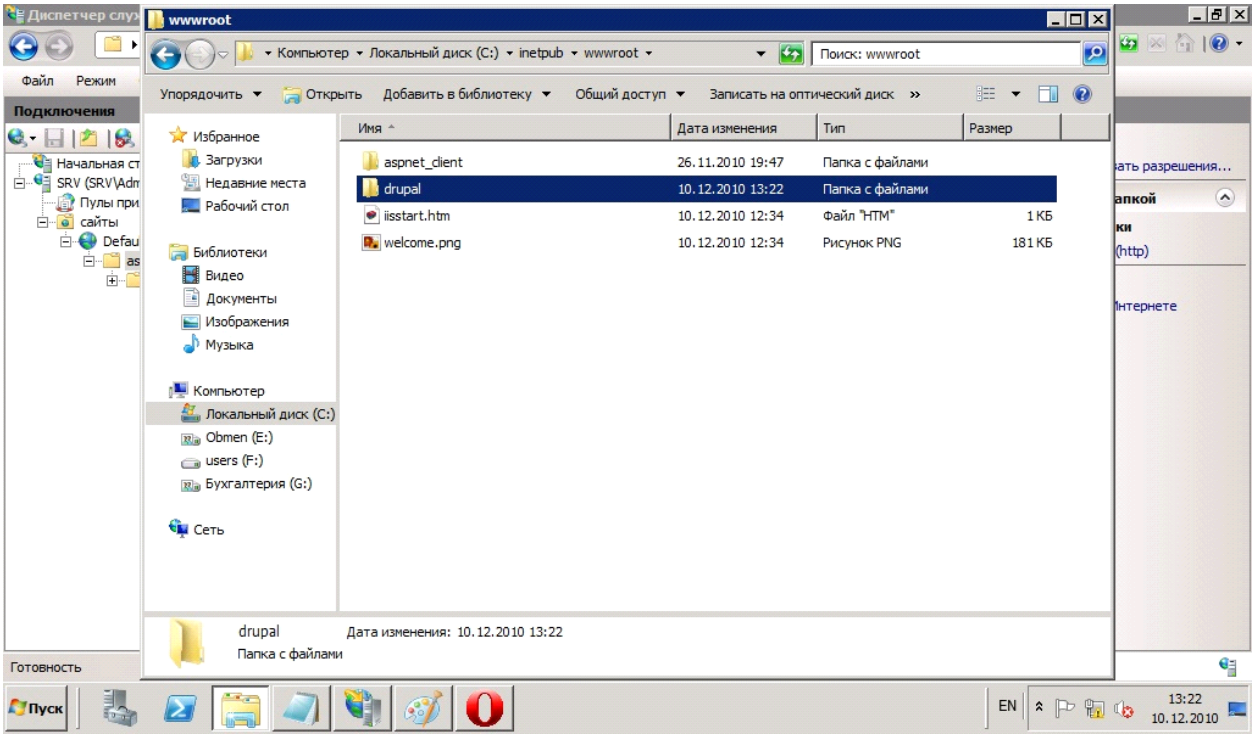

Далее возможны два варианта развития событий:

1) Ручная установка всех элементов IIS и ручная установка всех элементов cms. Этот вариант не рациональный, ведь нам нужно все сделать качественно, но в максимально сжатые сроки.

2) Мы можем воспользоваться автоматической установкой всех элементов. Как IIS, так и cms. Но все же рассмотрим оба метода.

**Ручная установка всех элементов.**

Готовим drupal для установки. качаем архив с официального сайта. Распаковываем. Создаем в папке iis каталог с названием вашего сайта, то есть путь будет выглядеть так: C:\inetpub\wwwroot и переносим все директории из распакованного архива в папку C:\inetpub\wwwroot\drupal



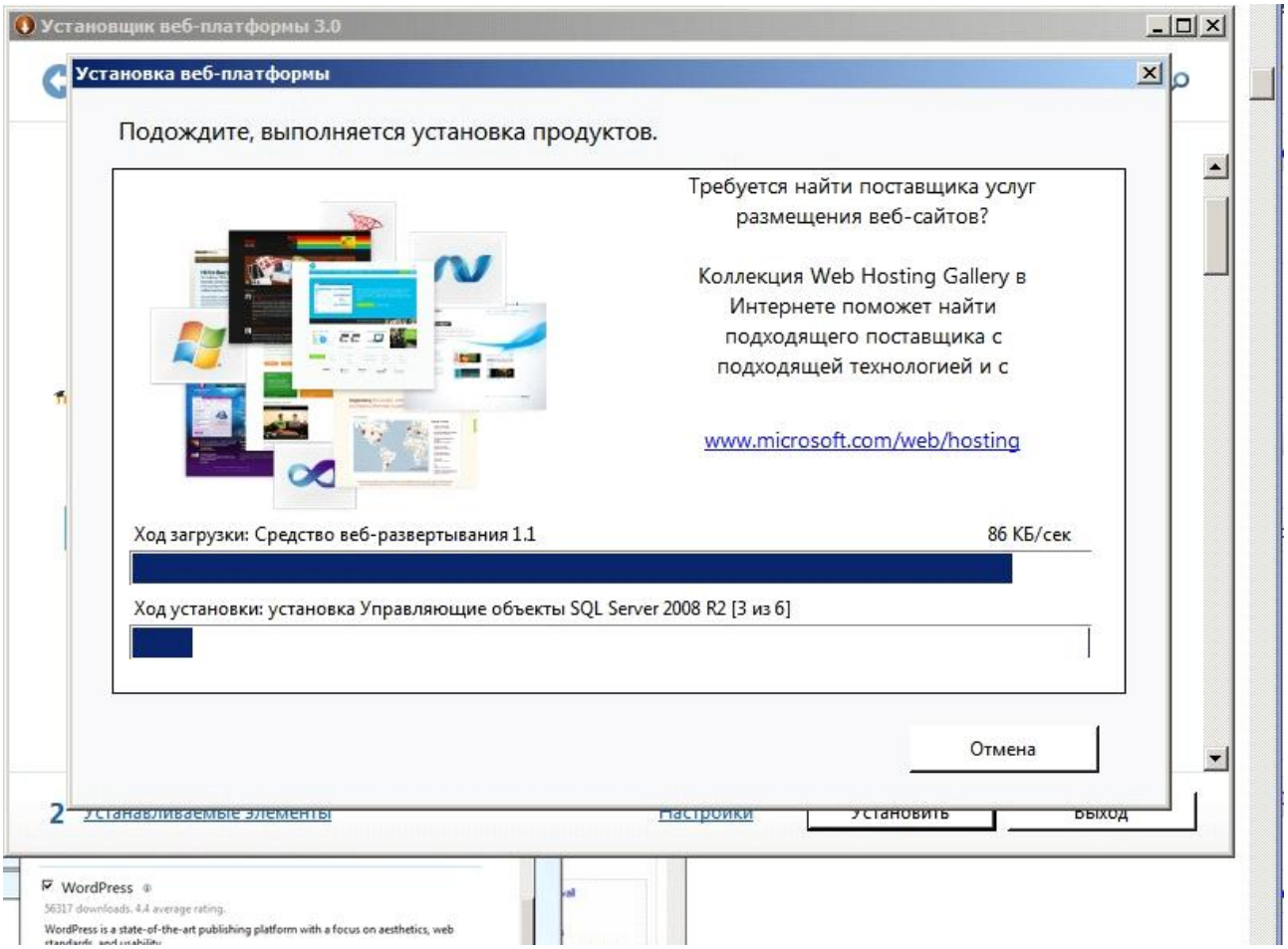

Установим php и mysql:

Заходим на сайт http://dev.mysql.com/downloads/mysql/ и качаем нужный для нашего сервера архив. В нашем случае для windows server 2008 r2 x64. Запускаем инсталлятор и следуем его действиям. Установка php. Для этого качаем инсталлятор по адресу http://windows.php.net/download/ и производим установку.

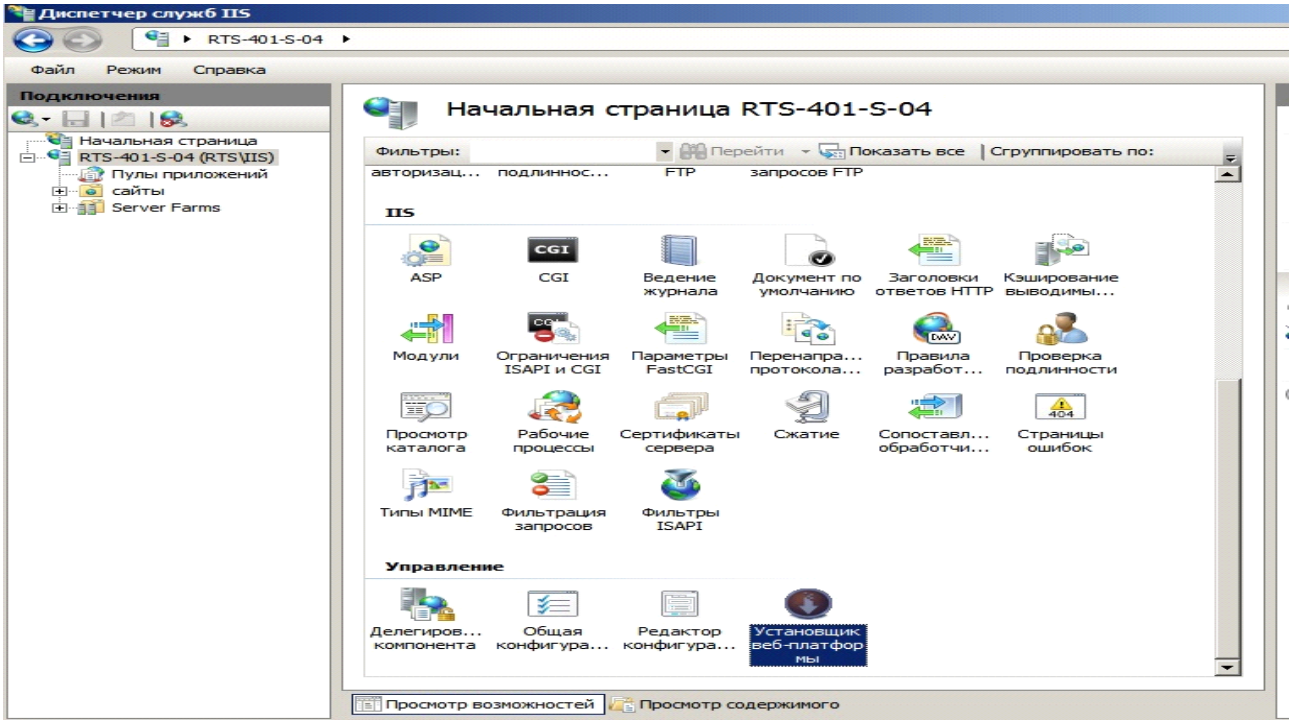
После этого мы идем по адресув браузере: http://localhost/drupal и видим, что нас перекинуло на экран установки cms!

**Автоматическая установка (рекомендуемый)**

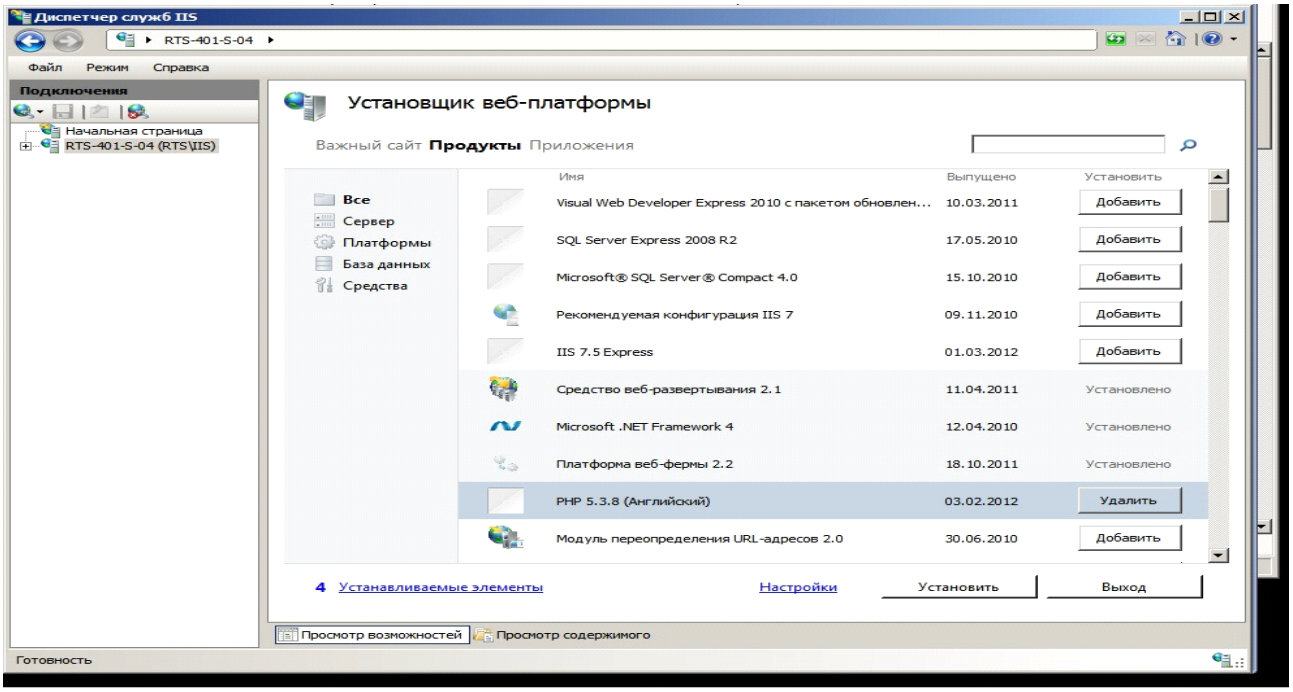
Для выполнения этой установки заходим в диспетчер служб iis и устанавливаем установщик веб-платформ.



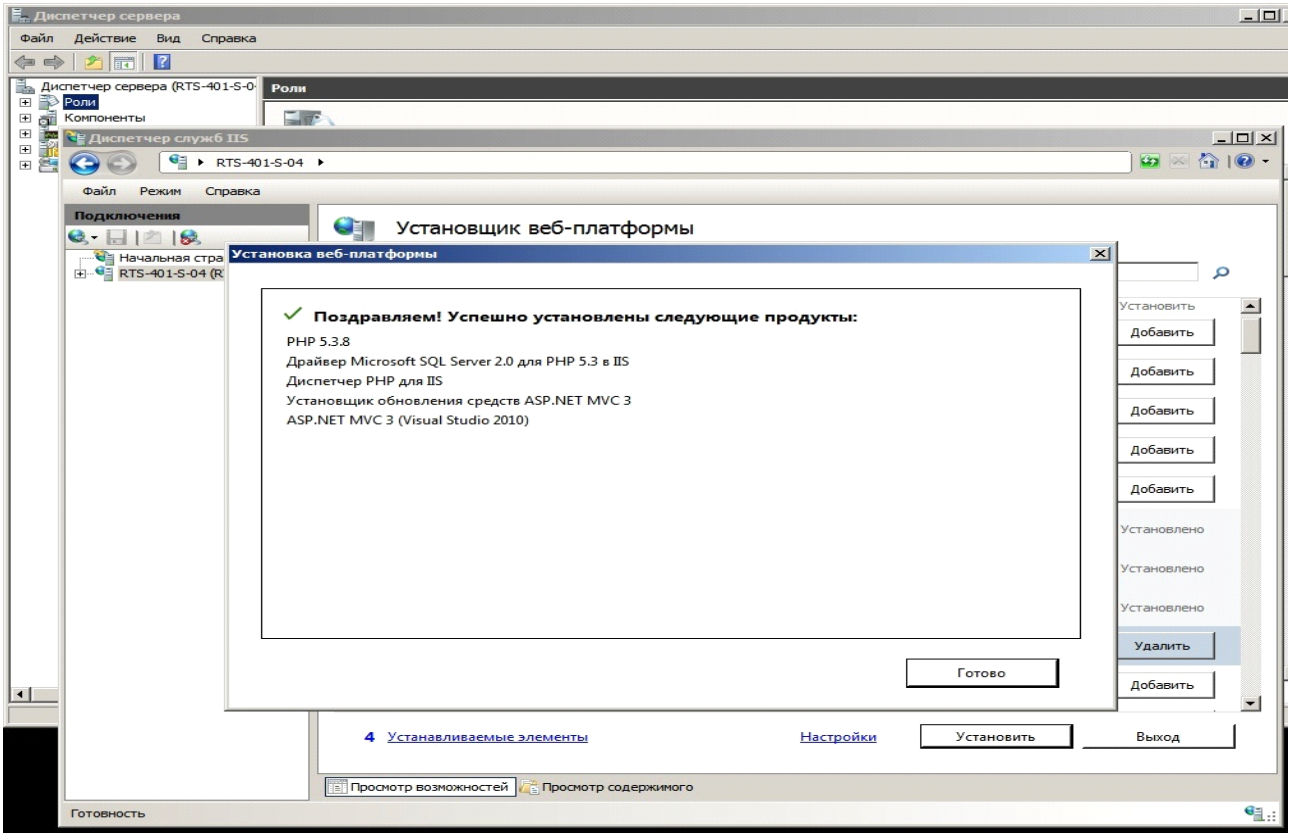

Выбираем закладку веб-платформа.



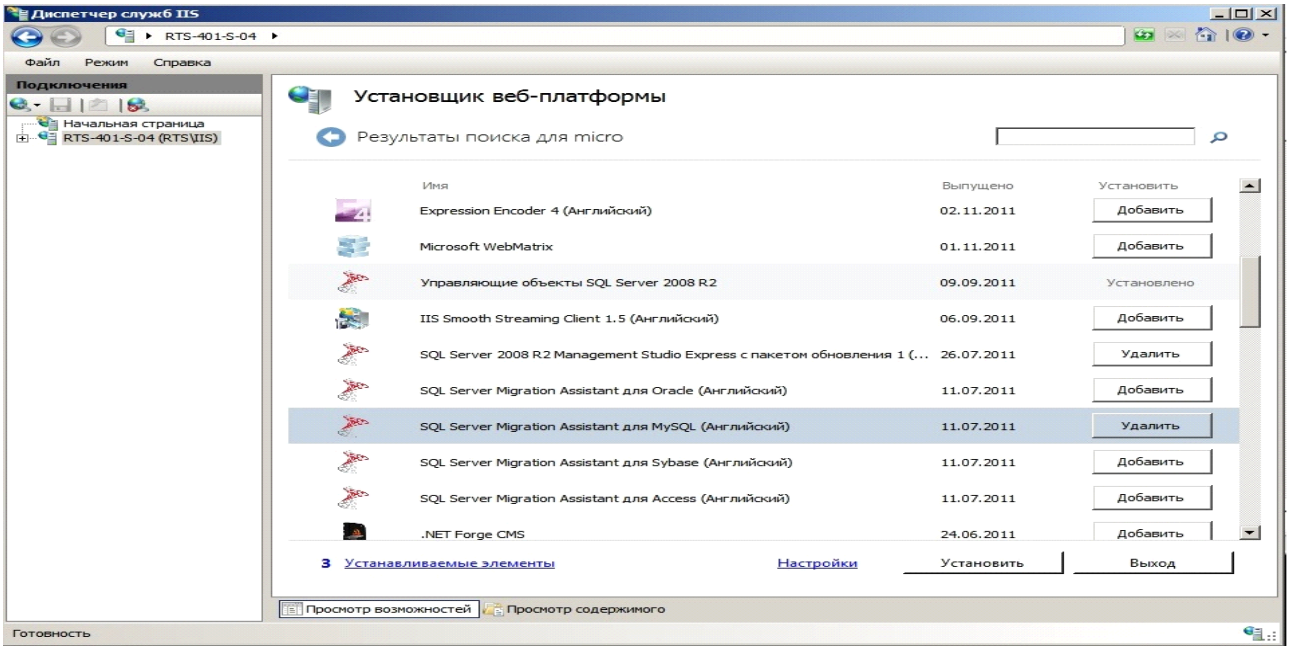

Отмечаем для установки продуктов ASP.NET, NET Framework 3.5, Microsoft.NET Framework 4, Windows Powershell 2.0, диспетчер PHP для IIS, PHP 5.2.13.



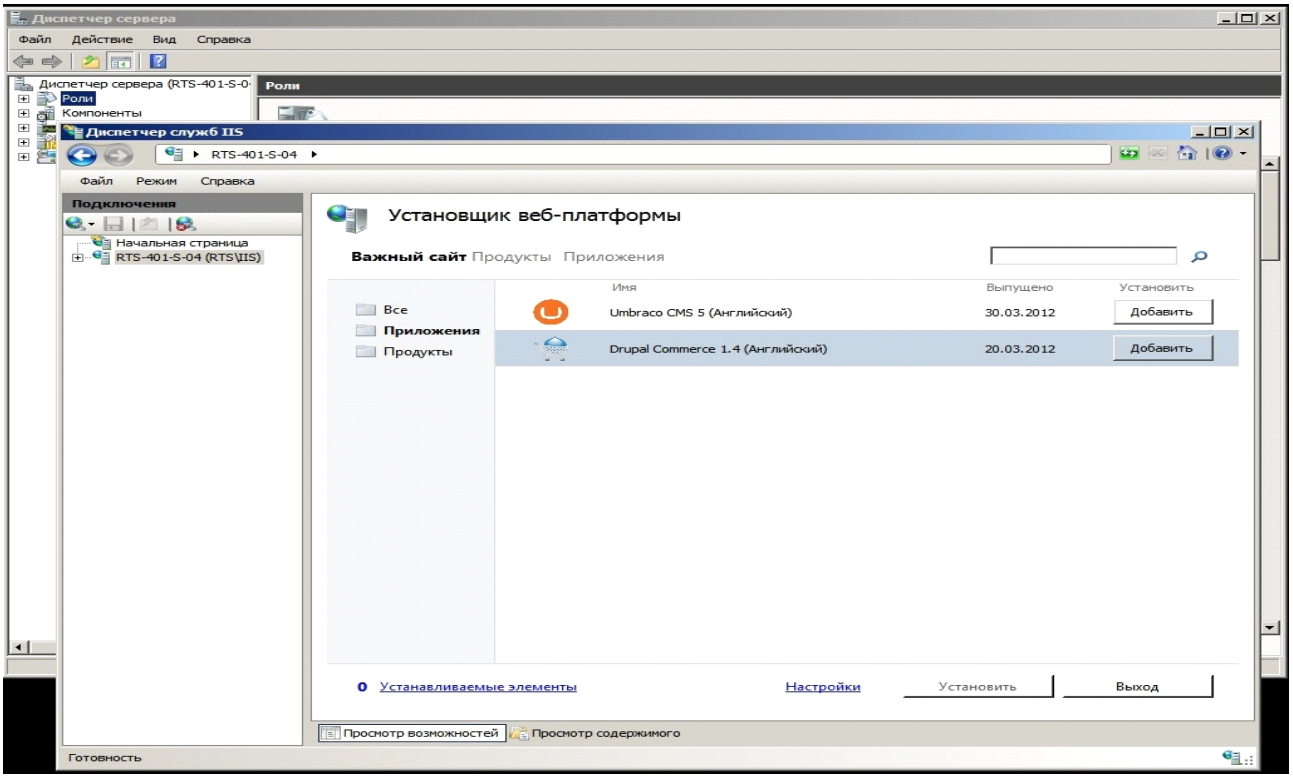

Жмем установить. Дожидаемся окончания установки.



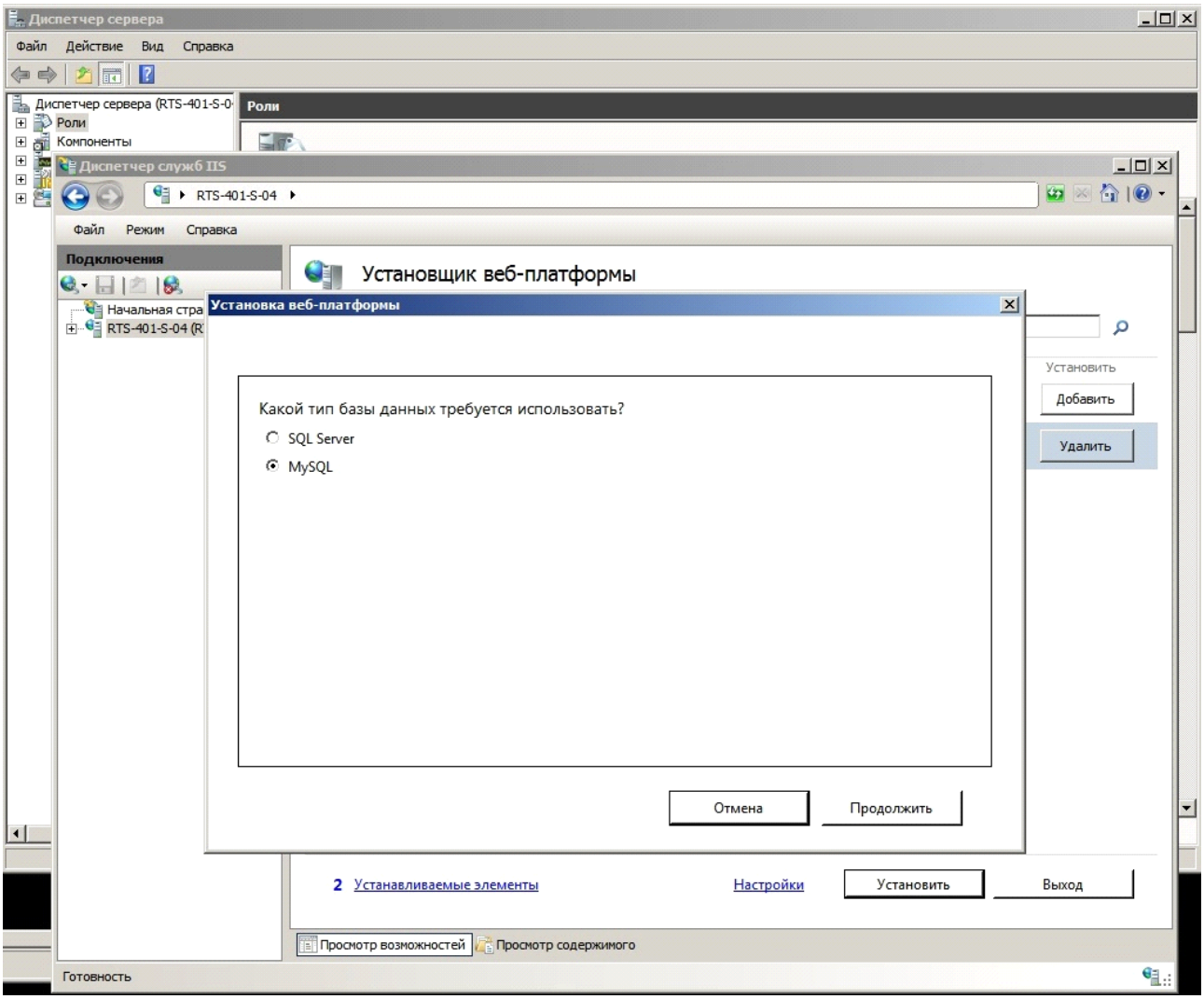

Заходим в установщик веб-приложений, выбираем драйвер SQL Server для PHP 2.0, SQL Server Express 2008 R2, SQL Server 2008 R2 Management Studio Express.



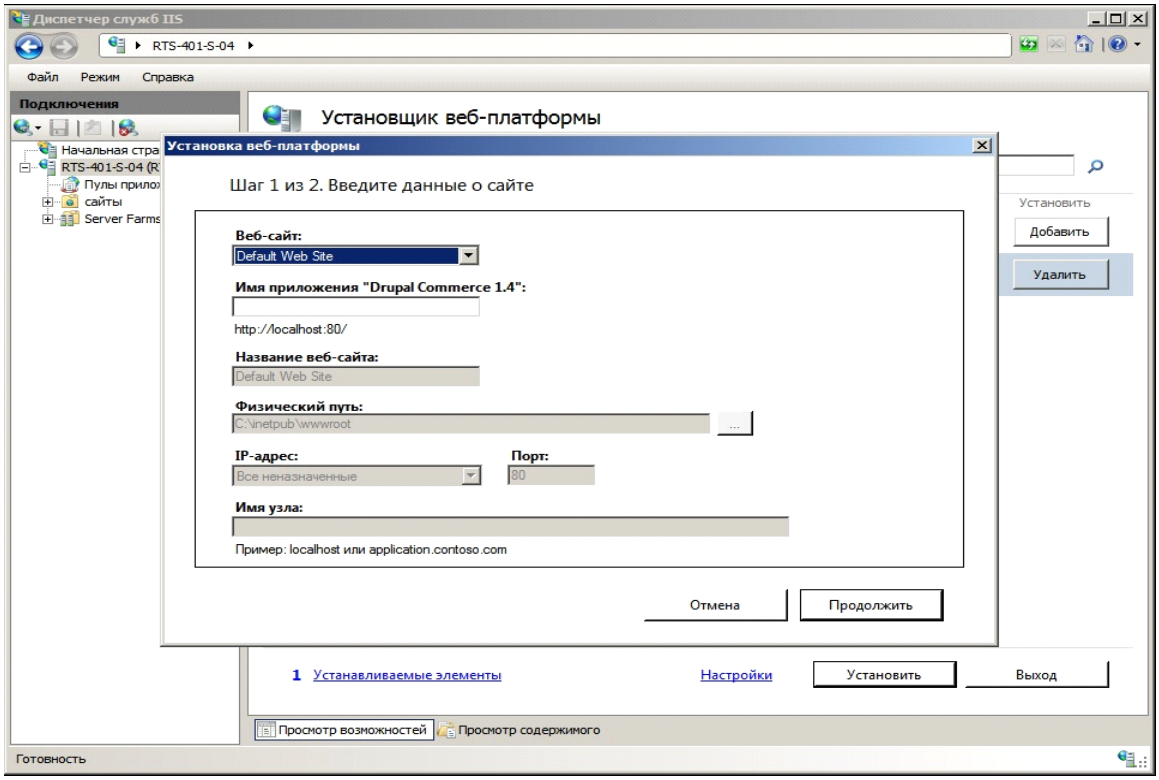

Теперь заходим снова ы установщик веб-платформ и выбираемпункт веб-приложения. Выбираем drupal и жмем установить.



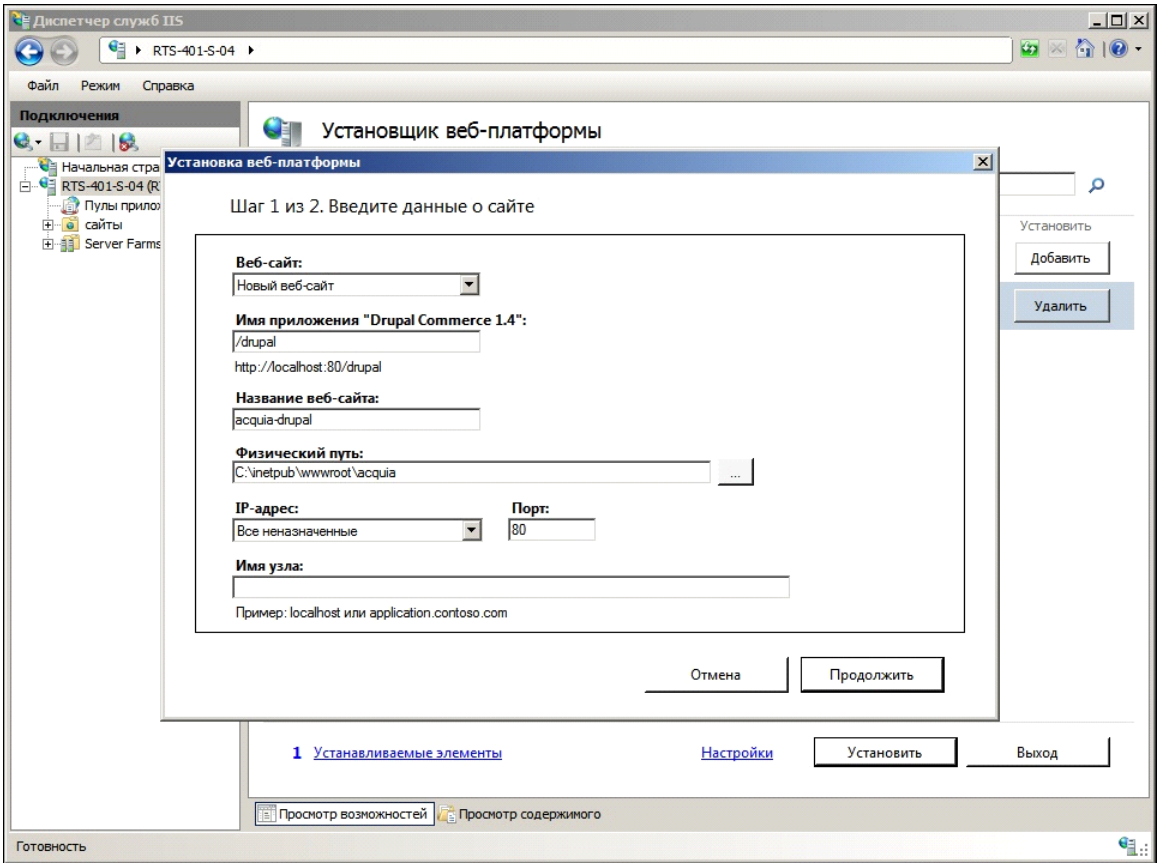

Видим запуск установки компонентов mySQL. Нам необходимо ввести пароль для администратора (пользователь root), используем пароль 12345.




Окно для ввода данных о сайте. Заполняем:

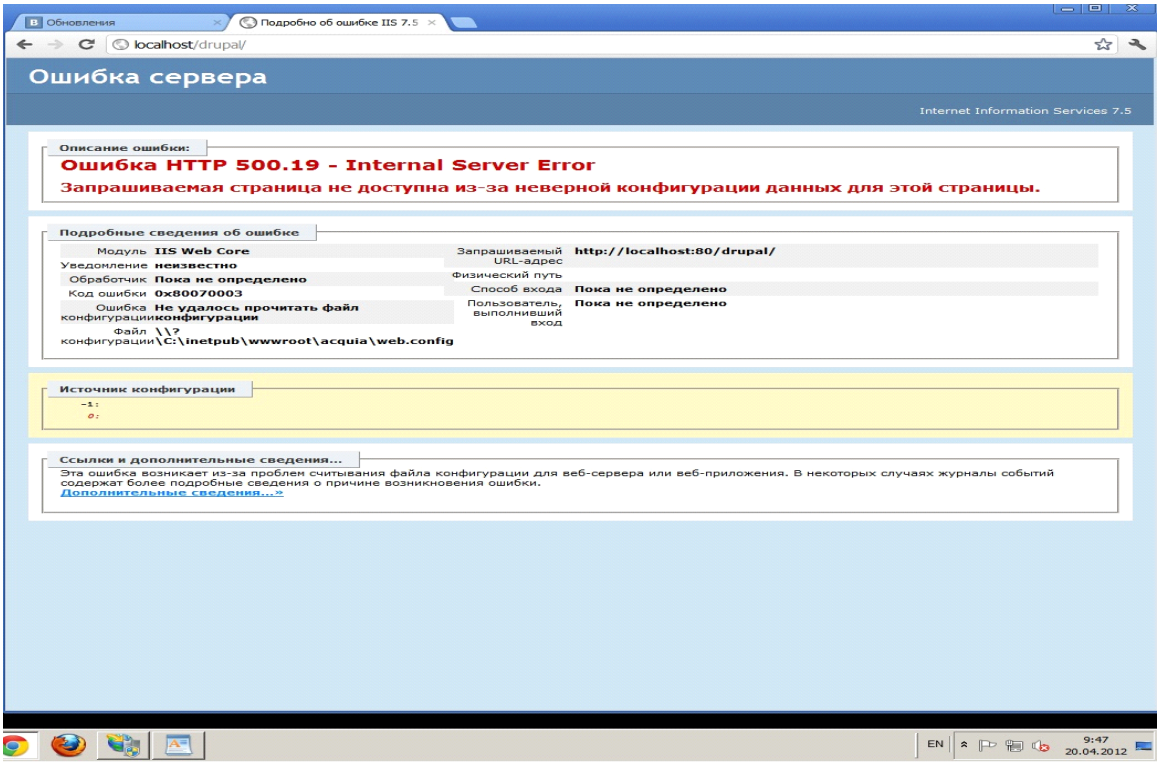



Приступаем ко второму шагу ввода данных о приложении (данные о базе данных):




Жмем далее и ждем завершения установки. Выводится на экран о не возможности завершения установки.

Запускается браузер, где видны частично установленные элементы.




Сайт доступен по адресу: http://localhost/drupal/

**Лабораторная работа №3: PGP кодирование и шифрование с открытым ключом**

## 1 Цель работы

Целью данной лабораторной работы является получение практических навыков по управлению ключами, шифрованию, расшифрованию, электронному подписанию документов/файлов и их безвозвратному удалению с диска посредством криптографической программы Pretty Good Privacy (PGP).

## 2 Методические указания

Все пользователи Интернета должны отчётливо понимать, что отправка обычного незашифрованного электронного послания аналогична отправке открытки почтой неэлектронной: такое сообщение может быть прочитано кем угодно и где угодно на участке между отправителем и получателем даже без всякой нужды осуществлять его целенаправленный перехват. Копия сообщения остаётся в кэше сервера вашего Интернет-провайдера, сетевые серверы у вас на работе, в университете или в Интернет-кафе, не говоря о бесплатных почтовых службах вроде mail.ru, также сохраняют копию, копии остаются на всех серверах, через которые сообщение проходит по пути к адресату. Системные администраторы этих серверов могут по своему желанию прочитать письмо и переслать его, кому захотят. Спецслужбы крупных государств в рабочем порядке сканируют электронную почту на предмет подозрительных ключевых слов и фраз. Деловые послания могут представлять интерес для ещё большего круга лиц – от конкурентов до организованной преступности – и ставки в этой игре оказываются гораздо выше.

С помощью PGP вы можете зашифровать сообщение для своего адресата, даже если никогда прежде с ним не общались. Все эти организации и люди смогут по-прежнему получить доступ к зашифрованному письму, но уже не будут иметь ни малейшего представления о его содержании, словно вы поместили его в непроницаемый конверт.

Pretty Good Privacy (буквально – "очень неплохая защита приватности"), свободно распространяемая криптографическая программа. Простая в использовании, PGP сегодня стоит на страже частной жизни миллионов пользователей Интернета.

PGP была придумана американским математиком и программистом Филипом Зиммерманом (Philip Zimmermann) в 1991 году. Получилась бесплатная программа для массового пользователя на основе алгоритма с открытым ключом. Она сразу стала набирать популярность. Правительство США пыталось бороться с распространением PGP (да и вообще стойкой гражданской криптографии). Зиммерману даже было предъявлено

обвинение в "незаконном экспорте вооружений". Но энтузиасты со всех стран мира уже вовсю размещали PGP у себя на сайтах, изучали код программы и переводили ее на другие языки. В конце концов власти махнули рукой на это дело, и сегодня PGP работает на миллионах компьютеров.

## 2.1 Основы

### 2.1.1 Интерфейс

PGP предоставляет пользователю ряд альтернативных путей для доступа функциям программы, выбор конкретного зависит от решаемой вами задачи.

Существует четыре способа, которыми вы можете добраться до нужных функций и компонентов программы:

- Иконка PGPtray.
- Контекстное меню Проводника Windows.
- Меню Пуск.
- Плагины в email-клиентах.

Наиболее удобный и часто используемый путь – это иконка PGPtray (  , в зависимости от версии Windows может быть либо золотой, либо серой), расположенная в системном трее – в правой части панели задач Windows рядом с системными часами (рисунок 2.1). Оттуда вы можете быстро произвести любые операции шифрования с содержимым буфера обмена или активного окна, например, email-клиента, текстового редактора или формы на интернет-сайте, получить доступ к меню настроек PGP или к любому из компонентов программы.

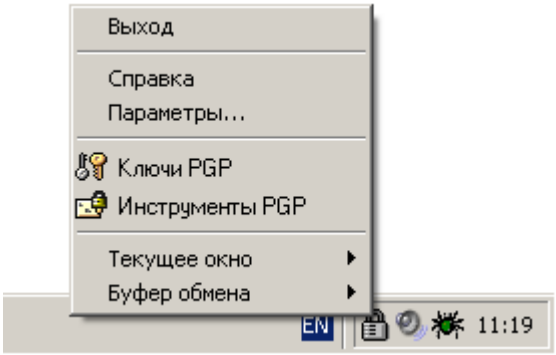



Рис. 2.1

Нажав на эту иконку, вам открывается следующее меню:

- *Выход* – скрыть иконку PGPtray.
- *Справка* – справочник по работе с программой.
- *Параметры* – меню настроек программы.

- *Ключи PGP* – позволяет быстро получить доступ к соответствующему компоненту программы.
- *Инструменты PGP* – предоставляет доступ к основным функциям шифрования, уничтожения файлов и очистки свободного пространства дисков.
- *Текущее окно* – операции с содержимым активного окна позволяют зашифровать, расшифровать, поставить или сверить электронную подпись с текстовой информации используемого в данный момент приложения (например, текстового редактора).
- *Буфер обмена* – аналогичные операции с содержимым буфера обмена позволяют, кроме перечисленного выше, быстро очистить или отредактировать находящийся в нём текст.

Вы можете воспользоваться средствами шифрования PGP из Проводника, нажав правой кнопкой на имя того или иного файла или папки, а затем в появившемся контекстном меню из пункта *PGP* выбрав нужную операцию (рисунок 2.2). Это весьма удобный способ работы с файлами.

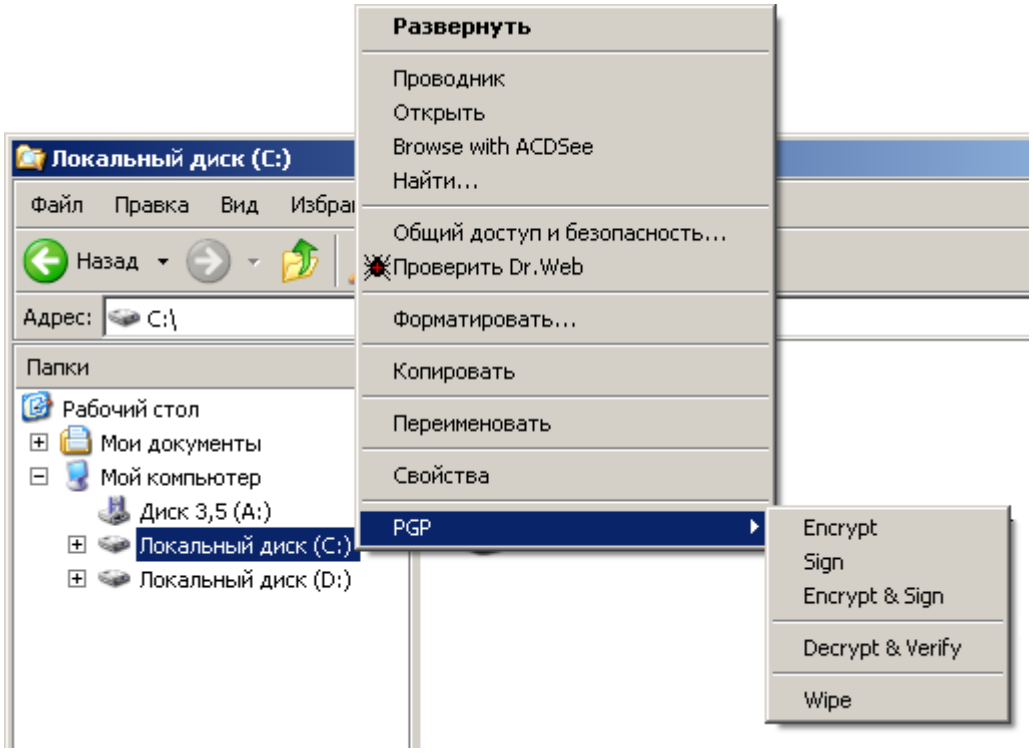



Рис. 2.2

Содержимое контекстного меню и список доступных функций напрямую зависят от выбранного объекта.

- **Для дисков и папок.** Нажав правой кнопкой на любой из накопителей или папку и выбрав в главном контекстном меню пункт *PGP*, вы можете сделать следующее:

- Зашифровать (*Encrypt*), расшифровать (*Decrypt*), поставить (*Sign*) или сверить (*Verify*) электронные подписи с содержащихся на диске / в папке файлов.

- Удалить файлы с диска или папку со всем ее содержимым (*Wipe*).

• **Для файлов.** Нажав правой кнопкой на файл и выбрав в главном контекстном меню пункт *PGP*, в зависимости от типа файла вы можете сделать следующее:

- Если выбран любой незашифрованый файл, вы можете уничтожить его (*Wipe*), зашифровать (*Encrypt*), подписать (*Sign*).

- Если выбран зашифрованный / подписанный файл, вы можете уничтожить его (*Wipe*) или расшифровать / сверить подпись (*Decrypt* & *Verify*).

- Если выбран файл в ASCII-формате (*.asc), вы можете уничтожить его (*Wipe*) или расшифровать / сверить подпись (*Decrypt* & *Verify*). При выборе последнего варианта для файла, содержащего материал ключа, вам будет предложено импортировать его на свою связку.

- Если выбран файл связки открытых или закрытых ключей (*.pkr или *.skr соответственно), вы можете уничтожить его (*Wipe*) или импортировать содержащиеся в нём ключи на свою связку.

### 2.1.2 Компоненты PGP

Основными компонентами PGP являются ключи PGP (PGPkeys) и инструменты PGP (PGPtools).

Менеджер PGPkeys имеет средства управления вашими парами открытых и закрытых ключей, а также открытыми ключами ваших корреспондентов (рисунок 2.3).

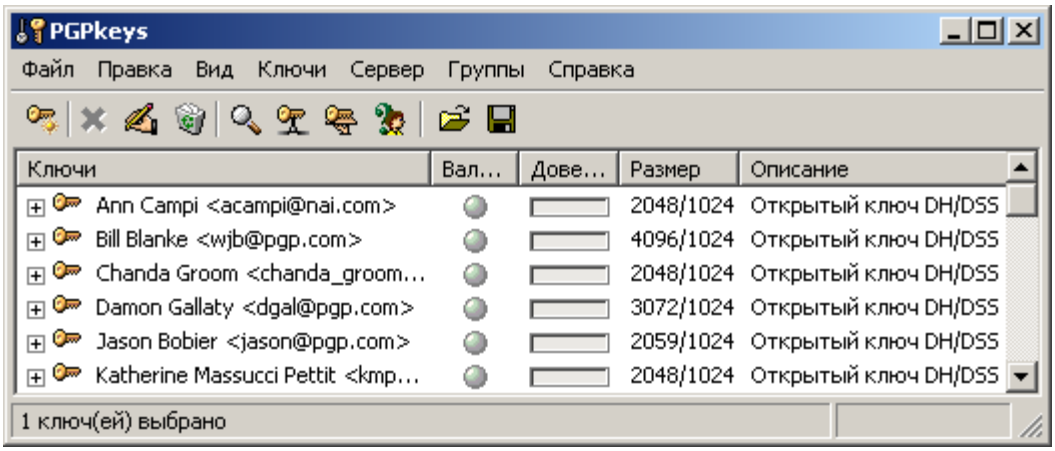



Рис. 2.3

Чтобы открыть компонент PGPkeys:

1. нажмите иконку PGPtray ( );
2. из меню выберите *Ключи PGP*.

PGPtools – это небольшое плавающее окошко, предоставляющее доступ к основным функциям шифрования, уничтожения файлов и очистки свободного пространства дисков (рисунок 2.4).


Рис. 2. 4

Чтобы открыть компонент PGPtools:

1. нажмите иконку PGPtray ( );
2. из меню выберите *PGPtools*.

### 2.1.2 Настройка

Изначальная настройка PGP пригодна для большинства пользователей. Тем не менее, предпочтительно перенастроить программу под специфику ваших условий и нужд до начала её эксплуатации. Ниже приведено описание всех опций настройки программы и рекомендации, могущие помочь в выборе конкретного варианта. Если сомневаетесь, какой вариант выбрать, опирайтесь на здоровую параною: чуть более строгие меры безопасности не доставят много дискомфорта, но помогут надёжнее сберечь информацию.

Будьте очень внимательны: некорректная настройка способна сильно повлиять на функциональность и безопасность работы программы.

Открыть меню настроек программы можно двумя разными способами:

- Нажать иконку PGPtray ( ) > *Параметры*.
- В окне любого компонента PGP в строке меню выбрать *Правка* > *Настройки*.

#### 2.1.2.1 Общие

Вкладка *Общие* содержит основные настройки PGP, связанные с общим функционированием программы (рисунок 2.5).

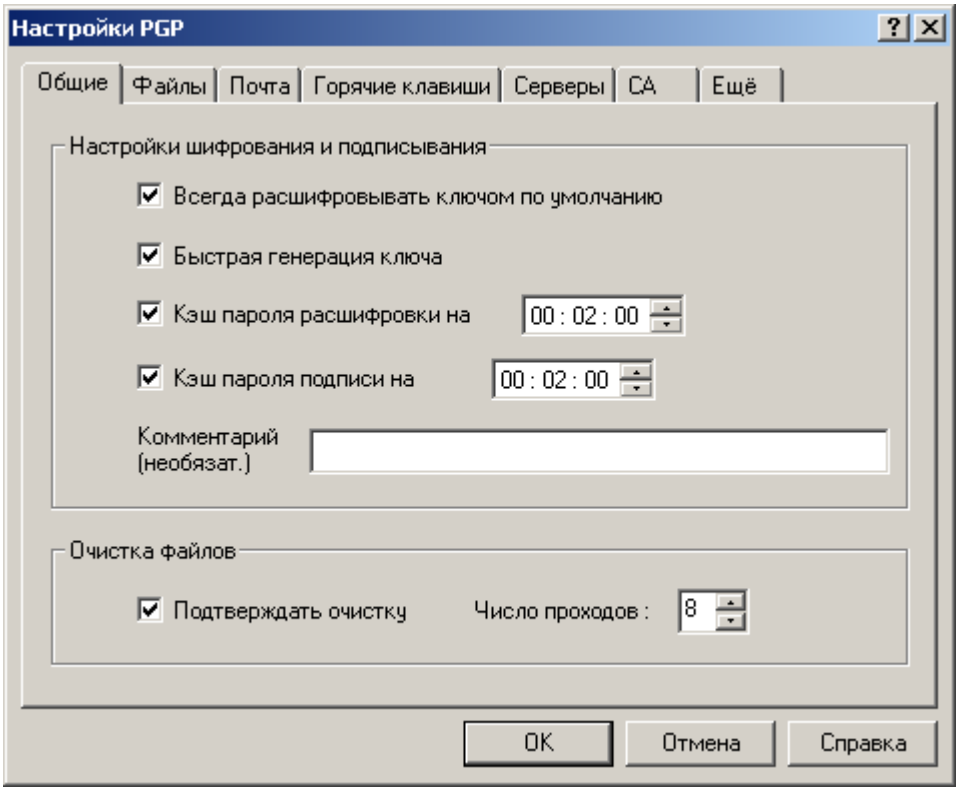



Рис. 2.5

**Раздел Настройки шифрования и подписывания**

- *Всегда расшифровывать ключом по умолчанию.*
- *Быстрая генерация ключа* – быстрая генерация ключей Diffie-Hellman / DSS. При включении данной опции, программа будет в несколько раз быстрее создавать ключи DH/DSS, используя набор предварительно расчитанного математического материала, ложащегося в их основу, вместо его вычисления с нуля. Учтите, эта опция имеет значение только для генерации ключей DH/DSS, но не для RSA вследствие особенностей самих алгоритмов. Считается, что знание этого предрассчитанного материала не даёт взломщику преимуществ для осуществления атаки на ключи DH/DSS, и включение опции не несёт ущерба безопасности; но если вам от этого всё равно неуютно, можете эту опцию отключить, что и рекомендуется сделать, если вы не планируете генерировать очень много ключевых пар (чего, как правило, не требуется).
- *Комментарий* – сюда можно вписать короткий комментарий, который будет отображаться во всех зашифрованных или подписанных вами сообщениях в поле *Comment* после служебного заголовка *BEGIN PGP MESSAGE* или *BEGIN PGP SIGNATURE*. Комментарий никак не влияет на безопасность и сам может быть любым образом изменён вами или посторонним уже в зашифрованном или подписанном сообщении, поскольку не входит в сообщение, а является только служебным блоком данных. Для этой опции рекомендации отсутствуют: пишите или не пишите на своё усмотрение.

- *Кэш пароля расшифровки/подписи на …* Если вы покинете рабочее место не перезагрузив компьютер или не очистив кэш, любой посторонний человек сможет беспрепятственно расшифровать ваши файлы и подделать подпись! В этом режиме программа будет хранить введённую ключевую фразу в памяти только указанный здесь срок. Это удобно, когда нужно расшифровать / подписать сразу несколько файлов, но не хочется несколько раз подряд вводить длинную ключевую фразу.

### Раздел Очистка файлов

Здесь можно настроить параметры уничтожения файлов (удаления без возможности восстановления).

- *Число подходов* – количество проходов очистки определяет, сколько раз сектора диска, содержавшие удаляемый файл, будут перезаписаны случайными данными. Обычно достаточно 3 (столько, например, предусматривает инструкция Минобороны США 5220.22). Для крайне ценных файлов увеличьте параметр до 9-12. Большее число проходов повышает надёжность уничтожения данных и снижает риск их намеренного восстановления, но и делает процесс стирания крайне долгим. Рекомендации таковы:
  - 1-3 прохода – для использования на домашнем компьютере;
  - 10-12 проходов – для использования в коммерческой и бизнес-сфере;
  - 16-18 проходов – для использования в военной сфере;
  - 26-28 проходов – для максимальной надёжности (может потребовать вплоть до нескольких часов работы для удаления достаточно крупного файла).

Коммерческие фирмы, специализирующиеся на восстановлении информации, могут восстановить данные, которые были перезаписаны примерно до девяти раз. Но вы должны учесть, что если ваша информация представляет чрезвычайную ценность (вероятно, ценность государственного масштаба), даже максимальное число проходов не обеспечит должного уровня надёжности. Питер Гутман, разработавший методику стирания информации, реализованную в PGP, рекомендует один достаточно надёжный способ уничтожения столь ценных данных: сжечь носитель информации, пепел растереть в порошок и развеять по ветру.

- *Подтверждать очистку* – если включить, PGP будет выдавать предупреждение перед уничтожением файлов с просьбой подтвердить ваши намерения – последний шанс передумать. Рекомендую включить, поскольку специально или случайно уничтоженные данные будет исключительно трудно восстановить не только злоумышленнику, но и вам самим.

### 2.1.2.2 Файлы

Вкладка *Файлы* содержит местоположение связок ключей и пула случайных чисел (рисунок 2.6).

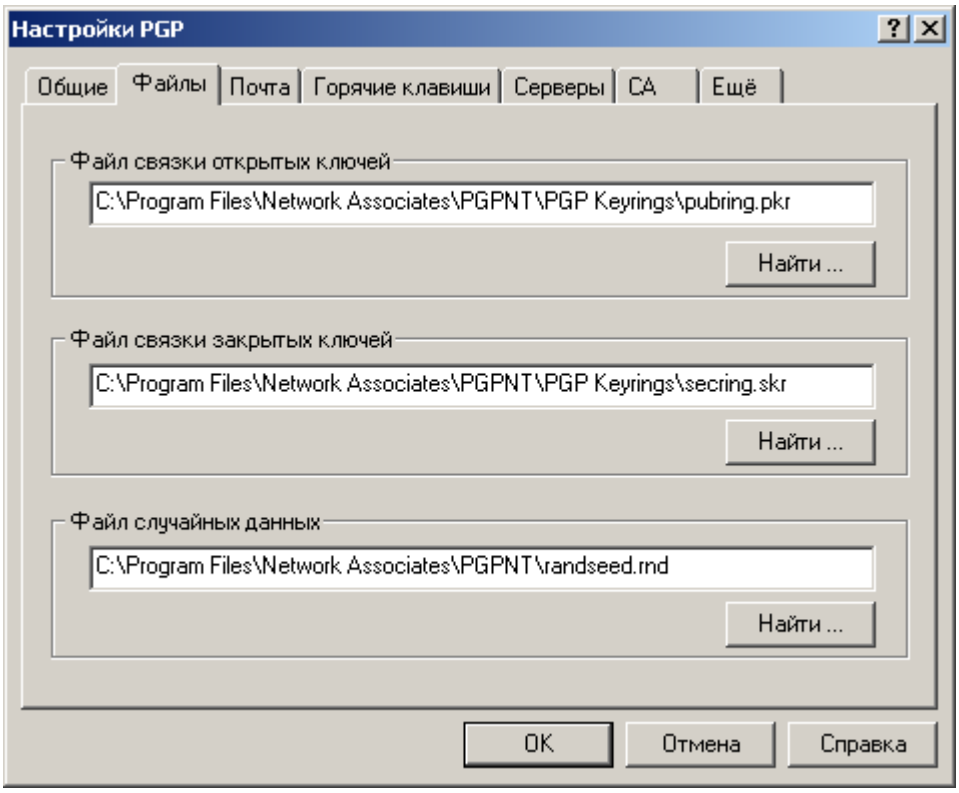



Рис. 2.6

Раздел “Файл связки открытых ключей” указывает директорию и файл, где находится ваша связка открытых ключей; именно на ней хранятся ваши открытые ключи и открытые ключи всех ваших корреспондентов. Если необходимо, переместите файл в каталог, где он не будет случайно удалён вами или кем-то посторонним. В то же время не стоит помещать файл на внешний носитель, тем более на CDR-диск, поскольку для редактирования, добавления новых и удаления ненужных ключей файл должен быть доступен для записи.

Раздел “Файл связки закрытых ключей” указывает директорию и файл, где находится связка ваших закрытых ключей. ВНИМАНИЕ: удаление или порча этого файла приведёт к фактической потере всей зашифрованной информации! Крайне желательно переместить закрытые ключи на аппаратное криптографическое устройство (смарт-карту или USB-токен) либо всю связку – на внешний носитель, скажем, дискету, ZIP или CD-RW диск: в этом случае, во-первых, будет снижен риск случайного или злонамеренного удаления файла и, во-вторых, все закрытые ключи всегда будут под вашим физическим контролем (при условии надёжного хранения носителя), и могут быть использованы как обыкновенный ключ от

дверного замка: подключаете к компьютеру, расшифровываете / подписываете что-либо, отключаете от компьютера и прячете.

В разделе “Файл случайных данных” указан путь к файлу с пулом псевдослучайных чисел, используемых программой для генерации сеансовых ключей и другого криптографического материала. Этот файл не содержит сколь-нибудь ценных данных, он лишь накапливает показатели энтропии. Чтобы воспользоваться этими показателями для проведения атаки на шифртекст, взломщику по меньшей мере придётся взломать гамма-генератор, обновляющий содержимое этого файла. Всё же стоит разместить его на логическом диске в оперативной памяти компьютера, дабы он (файл, а не компьютер) уничтожался при каждой перезагрузке.

#### 2.1.2.3 Электронная почта

Вкладка *Почта* содержит настройки интеграции с почтовым клиентом (рисунок 2.7).

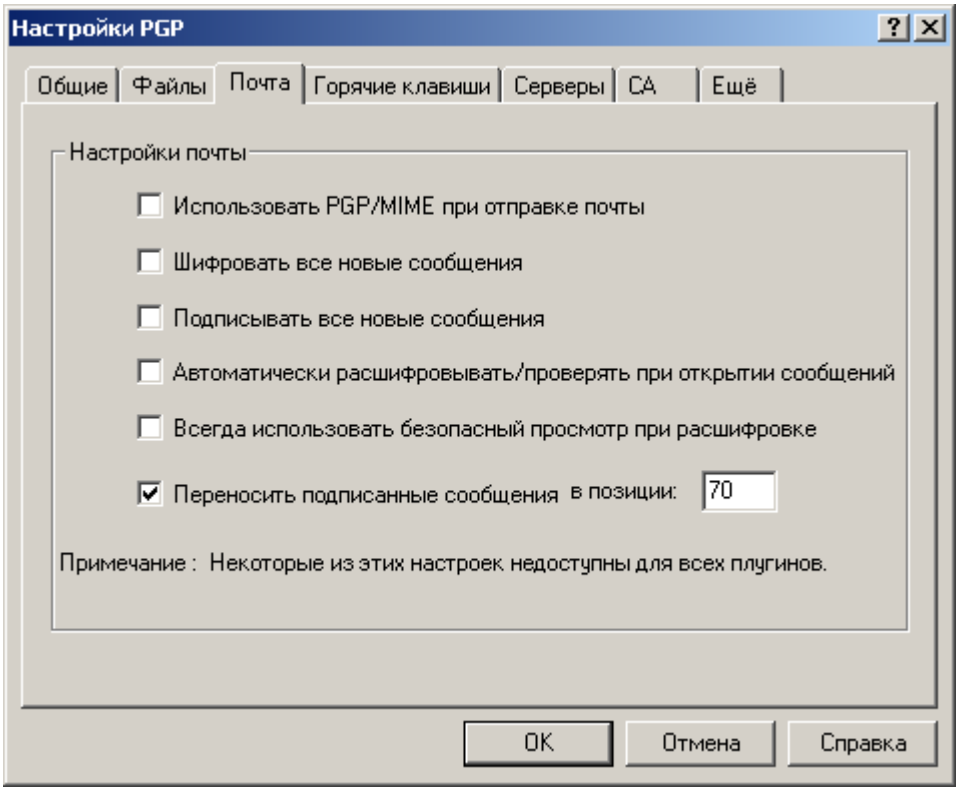



Рис. 2.7

Если наряду с PGP вы установили плагин для интеграции с почтовым клиентом, здесь можно настроить некоторые параметры обработки почты. Не все из этих опций поддерживаются каждой почтовой программой. Кроме того, перед включением той или иной опции убедитесь, что и почтовая программа получателя также её поддерживает.

- *Использовать PGP/MIME при отправке почты* – если вы и ваши корреспонденты используете email-клиент Qualcomm Eudora, включение этой опции позволит PGP автоматически зашифровывать всё содержимое письма (включая вложенные файлы и т.д.) и отправлять его в особом MIME-формате OpenPGP. Получателю нужно будет только нажать на ярлычок в пришедшем сообщении, и оно расшифруется с сохранением оригинального форматирования и всяческих украшательств в виде картинок и HTML-шаблонов. Данная опция (как для отправки, так и для получения) поддерживается только email-клиентом Qualcomm Eudora! Если вы не уверены в обратном, рекомендую отключить.
- *Шифровать все новые сообщения* – автоматически зашифровывать сообщения перед отправкой открытым ключом получателя. Поддерживается всеми email-клиентами. Если вам приходится часто пересылать зашифрованную корреспонденцию, лучше включить.
- *Подписывать все новые сообщения* – автоматически подписывать сообщения перед отправкой. Поддерживается всеми email-клиентами. Рекомендация аналогична предыдущей.
- *Автоматически расшифровывать / проверять при открытии сообщения* – автоматически расшифровывать / сверять подписи с открываемых сообщений. Поддерживается большинством email-клиентов.
- *Всегда использовать безопасный просмотр при расшифровке* – если включить, то любой расшифрованный текст (не только письма) будет выводиться в специальном окне *Secure Viewer*, используя шрифт, предотвращающий так называемую TEMPEST-атаку (удалённый съём информации по электромагнитному излучению монитора); кроме того, в этом случае сообщение невозможно будет сохранить в виде открытого текста. Для большинства случаев эту опцию лучше отключить (ещё и потому, что этот поставляемый с PGP TEMPEST-защитный шрифт не имеет кириллических символов).
- *Переносить подписанные сообщения в позиции ...* – производить на указанном символе в строчке жёсткий перенос (возврат каретки). Не меняйте установленное по умолчанию 70, если твёрдо не уверены, что в вашей почтовой программе используется меньший показатель, в противном случае сделайте эту цифру ниже, иначе ваш email-клиент, отформатировав текст перед отправкой, повредит цифровую подпись и шифртекст.

#### 2.1.2.4 Горячие клавиши

Вкладка *Горячие клавиши* содержит настройки клавиш быстрого доступа к функциям PGP (рисунок 2.8).

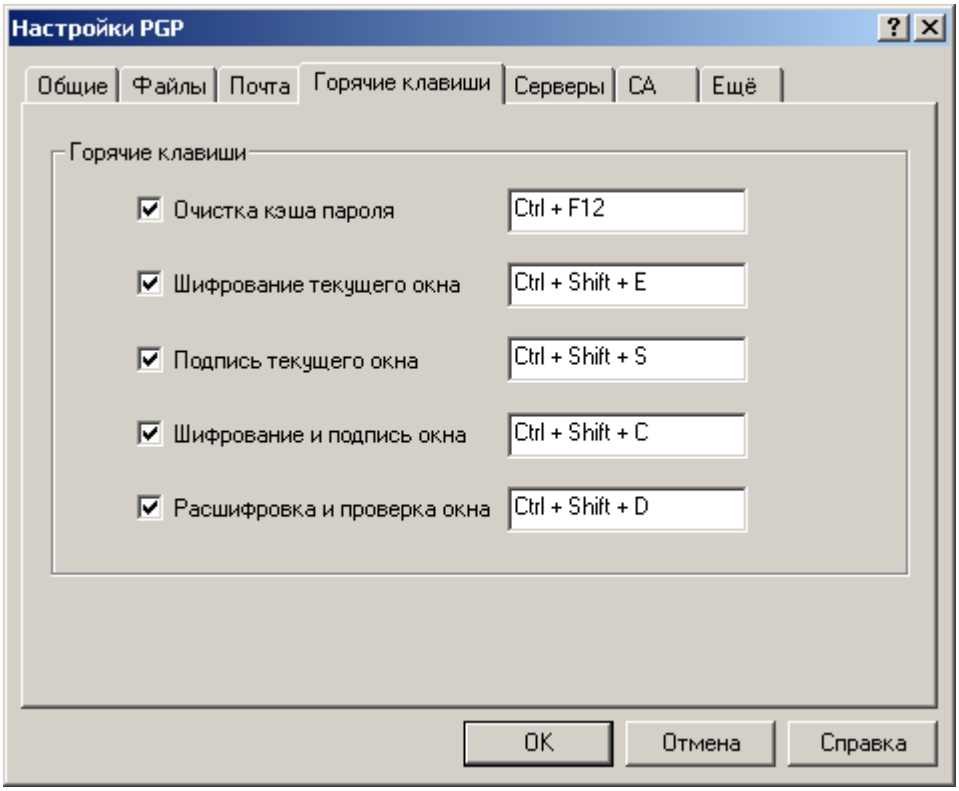



Рис. 2.8

Здесь можно указать комбинации клавиш для быстрого выполнения тех или иных основных операций: шифрования, подписания и пр.

- *Очистка кэша пароля* – быстрая очистка кэша от ключевых фраз. Если вы включили режим кэширования ключевых фраз, обязательно нажимайте эту комбинацию клавиш, когда отлучаетесь от компьютера.
- *Шифрование текущего окна* – зашифровать содержимое активного окна.
- *Подпись текущего окна* – подписать содержимое активного окна.
- *Шифрование и подпись окна* – зашифровать и подписать содержимое активного окна.
- *Расшифровка и проверка окна* – расшифровать / сверить подпись с содержимого активного окна.

### 2.1.2.5 Серверы

Вкладка *Серверы* содержит настройки списка серверов-депозитариев (рисунок 2.9).

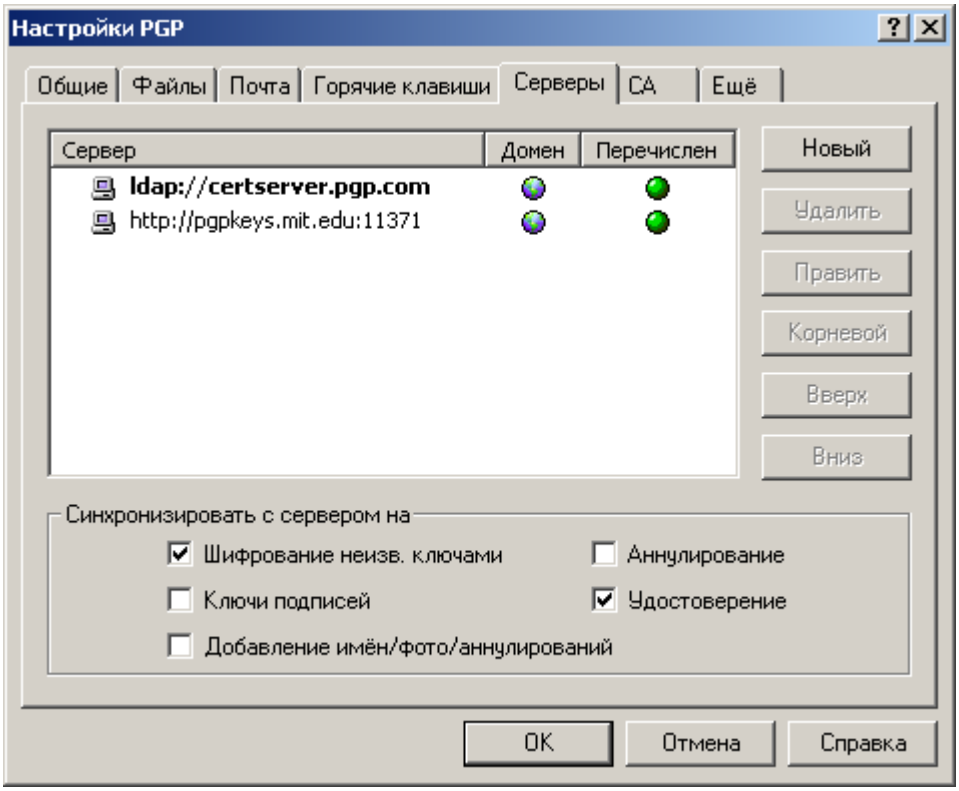



Рис. 2.9

Кнопки справа от списка серверов позволяют вносить в него следующие изменения:

- *Новый* – добавить в список новый сервер-депозитарий.
- *Удалить* – удалить из списка указанный сервер.
- *Править* – редактировать параметры выделенного сервера.
- *Корневой* – сделать выбранный сервер корневым (или доменным). В корпоративной среде таковой используется для специфических задач, в частности, для обновления списков рассылки, настроек программы, доверенных поручителей и т.д. Для частных пользователей эта опция не представляет ценности.
- *Вверх* и *Вниз* – сдвинуть сервер в списке вверх или вниз. Поиск ключей на серверах в ходе синхронизации происходит в приоритетном порядке: если ключ не найден на первом сервере, производится поиск на втором и т.д. Поэтому крупные общественные серверы-депозитарии (как ldap://certserver.pgp.com) лучше оставить на самом верху.

Настройки в разделе “Синхронизировать с сервером на” позволяют указать, в каких случаях будет производиться синхронизация ключей с серверами. Желательно включить их все.

- *Шифрование неизв. ключами* – если включить, при отправке электронного письма человеку, открытого ключа которого нет на вашей связке, PGP попытается подключиться к депозитарию и самостоятельно найти ключ по email-адресу получателя. (Только при использовании почтового плагина.)

- *Ключи подписей* – если включить, при подписании чужого открытого ключа PGP сначала обновит его с сервера, а затем отправит на сервер подписанную вами копию.
- *Добавление имен / фото / аннулирований* – аналогично предыдущей опции, если вы внесёте в сертификат своего ключа новую запись (имя или фото) либо добавите т.н. "отменителя", PGP обновит ключ с сервера, а затем загрузит на сервер внесённые вами изменения.
- *Аннулирование* – после аннулирования открытого ключа PGP синхронизирует его с сервером, дабы в дальнейшем ваши корреспонденты не могли его применять.
- *Удостоверене* – если сверяете с сообщения или файла чужую ЭЦП, к которой на вашей связке не может быть найден подходящий открытый ключ, PGP попытается связаться с сервером и найти ключ по номеру ID.

#### 2.1.2.6 Центр сертификации

Вкладка *CA* (*Certificate Authority*) содержит настройки установки соединения с Центром сертификации (ЦС) и объединения с инфраструктурой PKI. В основном эта функция применяется в корпоративной среде с развёрнутой PKI, основанной на стандарте X.509. Для частных пользователей она может не представлять интереса.

#### 2.1.2.7 Дополнительные

Вкладка *Еще* содержит расширенные настройки PGP (рисунок 2.10).

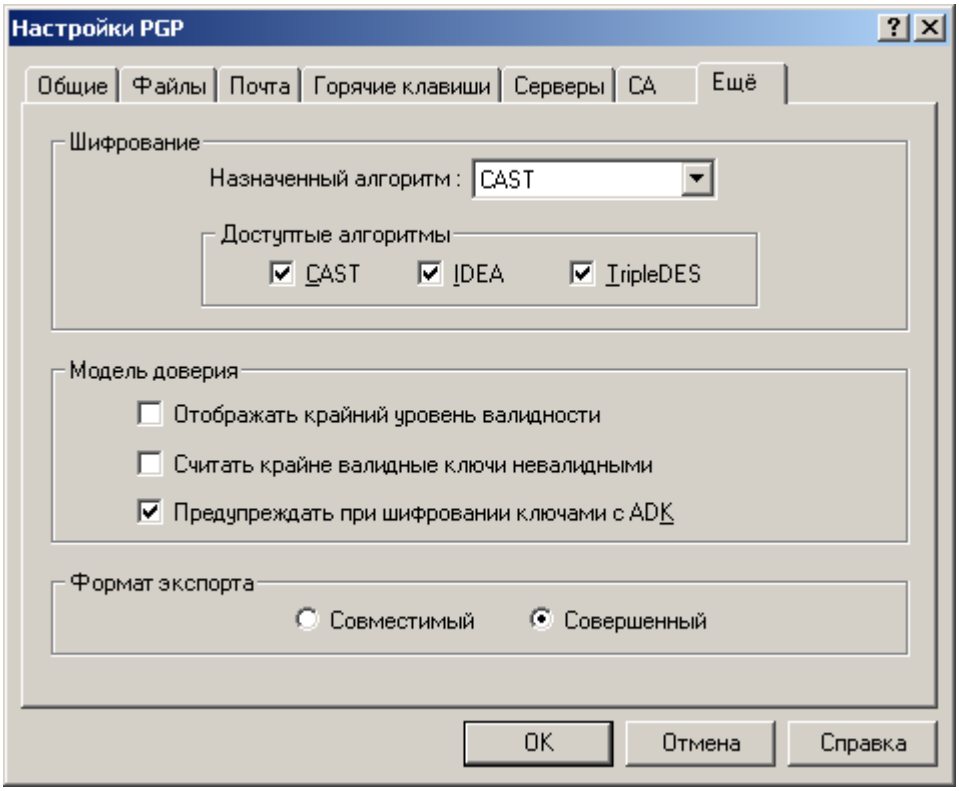



Рис. 2.10

**Раздел Шифрование**

Настройки используемых шифровальных алгоритмов. Учтите, выбранные здесь настройки ложатся в материал генерируемых вами ключей, поэтому для уже существующих ключевых пар вы не обнаружите никаких изменений.

- *Назначенный алгоритм* – предпочтительный алгоритм симметричного шифрования. Следующая сгенерированная вами ключевая пара будет предпочтительно использовать указанный здесь блочный шифр. Иными словами, программа PGP отправителя зашифрует сообщение, предназначенное вам, именно этим алгоритмом, если и сама его поддерживает. Кроме того, этот же шифр будет применятся в дальнейшем и для симметричного шифрования с помощью обычного пароля.

По умолчанию выставлен CAST, в самых ранних был IDEA. С точки зрения обычного пользователя практических различий между ними нет – все чрезвычайно стойки. Некоторые были изобретены раньше, другие несколько новее:

- *CAST* – разработанный в 1993 году шифр со 128-битовым ключом и 64-битовым блоком. Дизайн основан на формальной архитектуре DES. Совершенно устойчив к линейному и диффиренциальному криптоанализу, может быть взломан только "в лоб". Имеет множество модификаций, часть которых была признана ненадёжными. В PGP реализован стойкий вариант CAST5.

- *Triple-DES* – он же 3DES или тройной DES. Базовый алгоритм DES был разработан IBM в середине 1970-х и принят в качестве государственного стандарта шифрования США (и весьма распространился по миру). 3DES – это его вариация, в которой базовый DES выполняется трижды на одном блоке данных. В PGP он реализован в режиме EDE (зашифрование-расшифрование-зашифрование) с тремя независимыми подключами. Длина общего ключа – 168 бит, оперирует на 64-битовых блоках. Теоретическая расчётная стойкость такого алгоритма к лобовой атаке составляет 112 бит, практическая – по меньшей мере 129 бит, что, вкупе с его проверенной годами надёжностью, крайне хороший показатель.
- *IDEA* – опубликованный в 1990, именно он лёг в основу первых версий PGP. Имеет ключи длиной 128 бит и оперирует на 64-битовых блоках открытого и шифртекста. Построен на концепции смешения операций различных алгебраических групп, а именно: XOR, сложение по модулю $2^{16}$ и умножение по модулю $2^{16}+1$. В ослабленных вариантах может быть подвержен криптоаналитическим атакам, но в базовом, который реализован в PGP, – нет.

- *Доступные алгоритмы* – допустимые симметричные алгоритмы. Как и предыдущая опция, данные установки ложатся в материал следующих генерируемых ключевых пар, а также используются вашей программой для шифрования отправляемых сообщений. Назначение этих опций в следующем: если программа PGP отправителя не поддерживает алгоритм, указанный у вас в качестве предпочтительно, она воспользуется одним из отмеченных здесь алгоритмов в качестве альтернативы. Выбор осуществляет в приоритетном порядке слева направо: скажем, если отправитель не поддерживает CAST, он зашифрует сообщение с помощью IDEA; если он не поддерживает CAST, а IDEA выключил, считая недостаточно надёжным, программа воспользуется 3DES, и т.д.

Снимайте галочки с перечисленных алгоритмов только в том случае, если у вас возникнут серьёзные и обоснованные (!) опасения в их стойкости, например, если станет доподлинно известно, что один из них был взломан! Если снять галочку с того или иного алгоритма, вы запретите вашей программе шифровать с его помощью сообщения для корреспондентов, а корреспонденты не смогут с его помощью шифровать сообщения для вас, если те же настройки легли в материал вашего открытого ключа.

### Раздел Модель доверия

Ряд расширенных настроек отношений доверия PGP.

- *Отображать крайний уровень валидности* – показывать или нет частичный уровень достоверности ключей. Если включить, уровень достоверности (подлинности) ключей в окне

PGPkeys будет показан в виде шкалы с тремя состояниями: недостоверен (пустая шкала), частично достоверен (наполовину заполненная шкала), достоверен (целиком заполненная шкала). Если опция выключена, уровень достоверности будет показан как зелёный (достоверный ключ) или серый (недостоверный ключ) кружок. Если вам необходимо иметь полное представление о состоянии ключей на вашей связке – включите.

- *Считать крайне валидные ключи невалидными* – расценивать частично достоверные ключи как недостоверные. Если включено, при попытке зашифровать сообщение частично достоверным ключом, будет показано окно выбора ключей *Key Selection Dialog*, дабы предупредить о состоянии достоверности открытого ключа получателя.
- *Предупреждать при шифровании ключами с ADK* – выдавать ли предупреждение при зашифровании, если ключ получателя содержит дополнительный ключ расшифрования (ADK). ADK используются в корпоративной среде, чтобы в определённых случаях иметь возможность расшифровать информацию своих служащих. Таким образом, наличие ADK говорит о том, что в этих определённых чрезвычайных случаях доступ к отправляемой информации могут иметь третьи лица, а не только фактический получатель.

Раздел Фомат экспорта

Выбор формата экспортируемых со связки ключей:

- *Совместимый* – совместимый с версиями PGP до 6.x. Будет экспортирован только сам ключ и связанные с ним текстовые поля сертификата.
- *Совершенный* – новый формат, совместимый с PGP 6.x и выше. Кроме ключа будут экспортированы фотографии и прочее.

### 2.2 Управление ключами

Первая задача, возникающая после инсталляции и настройки программы – это генерация пары "открытый ключ / закрытый ключ". Именно асимметричные ключи позволят вам беспрепятственно обмениваться зашифрованными и подписанными сообщениями с людьми, живущими в любом конце света.

В рамках дельнейшего описания будут использованы следующие термины:

- *Ключевая пара* – асимметричная пара "открытый ключ / закрытый ключ".
- *Ключ* – в зависимости от контекста может подразумевать открытый ключ или ключевую пару.
- *Ключевая фраза, парольная фраза, пароль* – уникальная последовательность символов и/или слов, позволяющая использовать закрытый ключ асимметричной ключевой пары.

- *Связка* – связки открытых и закрытых ключей; pkr-, skr-файлы, указанные в настройках программы.
- *Основной ключ* – ключ, указанный как "ключ по умолчанию".
- *"Отменитель"* – designated revoker, человек, уполномоченный вами при необходимости аннулировать ваш ключ.

PGP предоставляет на выбор следующие типы асимметричных ключей: *Diffie-Hellman / DSS* (или просто *DH/DSS*) и *RSA*. В старых версиях PGP (до 5.0) применялись только ключи RSA, использующие для шифрования и цифровой подписи асимметричный алгоритм RSA. В PGP 5.0 были добавлены ключи Diffie-Hellman, использующие шифрование по схеме Эльгамаля и подписание по стандарту DSS.

При генерации нового ключа вам придётся сделать выбор его типа:

- Если вам нужна полная функциональность последних версий PGP и широкая совместимость вплоть до PGP 5.0, выбирайте *DH/DSS*. В большинстве случаев это предпочтительно. Однако следует помнить, что размер ключа подписания DSS всегда равен 1024 битам, независимо от размера ключа шифрования DH.
- Если вы не хотите быть скованными ограничением на 1024-битовый ключ подписания, выбирайте тип *RSA*.
- Если вы планируете общаться с людьми, использующими исключительно старые версии PGP (до 5.0), выбирайте *RSA*. Для целей совместимости эти ключи имеют ограничение длины до 2048 бит и не поддерживают множества новых функций (фотографические удостоверения, "отменителей" и пр.).

Также не забывайте, что вы можете сгенерировать столько ключей различных типов, сколько пожелаете.

Если вы прежде не использовали PGP и не имеете готовых связок ключей, которые указали в ходе инсталляции, то первое, что нужно сделать после установки и настройки программы – это создать свой первый ключ.

Хотя это может показаться увлекательным занятием, не создавайте больше одной ключевой пары, если в ином нет явной необходимости! Тому есть ряд причин. Во-первых, не пройдёт много времени, как вы окончательно в них запутаетесь. Во-вторых, что более важно, ни один ключ не может быть надёжнее защищающей его ключевой фразы. Нет смысла создавать множество ключей с идентичными ключевыми фразами (а много разных и *хороших* вы вряд ли запомните), поскольку взлом любой из них будет равносилен взлому всех. Наконец, в-третьих, при необходимости отправить вам сообщение, незнакомый корреспондент может столкнуться с проблемой выбора ключа для зашифрования.

Чтобы сгенерировать новую ключевую пару сделайте следующее:

1. Откройте менеджер PGPkeys.
2. Нажмите иконку *Создать новую пару ключей* (  ) в панели инструментов менеджера. Появится окно генерации ключа с описанием того, что такое открытые и закрытые ключи.
3. Нажмите кнопку *Далее* для продолжения.
4. В поле *Полное имя* введите своё имя, а в поле *Адрес Email* – адрес электронной почты. Несмотря на то, что указывать своё настоящее имя не обязательно, это может помочь корреспондентам идентифицировать данный открытый ключ как принадлежащий вам. То же касается и email-адреса, по которому ваш ключ будет проще отыскать на сервере и упростит корреспондентам отправку вам сообщений.
5. В меню *Тип пары ключей* выберите тип создаваемого ключа.
6. В поле *Размер пары ключей* укажите размер создаваемого ключа в битах. Более крупный ключ потребует больше времени на генерацию и на дальнейшие операции зашифрования / расшифрования, в то же время предоставляя бо̲льшую степень надёжности. Если передаваемая вами информация не представляет ценность, сопоставимую с ценой проведения чрезвычайно дорогостоящей криптоаналитической атаки, будет более чем достаточно выставленных по умолчанию 2048 бит.
7. В разделе *Срок годности ключа* укажите дату истечения срока действия создаваемого ключа. Выберите либо установленное по умолчанию *“Вечный” ключ* (бессрочный), либо укажите определённую дату, с которой ключавая пара не сможет применяться для задач зашифрования и подписания (тем не менее, ею можно будет продолжать пользоваться для расшифрования и сверки ЭЦП). *“Вечный” ключ* является предпочтительным. Если, однако, вы планируете использовать данный ключ только определённый период (например, в течение срока действия контракта с работодателем), укажите здесь дальнюю границу этого периода.
8. Нажмите *Далее*.
9. В окне выбора ключевой фразы введите в оба представленных поля пароль, которым хотите защитить свой новый закрытый ключ.

Парольная фраза – это единственный и по этой причине самый главный механизм защиты закрытого ключа от несанкционированного использования. Вся надёжность PGP упирается в качество выбранной вами на этом этапе ключевой фразы. В порядке меры предосторожности программа скрывает вводимые символы. Если вам от этого неудобно и вы уверены, что в помещении нет посторонних глаз, снимите галочку со *Скрыть*.

ВНИМАНИЕ: Если вы позднее забудете введённую на этом этапе парольную фразу, никто не сможет помочь вам воспользоваться закрытым ключом данной ключевой пары, и вся зашифрованная с её помощью информация фактически будет утеряна!

В целях совместимости крайне не рекомендуется использовать для ключевой фразы кириллицу и другие нелатинские национальные буквенные символы. Если же вы считаете, что их использование необходимо, протестируйте созданный ключ на не представляющей ценности информации и убедитесь, что можете свободно её расшифровать, прежде чем применять ключ по назначению.

10. Нажмите *Далее*.

11. Если введённая на предыдущем этапе ключевая фраза не соответствует нормам безопасности, PGP выдаст предупреждение. Вернитесь назад и устраните проблему, ибо её игнорирование повлечёт серьёзные проблемы с защищённостью ключа.

12. Движения вашей мышки и нажатия на клавиши создают множество случайной информации (энтропии), обязательной для генерации ключей. Однако бывает так, что PGP не успевает накопить достаточно энтропии до начала генерации ключа. В таком случае появится окно сбора случайных данных *PGP Random Data*: просто подвигайте мышкой и понажимайте на произвольные клавиши, пока шкала не заполнится целиком. Если же всё нормально, PGP приступит к формированию ключа.

13. В зависимости от мощности компьютера и от длины создаваемого ключа на этот этап может потребоваться разное количество времени: от нескольких секунд до десятков минут. Дождитесь, пока не появится сообщение *Завершено*. После этого можете нажать кнопку *Далее* и затем *Готово*.

PGP самостоятельно разместит открытый и закрытый ключи в соответствующих файлах связки, а имя ключа появится в окне менеджера PGPkeys.

Зашифровать файл, а после обнаружить, что не можешь его расшифровать – это болезненный опыт, тем не менее, помогающий понять, как правильно выбирать ключевую фразу, которую удастся запомнить.

Большинство приложений с ограничением доступа предлагают использовать в качестве пароля слово из трёх-восьми букв. Очень нежелательно использовать подобные пароли по ряду причин. Во-первых, они сильно уязвимы к атакам "по словарю", когда взломщик заставляет компьютер перебирать все слова из словаря, пока не угадает пароль. Во-вторых, они могут взломаны полным перебором всех возможных комбинаций букв, печатных символов и цифр.

Чтобы защититься от подобного рода атак рекомендуется создавать парольное слово, состоящее из заглавных и строчных букв, цифр, знаков препинания и пробелов. В результате получается пароль, который довольно сложно подобрать, но ещё труднее запомнить. Использование в составе пароля множества произвольных небуквенных символов повышает его стойкость к атакам "по словарю", но и затрудняет его запоминание, что, рано или поздно,

может привести к катастрофической потере информации по той лишь причине, что вы не сможете расшифровать собственные файлы.

С другой стороны, ключевая фраза, или *осмысленный пароль*, – это последовательность логически связанных слов, обычно, длинное предложение, которое гораздо менее уязвимо к "словарным" атакам. Однако, если вы не выберите в качестве ключевой фразы нечто, давно хранящееся в долгосрочной памяти мозга, то едва ли сможете запомнить её буквально.

Выбор ключевой фразы под влиянием обстоятельств скорее всего приведёт к тому, что вы начисто её забудете; не поможет и попытка "зазубрить" – так устроена память. Выберите что-то, уже находящееся в вашей долгосрочной памяти. *Это не должна быть* фраза, которой вы с кем-то недавно делились или которую часто любите повторять, и не должен быть известный афоризм или цитата, поскольку всё это будет со временем подобрано опытным взломщиком. Можете построить ключевую фразу на ассоциации или ассоциативном ряде, задав себе вопрос, ответ на который знаете только вы. Но это должно быть нечто, давно и глубоко хранящееся в вашем мозге, однако и не что-то очевидное и легко предсказуемое. Альтернативный вариант – это мнемотехнические методики, но они требуют определённой практики и опыта. Постарайтесь несколько "усилить" результат заглавными буквами в произвольных местах и небуквенными символами, только не переусердствуйте.

Разумеется, если вы будете столь недальновидны, что запишите результат на листке бумаги и положите его в ящик письменного стола, не имеет большого значение, сколь хорошую ключевую фразу вы придумаете.

Сгенерировав новую ключевую пару немедленно сделайте несколько её резервных копий на разных внешних носителях! (В действительности, PGP сам предложит вам это сделать, когда вы закроете окно PGPkeys. Ни в коем случае не пренебрегайте этой рекомендацией!) Игнорирование этого требования приводит к неоправданному риску потери всех ценных данных. Если что-то случится с единственным файлом связки закрытых ключей, никто во всём мире не поможет вам расшифровать ваши файлы.

Кроме резервного копирования pkr- и skr-файлов связки ключей, обратите особое внимание на то, где хранится ваш закрытый ключ. Хотя закрытый ключ защищён ключевой фразой, известной только вам, посторонний может узнать её, например, просто подсмотрев из-за спины, какие клавиши вы нажимаете, или перехватив нажатия клавиш через локальную сеть или даже через Интернет, а затем воспользоваться закрытым ключом, чтобы расшифровывать вашу информацию и подделывать подпись.

Чтобы избежать подобных сценариев, храните закрытый ключ только на своём компьютере. Если ваш компьютер подключён к локальной сети, убедитесь, что файлы связок не подлежат автономному резервному копированию на носители, к которым могут получить доступ посторонние лица. Учитывая лёгкость, с которой злоумышленник может проникнуть

в компьютер через сеть, установите дополнительные защитные барьеры в виде межсетевых экранов и антивирусных программ. Работая со сверхценной информацией, разместите свой закрытый ключ на дискете или, что предпочтительнее, на смарт-карте, которую можно использовать аналогично ключу от дверного замка, подключая к компьютеру, только когда нужно подписать или расшифровать информацию.

Ещё одна мера предосторожности заключается в переименовании связки закрытых ключей (skr-файла) и перемещении её в отдельный от открытых ключей каталог. Для этого воспользуйтесь вкладкой *Файлы* меню настроек программы.

### 2.3 Управление связкой ключей

Ключи, созданные вами или полученные от корреспондентов, хранятся на связках, по сути представляющих собой два файла (базы данных): один содержит открытые ключи и по умолчанию назван *pubring.pkr*, другой предназначен для закрытых и называется *secring.skr*. Изначально эти файлы хранятся в каталоге с программой PGP или в папке “Мои документы\PGP”.

В некоторых случаях вам может потребоваться изучить атрибуты ключей и их сертификатов или изменить их параметры. Скажем, получив от корреспондента открытый ключ, вы захотите установить его тип, проверить отпечаток и по содержащимся на сертификате подписям определить достоверность. Затем вы решите сами подписать этот ключ, чтобы указать на его подлинность, и настроить уровень доверия владельцу в заверении других ключей.

Порой может возникнуть необходимость изменить ключевую фразу вашего собственного закрытого ключа или найти чей-то открытый ключ на общественном сервере.

Для выполнения всех перечисленных и некоторых других мероприятий служит менеджер PGPkeys.

#### 2.3.1 Основы PGPkeys

Окно менеджера PGPkeys содержит список всех ваших ключевых пар и чужих открытых ключей, добавленных вами на связку. В верхней части окна расположена панель инструментов, предназначенная для выполнения наиболее обыденных задач, и строка меню, предоставляющая доступ к дополнительным функциям.

Большинство операций с ключами может быть выполнено четырьмя разными способами:

- Через иконки в панели инструментов.
- Через строку меню в верхней части окна.

- Через контекстное меню по нажатии правой кнопкой на имя ключа или составляющих его элементов.
- С помощью горячих клавиш PGPkeys (они отображены напротив соответствующих функций в меню в верхней части окна).

Все эти способы совершенно равноправны.

#### 2.3.1.1 Атрибуты ключей

Наряду с именами ключей окно PGPkeys отображает некоторые из их параметров и атрибутов. В меню *Вид* вы можете указать, какие атрибуты будут отображаться в окне менеджера, а в самом окне при желании можете изменить порядок расположения столбцов атрибутов (перетащив столбец за шапку) и сортировку списка ключей по любому из атрибутов (нажав левой кнопкой на шапку нужного столбца).

Окно PGPkeys может показывать следующие параметры ключей:

- ***Ключи* (*Keys*)** – этот атрибут представлен набором пиктографических изображений, обозначающих различные параметры ключа. Также он содержит имя владельца, сведения сертификата ключа и имена его поручителей. В таблице 2.1 приведено описание пиктограмм, соответствующих атрибуту “Ключи”.

Таблица 2.1

| | |
|---|---|
| | Золотой ключ и человечек обозначают принадлежащую пользователю пару "открытый ключ / закрытый ключ" типа Diffie-Hellman / DSS. |
| | Серый ключ и человечек обозначают принадлежащую пользователю пару "открытый ключ / закрытый ключ" типа RSA. |
| | Золотой ключ обозначает открытый ключ типа Diffie-Hellman / DSS. |
| | Серый ключ обозначает открытый ключ типа RSA. |
| | Пара ключей обозначает разделённый ключ. Такой может использоваться для расшифрования / подписания только после объединения. |
| | Тусклый ключ обозначает временно дезактивированный открытый ключ. Такой не может использоваться для зашифрования. Это удобно при большом количестве открытых ключей на связке, сильно захламляющих окно *Key Selection Dialog*. |

| | |
|---|---|
| | Серый ключ на золотой карте обозначает сохранённый на смарт-карте ключ типа RSA. |
| | Ключ с красным запрещающим знаком обозначает аннулированый открытый ключ. Это значит, что он либо был скомпрометирован, либо по иным причинам более не используется владельцем. |
| | Ключ с часиками обозначает просроченный открытый ключ, чей период действия уже истёк. |
| | Два человечка обозначают группу открытых ключей списка рассылки. |

В таблице 2.2 приведены пиктограммы, обозначающие содержимое сертификата:

Таблица 2.2

| | |
|---|---|
| | Конверт обозначает обычное имя в сертификате ключа; как правило, это просто имя и email-адрес владельца ключа. Конверт может быть жёлтым или серым в зависимости от типа ключа (DH/DSS или RSA). |
| | Конверт с красным запрещающим знаком обозначает аннулированную запись сертификата. |
| | Картинка обозначает фотографическое удостоверение в сертификате. |
| | Карандаш (или шариковая ручка) обозначает подпись, подтверждающую ту или иную запись сертификата ключа. Иконка карандаша без дополнилнительных символов – это неэкспортируемая подпись, заверяющая ключ только на связке пользователя. |
| | Карандаш с синей стрелкой обозначает экспортируемую со связки подпись. Такая используется как поручительство пользователя в подлинности ключа и данной записи сертификата |
| | Карандаш с красным запрещающим знаком обозначает отозванную подпись. |
| | Тусклый карандаш обозначает неверную или повреждённую подпись. |

- ***Достоверность* (*Validity*)** – jбозначает степень убеждённости в том, что открытый ключ действительно принадлежит предполагаемому владельцу. Зависит от состава подписей, заверяющих данный ключ, и уровней доверия пользователя поручителям (людям, подписавшим ключ). Ключ, подписанный непосредственно пользователем, становится полностью достоверным, исходя из логики программы, что пользователь не станет подписывать поддельный открытый ключ. Ключ, не имеющий подписей, считается недостоверным, о чём программа будет напоминать всякий раз при попытке зашифровать информацию данным ключом. Атрибут достоверности может быть показан либо в виде цветного кружка, либо в виде шкалы, в зависимости от установок параметра *Display marginal validity level* в настройках программы. Если опция выключена, то атрибут отображается следующим образом (таблица 2.3):

Таблица 2.3

| | |
|---|---|
| | Серый кружок обозначает недостоверные ключи (и частично достоверные ключи, если опция *Treat marginally valid keys as invalid* в настройках программы включена). |
| | Зелёный кружок обозначает достоверные открытые ключи. |
| | Зелёный кружок и человечек обозначают безусловно достоверную ключевую пару пользователя. |

- ***Размер* (*Size*)** – длина асимметричного ключа в битах. Для ключей типа DH/DSS и RSA отображается два числа: первое – длина подключа шифрования, второе – длина ключа подписания. Ключ подписания DSS всегда равен 1024 битам.
- ***Доверие* (*Trust*)** – обозначает указанный пользователем уровень доверия владельцу данного ключа в заверении чужих открытых ключей (таблица 2.4). Это влияет на степень достоверности чужих ключей, поручителем которых выступает владелец данного.

Таблица 2.4

| | |
|---|---|
| | Пустая шкала говорит о том, что владелец данного ключа не имеет доверия и не может выступать поручителем (его подпись не учитывается при расчёте достоверности ключей). |
| | Частично заполненная шкала говорит о том, что подписанный владельцем данного ключа открытый ключ будет иметь частичную достоверность. |

| | |
|---|---|
|  | Полностью заполненная шкала обозначает, что владелец данного ключа имеет полное доверие в заверении других открытых ключей, и любой ключ, подписанный им, считается программой достоверным. |
|  | Заштрихованная шкала указывает на безусловно доверенный ключ пользователя. |

- ***Описание* (*Description*)** – краткое описание объекта в колонке ***Ключи***: тип и состояние ключа, тип удостоверения, вид подписи и т.п.
- ***ID ключа* (*Key ID*)** – уникальный идентификационный номер, помогающий отличить несколько открытых ключей с одинаковыми именами владельца (в очень редких случаях сами номера ID у разных ключей совпадают).
- ***Создание* (*Creation Date*)** – указывает дату, когда ключ был сгенерирован. Иногда можно исходить из этой информации при анализе подлинности ключа. Если он был создан довольно давно, маловероятно, что его станут подменять, поскольку за прошедшее время оригинальные копии должны были получить широкое распространение. Но никогда не полагайтесь на этот показатель как на единственный параметр анализа (его крайне легко сфальсифицировать)!
- ***Срок годности* (*Expiration Date*)** – указывает дату, когда ключ станет неприменим для новых криптографических задач, либо “Вечный” (*Never*), т.е. неограниченный срок действия.
- ***ADK*** – наличие дополнительных ключей расшифрования. Серым или зелёным кружком показывает, содержит ли конкретный ключ ADK.

Также в меню *Вид* можно включить или выключить показ панели инструментов (*Панель инструментов*).

#### 2.3.1.2 Выбор основного ключа

Основной ключ пользователя, или ключ по умолчанию, используется программой, чтобы автоматически зашифровывать информацию не только для получателя, но и для вас самих, дабы в дальнейшем вы имели возможность, например, расшифровать и прочитать отправленное письмо. Подписывая сообщение или чей-то открытый ключ, PGP будет также предлагать использовать ваш ключ по умолчанию (разумеется, если вы пожелаете воспользоваться другим своим закрытым ключом, то сможете это сделать). В окне PGPkeys основной ключ выделен **жирным шрифтом**, дабы отличить его от остальных. Если вы

используете несколько ключевых пар, выбор одной как основной сделает работу с PGP более удобной.

Чтобы выбрать основной ключ:

1. В окне PGPkeys выделите тот свой ключ, который хотите сделать основным.
2. В строке меню нажмите *Ключи* > *Назначить ключом по умолчанию*.

Имя ключа станет жирным, обозначая, что теперь он используется по умолчанию.

#### 2.3.1.3 Импортирование и экспортирование ключей

Наиболее удобным способом обмена ключами является их пересылка через сервер-депозитарий, но иногда может потребоваться отправить открытый ключ в виде отдельного файла (например, через FTP-сервер). Или вы можете захотеть сохранить резервную копию отдельных ключей, а не связок целиком (чтобы зарезервировать связку, достаточно скопировать файлы pubring.pkr и secring.skr, расположение которых можно узнать во вкладке *Файлы* меню настроек программы). В этом случае можно экспортировать или копировать ключи в файл.

Если же ваш корреспондент изберёт в качестве способа передачи отправку открытого ключа по электронной почте, воспользуйтесь возможностью импортирования, чтобы добавить полученный ключ на свою связку. То же касается и восстановления резервных копий, и иных схожих задач.

Ниже приведены способы импортирования / экспортирования ключей.

Экспортирование ключа со связки в файл:

1. В окне PGPkeys выделите ключ, который хотите экспортировать. Можете экспортировать сразу группу ключей, выделив несколько нужных.
2. В строке меню нажмите *Ключи* > *Экспорт*.
3. Чтобы вместе с ключами экспортировать фото-удостоверения, отметьте опцию *Включить расширения 6.0*. Однако учтите, что в этом случае экспортированные ключи будут несовместимы с версиями PGP до 6.0.
4. Если в числе экспортируемых ключей присутствуют ваши ключевые пары, и кроме открытых вы хотите сохранить и закрытые ключи, отметьте галочкой опцию *Включить закрытые ключи*. В этом случае будьте внимательны, чтобы экспортированный файл не попал в руки к посторонним.
5. Укажите имя файла и каталог, где хотите его сохранить.

Копирование материала ключа со связки позволяет позднее вставить его в любой текстовый файл или в тело письма. Весьма удобный способ для некоторых мероприятий. Но копировать таким образом материал закрытых ключей невозможно.

Копирование материал ключа со связки в документ:

1. В окне PGPkeys выделите ключ, который хотите копировать. Можете копировать сразу группу ключей, выделив несколько нужных.

2. В строке меню нажмите *Правка* > *Копировать*.

Материал ключа (или ключей) помещён в буфер обмена (рисунок 2.11). Теперь можете вставить его в любой текстовый документ простой функцией *Вставить* или комбинацией клавиш *Ctrl+V*.

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGPfreeware 6.5.8 for non-commercial use <http://www.pgp.com>
Comment: Копированный блок открытого ключа

mQCNBEFiQG8BBACyXzMkqNm0gEB6CejyiftiHtAbahwF79++mwGnA2nEWW+g7iUt
Y9/ZXjpKEEM6Y3ZeOCiCtlSyOq4aqpiM+74BoBgoqCPkcQ7eFAOq3Ihkoiz3CmjR
LLNo1yz5N12/Q6fU+U4LTAC3u4en+m+MavdLp85EhOEiEmPxiUcbgVE4BwARAQAB
tAMxMjOJAK4EEAECABgFAkFiQG8ICwIDCQgHAQoCGQEFGwMAAAACgkQ4+j9xbFm
GcOKBQP+Nr17DYyzatk7gtgXLJvjYbfNIEgTDww97kocBYOAfq1ETDD3ObVkWP0F
y8hOUpkpxBE4+C7F1CCv6CWpk96dN/F3w0v6XkHMeP170WOGhk7dJKaH70y0aWK0
/mMNpnz5ZtzLvodANG6Q0ddHBvXuJW8KBl3yOxVm0nT7AjbBmZi5AI0EQWJAcAEE
AJ+kaOL9lYIbOMd/mfRw5yiAMrU/QdSLKhyzYf98OVuSTqDH1BLwXbAOvEN5U/al
eKNWegfmFdXqRct9PXv8ECtZCVVxobo5IhXAOkL3nCyxAdadBgMV1BASdKZtd8QZ
BcFeUEdSqcAVe992jXWs4xec0aIwlk2gRk3J3kFlgjGjABEBAAGJAKIEGAECAAwF
AkFiQHAFGwwAAAACgkQ4+j9xbFmGcOBagQAqF/ODSYBha5+dC/95PkTtPGulF7M
BqWwrPv3luIPOSCmNCobHVZCRYsl5O7WLoirMwi7sSA8K0OeWASbXJMtgKSXHxnq
M5A3TD9rkPlCOvB8iS1jM6qPlguD9CTuIU6hSQGtGtSnZBQ51wgcTyg42aR/D5YZ
KCmMi1mVpwrKZqI=
=lZr7
-----END PGP PUBLIC KEY BLOCK-----
```

Рис. 2.11

Импортирование ключа из файла на связку:

1. В строке меню PGPkeys нажмите *Ключи* > *Импорт*.

2. В меню *Тип файла* (*File Types*) выберите тип импортируемого файла. Это может быть *txt* или *asc* для текстового материала ключа PGP, файлы связок PGP с расширениями *pkr*, *skr*, *pubkr*, *seckr* и *pgp*.

3. Укажите импортируемый файл и нажмите кнопку *Открыть* (*Open*).

4. В появившемся окошке *Укажите ключ*(*и*) отметьте те ключи из выбранного файла, которые хотите импортировать, и жмите *Импорт*.

Ключи будут присоединены к вашим связкам. Если среди импортированных были и закрытые ключи, программа предупредит, что им необходимо указать соответствующий уровень доверия. Для этого откройте свойства этих ключей (*Ключи* > *Свойства* в строке меню) и установите флажок на опцию *Имплицитное доверие*, наделяющую ключ безусловным уровнем доверия.

Если полученное вами письмо или текстовый файл содержат материал ключа, можете добавить его на связку следующим образом:

1. В полученном тексте выделите блок, начиная с заголовка “-----BEGIN PGP PUBLIC KEY BLOCK-----” (или “PRIVATE KEY BLOCK” для закрытого ключа) и заканчивая строкой “-----END PGP PUBLIC KEY BLOCK-----” и копируйте выделенный материал в буфер обмена (обычно можно просто нажать *Ctrl+C*).

2. В строке меню PGPkeys нажмите *Правка* > *Вставить*.

3. В появившемся окошке *Укажите ключ(и)* отметьте те ключи из полученного материала, которые хотите импортировать, и жмите *Импорт*.

#### 2.3.1.4 Удаление ключей, подписей и сертификатов

Иногда может потребоваться удалить со связки ненужный ключ, заверяющую его подпись или запись из сертификата.

Удаление ключа со связки необратимо. Хотя вы можете повторно импортировать открытый ключ, добавить запись в сертификат или снова заверить ключ прежде удалённой подписью, удаление закрытого ключа, не имеющего резервных копий, приведёт к фактической потере всей информации, зашифрованной соответствующим открытым ключом, поскольку эта информация более не сможет быть расшифрована!

Не забывайте, что удаление своего ключа со связки не аналогично его аннулированию. Если вы больше не собираетесь использовать ключевую пару, аннулируйте её и обновите на сервере, чтобы корреспонденты не использовали данный открытый ключ для отправки вам сообщений.

Чтобы удалить ключ, сертификат или подпись со связки:

1. В окне PGPkeys выделите объект, который хотите удалить.

2. В строке меню нажмите *Правка* > *Удалить* либо нажмите кнопку *Удалить выбранный элемент* (  ) в панели инструментов.

3. На просьбу подтвердить удаление нажмите *Да*.

Выбранный объект будет удалён со связки.

#### 2.3.1.5 Активирование / дезактивирование ключей

Если количество ключей на вашей связке становится угрожающе велико, и поиск нужного для зашифрования письма оборачивается всё более трудной задачей, вы можете временно дезактивировать ключи, которые не используете постоянно, но и не хотите удалять. С этого момента они не будут захламлять окно *Key Selection Dialog*.

Для дезактивации открытых ключей корреспондентов:

1. В окне PGPkeys выделите ключ, который хотите дезактивировать.
2. В строке меню нажмите *Ключи* > *Запретить*.

Пиктограмма ключа потускнеет, обозначая, что он временно отключён. Чтобы снова активировать ключ для использования:

1. Выделите ключ, который хотите активировать.
2. В строке меню нажмите *Ключи* > *Разрешить*.

Пиктограмма станет обычной, а ключ – готовым к работе.

Если фраза об угрожающем количестве ключей на связке справедлива для ваших собственных ключевых пар, некоторыми из которых вы пользуетесь относительно редко, можете дезактивировать и их. В этом случае конкретный ключ не сможет применяться для зашифрования и подписания данных, но вы сможете продолжать им пользоваться для расшифрования файлов и сверки своих ЭЦП.

Чтобы дезактивировать ключевую пару:

1. В окне PGPkeys нажмите правой кнопкой на ключ, который хотите дезактивировать > *Свойства ключа*.

2. В окне свойств ключа снимите галочку с опции *Имплицитное доверие*, а затем с *Разрешен*. Закройте окно свойств.

Изображение человечка с пиктограммы ключа пропадёт, а сам ключ потускнеет, обозначая, что он временно неактивен. Чтобы снова активировать ключевую пару:

1. Нажмите правой кнопкой на ключ, который хотите активировать > *Свойства ключа*.
2. В окне свойств ключа отметьте галочкой параметр *Разрешен*, а затем – *Имплицитное доверие*. Закройте окно свойств.

Пиктограмма станет обычной, а ключевая пара – готовой к работе.

### 2.3.2 Просмотр и настройка свойств ключей

Кроме просмотра наиболее общих атрибутов ключей непосредственно в окне менеджера PGPkeys, вы можете изучить и отредактировать дополнительные параметры любого ключа в окне его свойств.

Сведения в окне свойств ключа (*Свойства ключа*) разбиты по четырём вкладкам (рисунок 2.12):

- “*Общие*” содержит основные параметры и описание ключа;
- “*Подключи*” позволяет редактировать подключи шифрования;
- в “*Аннуляторы*” перечислены "отменители" данного ключа;
- в “*ADK*” указаны дополнительные ключи расшифрования.

Учтите, что вкладки “*ADK*” и “*Аннуляторы*” могут отсутствовать, если ключи ADK и "отменители" не были добавлены к данному ключу.

Чтобы открыть окно свойств, в менеджере PGPkeys нажмите правой кнопкой на имя ключа > *Свойства ключа*. Либо выделите нужный ключ и в панели инструментов нажмите кнопку *Показать свойства ключа или сертификата* ( ).

### *2.3.2.1 Основные свойства и смена ключевой фразы*

Во вкладке основных свойств *Общие* (рисунок 2.12) содержатся следующие сведения и настройки.


Рис. 2.12

- Технические параметры ключа, а именно:
- *ID* – уникальный идентификационный номер ключа.
- *Тип* – тип асимметричного ключа.
- *Размер* – длина асимметричного ключа в битах.
- *Создан* – дата создания ключа.
- *Срок* – окончание срока действия ключа (*Вечный*, если не имеет ограничения).
- *Шифр* – симметричный алгоритм, используемый для шифрования этим ключом.

- Опцию *Разрешен*, позволяющую активировать / дезактивировать ключ.
- Фото-удостоверение.
- Кнопку *Смена пароля* для смены ключевой фразы либо *Соединение с ключом* для восстановления разделённого ключа в единое целое.
- Параметры *Отпечаток* с отпечатком открытого ключа и *Модель доверия*, показывающий уровень достоверности открытого ключа и степень доверия его владельцу.

Регулярная смена ключевой фразы не является обязательной практикой для асимметричных ключей (важнее, чтобы она просто была очень надёжной): если кто-то получит ваш закрытый ключ в своё распоряжение, замена прежней ключевой фразы уже не избавит ключ от угрозы компрометации. Поэтому важно менять её только при угрозе компрометации самой ключевой фразы, например, если кто-то стоял у вас за спиной и, вероятно, мог подсмотреть за нажатиями клавиш, когда вы её набирали.

Но если злоумышленник уже похитил копию закрытого ключа, процедура смены пароля вас не спасёт. В этом случае немедленно изготовьте новую ключевую пару и перешифруйте все зашифрованные документы, файлы и корреспонденцию, уничтожив копии, зашифрованные скомпрометированным ключом.

Чтобы изменить текущую ключевую фразу:

1. Во вкладке *Общие* нажмите кнопку *Смена пароля*.
2. Введите текущую ключевую фразу и нажмите *OK*.
3. В оба представленных поля введите новую ключевую фразу. Если хотите видеть, что набираете, снимите галочку с *Скрыть* (убедитесь, что в помещении нет посторонних). Нажмите *OK*.

Если вы сменили ключевую фразу из-за подозрений её компрометации, после процедуры обязательно примите меры к уничтожению всех резервных копий своих связок и данной ключевой пары, а затем очистите свободное пространство диска, поскольку оставшиеся копии закрытого ключа по-прежнему защищены скопрометированной ключевой фразой!

#### 2.3.2.2 Свойства подключей шифрования и их настройка

Каждая асимметричная ключевая пара по определению состоит из двух ключей: открытого и закрытого. В PGP версии 6.0 и выше появилась возможность создавать, удалять и аннулировать дополнительные подключи шифрования без необходимости жертвовать своей базовой ключевой парой и собранными на её сертификате подписями. В целом это похоже на превращение вашего базового ключа в своего рода связку с хранищимися на ней подключами. Сущностное отличие лишь в том, что эти подключи используются только для

зашифрования и расшифрования; для задач подписания информации служит только базовый закрытый ключ.

Основным назначением описанной функции является создание нескольких подключей шифрования, каждый из которых будет действовать в строго определённый период жизни базового ключа. Скажем, если вы сгенерировали базовый ключ со сроком жизни 3 года, можно создать ему три дополнительных подключа шифрования для каждого года жизни. Эта дополнительная система безопасности будет автоматически и регулярно заменять вам ключ шифрования без трудоёмкого процесса генерации и распространения нового открытого ключа. Но гораздо лучше не создавать несколько подключей сразу, а добавлять каждый новый по мере необходимости, когда период действия текущего начинает подходить к концу. Так каждый новый подключ будет совершенно непредсказуем для взломщика, что в свою очередь, многократно повысит надёжность всей системы.

Для просмотра и настройки подключей шифрования в окне свойств откройте вкладку *Подключи* (рисунок 2.13).

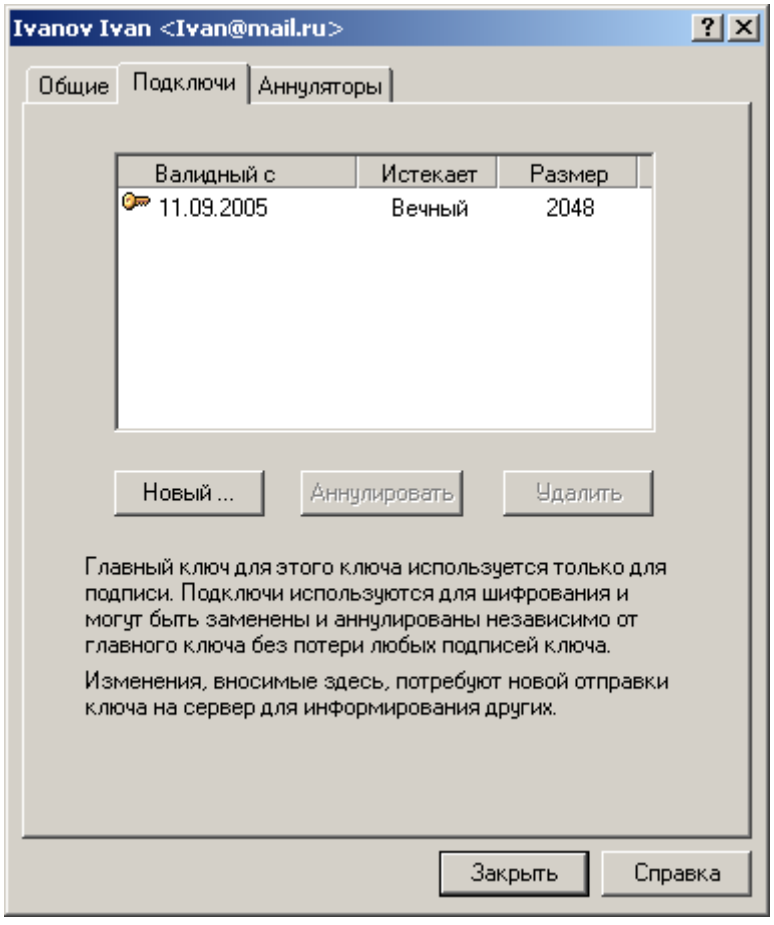



Рис. 2.13

Чтобы создать новый подключ:

1. Во вкладке *Подключи* нажмите кнопку *Новый*.

2. В появившемся окне в поле *Размер ключа* введите необходимый размер подключа в пределах 1024-4096 бит или выберите один из заданных в списке.

Не создавайте подключ меньшей длины, чем базовый ключ шифрования. Скажем, если ваш базовый ключ имеет длину 2048 бит, не создавайте подключи меньшего размера – это снизит стойкость вашей ключевой пары.

3. В поле *Начальная дата* укажите дату, когда данный подключ должен быть активирован.

4. Для параметра *Срок истекает* выберите либо *Никогда*, чтобы не ограничивать период действия подключа, либо *Дата* и укажите дату окончания его действия. Во избежание недоразумений при использовании нескольких подключей не допускайте совпадения, наложения и пересечения дат начала и окончания их действия.

5. Нажмите *OK*.

6. Введите ключевую фразу и снова нажмите *OK*.

Дополнительный подключ шифрования будет сгенерирован и добавлен к базовому ключу. Теперь вам нужно обновить ключ на сервере или самостоятельно передать его всем корреспондентам с тем, чтобы при шифровании они использовали новые сгенерированные подключи.

Если у вас возникли подозрения, что любой из подключей был скомпрометирован (обычно это относится к тому, который действует в настоящий момент), вы можете аннулировать его вместо аннулирования открытого ключа в целом.

Чтобы аннулировать подключ шифрования:

1. Во вкладке *Подключи* выделите нужный и нажмите кнопку *Аннулировать*.

2. PGP предупредит, что аннулирование подключа сделает невозможным зашифрование с его помощью любой информации. Если вы уверены в своих действиях, нажмите *Да*.

3. Введите ключевую фразу и нажмите *OK*. Обязательно обновите свой открытый ключ на сервере и разошлите соответствующие уведомления своим постоянным корреспондентам!

Чтобы удалить подключ с базового ключа:

1. Во вкладке *Подключи* выделите нужный и нажмите кнопку *Аннулировать*.

2. PGP предупредит, что удаление подключа носит необратимый характер и сделает невозможным расшифрование любой зашифрованной им информации (поскольку будет удалена и соответствующая часть с базового закрытого ключа).

3. Если действительно хотите это сделать, нажмите *Да*. Обязательно обновите свой открытый ключ на сервере и разошлите обновлённые копии своим постоянным корреспондентам!

#### *2.3.2.3 Свойства "отменителя"*

Вкладка *Аннуляторы* (рисунок 2.14) содержит список ключей, владельцы которых уполномочены при необходимости аннулировать данный открытый ключ.

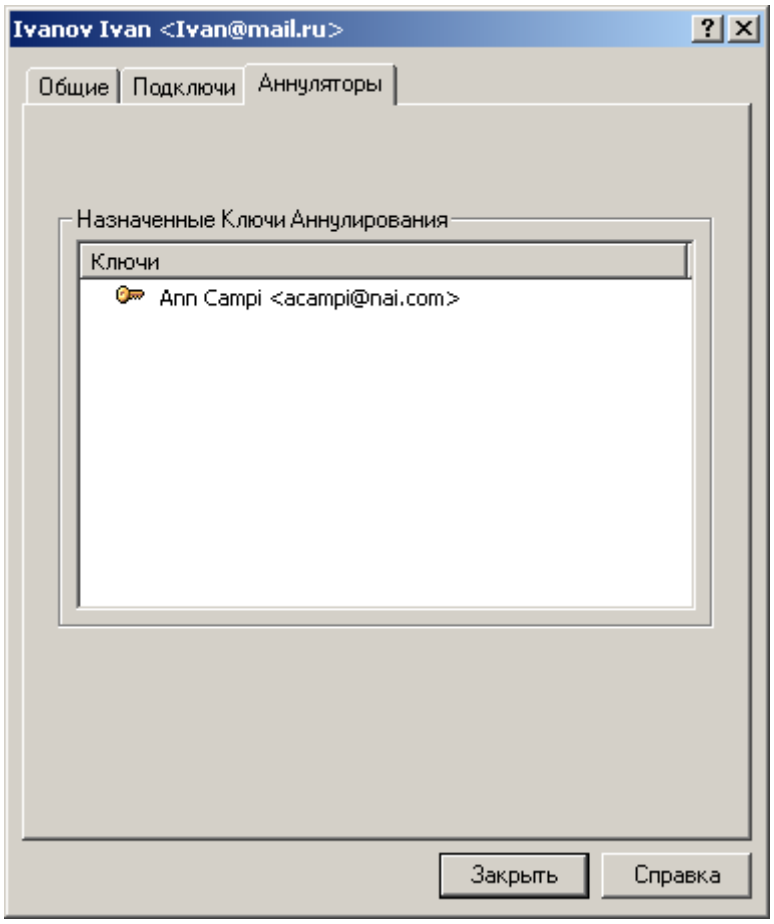



Рис. 2.14

Если ключ "отменителя" отсутствует на вашей связке, он будет представлен строкой *"Неизвестный ключ"*, за которой следует идентификационный номер. Выделите номер и нажмите кнопку *Update from Server*, чтобы загрузить копию открытого ключа с сервера.

Обязательно загружайте к себе на связку ключи всех уполномоченных вашими корреспондентами "отменителей". В противном случае PGP не сможет корректно проверять ключи на предмет "аннулированности" и в итоге вы можете использовать скомпрометированный ключ!

### 2.3.3 Сертификация открытых ключей

Хотя асимметричные криптосистемы являются лучшим решением для обмена ключами и зашифрованной информацией, они крайне уязвимы к атакам "человек в середине", когда злоумышленник пытается выдать свой поддельный открытый ключ за ключ вашего корреспондента, чтобы позднее перехватывать, читать и изменять пересылаемые сообщения.

Взаимное заверение пользователями открытых ключей друг друга – это краеугольный камень распределённой модели доверия Web of Trust, лежащей в основе PGP и служащей мерой противодействия таким атакам.

Считать открытый ключ корреспондента априорно подлинным можно лишь в одном случае – если он вручил вам свой ключ на жёстком носителе при личной встрече или если очно передал вам отпечаток (не номер ID!) своего ключа. Но зачастую это невозможно, ведь через Интернет приходится общаться с людьми, живущими за тысячи километров. Специально для цели точной идентификации любого открытого ключа они снабжены так называемыми отпечатками. Цифровой отпечаток открытого ключа (fingerprint) – это хэш-значение его материала, столь же уникальное, сколь и сам ключ.

Лучший способ установить подлинность полученной вами копии открытого ключа корреспондента – позвонить ему и попросить прочитать отпечаток с оригинала, хранящегося на его связке (прочитать отпечаток должен именно он вам, а не вы ему!). Маловероятно, что злоумышленник сможет перехватить такой произвольный звонок и провести активную атаку, попытавшись выдать себя за корреспондента. А если вам знаком голос корреспондента, это сделать будет практически невозможно.

Чтобы просмотреть отпечаток ключа, в менеджере PGPkeys нажмите правой кнопкой на имя ключа > *Свойства ключа*. Либо выделите нужный ключ и в панели инструментов нажмите кнопку *Показать свойства ключа или сертификата* (  ). В появившемся окне свойств ключа обратите внимание на *Отпечаток* (рисунок 2.15).

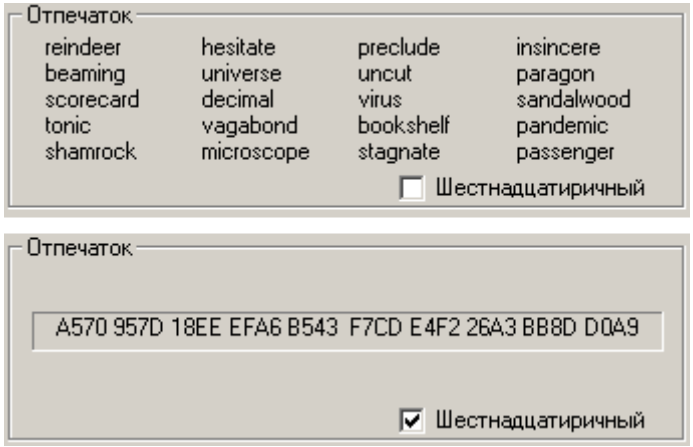



Рис. 2.15

Отпечаток ключа может быть представлен в двух формах: в виде уникального списка слов или в виде уникальной буквенно-числовой последовательности.

По умолчанию отпечаток представлен уникальным списком т.н. биометрических слов. Эти слова по своему назначению аналогичны международному авиационному алфавиту (наверное, вы слышали в западных фильмах эти "альфа-зулу-фокстрот-гольф" и т.п.),

предназначенному для безошибочной передачи буквенной информации по аудио-каналу с сильными помехами, но в отличие от того алфавита, содержащего всего 26 букв-слов, биометрический словарь PGP включает 256 слов. Если вы решите сравнить отпечаток ключа, позвонив его владельцу, эти фонетически отчётливые слова позволят точно идентифицировать ключ даже по плохой междугородней связи и даже если вы или корреспондент не знаете английского языка.

Отметив галочкой опцию *Шестнадцатиричный*, вы отобразите отпечаток в виде шестнадцатеричного числа. Такой формат удобен для передачи отпечатка через Интернет или его размещения на своём веб-сайте. Можно выделить и копировать число, а затем вставить его в любой документ. Кроме того, отпечаток открытого ключа в шестнадцатеричной форме иногда печатают на оборотной стороне визитных карточек.

Кроме непосредственно заверения чужого открытого ключа вы можете указать некоторый уровень доверия его владельцу в заверении других ключей и в выступлении в качестве их поручителя. Этот показатель считается вашим субъективным мнением о том, насколько данный пользователь компетентен в проверке подлинности открытых ключей, и насколько весомой вы считаете его подпись, заверяющую тот или иной ключ. Это значит, что если в будущем к вам в руки попадёт ключ, подписанный данным пользователем, он изначально будет для вас достоверным, хотя вы лично и не проверяли его подлинность.

Поскольку показатель степени доверия является вашим субъективным конфиденциальным мнением, он не экспортируется вместе с ключом и действенен только на вашей связке.

Чтобы установить степень доверия владельцу ключа убедитесь, что этот ключ вами подписан (экспортируемой или неэкспортируемой подписью). Затем:

1. В окне PGPkeys выделите ключ, и в строке меню выберите *Ключи* > *Свойства ключа*. В появившемся окне свойств ключа обратите внимание на раздел *Модель доверия* (рисунок 2.16).

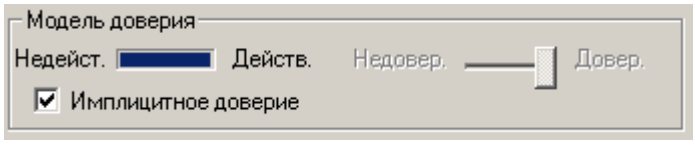



Рис. 2.16

2. Используйте регулятор *Уровень доверия*, чтобы установить нужный уровень доверия.

- По умолчанию уровень доверия ключа установлен на *Недовер.* (нет доверия): подписи этого ключа не будут приниматься в расчёт при вычислении достоверности других ключей.
- Если сдвинуть регулятор на средний уровень, подпись станет частично доверяемой и будет частично заверять другие ключи, т.е. одной этой подписи будет недостаточно, чтобы

считать подписанные ключи достоверными: потребуется по меньшей мере две частично доверяемых подписи.

- Если вы считаете, что владелец этого ключа достаточно осторожен и с большой тщательностью проверяет подлинность подписываемых ключей, установите регулятор в положение *Довер.* (полное доверие), и подпись этого ключа будет заверять другие так же, как ваша собственная. Учтите, что ключ, заверенный вами с помощью подписи *Экспортируемая доверенного представителя* или *Неэкспортируемая псевдо-представителя*, уже имеет максимальный уровень доверия, снизить который невозможно.

3. Сделав выбор, закройте окно свойств, чтобы сохранить изменения.

Учтите, что вы не можете менять уровень доверия своих ключей, поскольку логика программы исходит из допущения, что вы полностью доверяете собственным действиям, и ставит вас в основу иерархии вашего дерева сертификации. Программа считает, что конкретный открытый ключ принадлежит вам, если находит на связке соответствующий ему закрытый. Полная ключевая пара всегда имеет уровень доверия *Имплицитное доверие* – безусловное доверие.

### 2.3.4 Редактирование сертификата ключа

Сертификат каждого открытого ключа PGP содержит по меньшей мере одну идентифицирующую запись (удостоверение), позволяющую соотнести ключ с владельцем или с одним из его реквизитов: адресом электронной почты, номером ICQ и пр. Новый только что сгенерированный ключ имеет лишь одну такую запись. Но если вы хотите использовать данный ключ для различных email-адресов и других средств связи, хотите добавить фото-удостоверение как дополнительный способ опознавания, то в любой момент можете это сделать.

Обычная запись сертификата OpenPGP включает имя или псевдоним владельца ключа и, по желанию, его email-адрес.

Чтобы добавить обычную запись в сертификат ключа:

1. В окне PGPkeys выделите нужный ключ, в строке меню нажмите *Ключи* > *Добавить* > *Имя*.

2. В появившемся окне *Имя нового пользователя* в поле *Новое имя для добавления к ключу* введите своё имя и в поле *Новый адрес для добавления к ключу* – адрес электронной почты. Нажмите *OK*.

3. Введите ключевую фразу и снова *OK*.

Новая идентифицирующая запись будет внесена в сертификат ключа. Если вы захотите сделать только что добавленную или любую другую запись сертификата главной (имя и

email-адрес главной записи отображаются в имени ключа напротив иконки , а сама запись стоит первой в списке), выберите нужную, в строке меню нажмите *Ключи* > *Установить как основное имя* и введите ключевую фразу.

Не забывайте, что после редактирования открытого ключа или внесения любых изменений в содержание его сертификата, ключ нужно обновить на сервере.

Кроме адреса электронной почты сертификат ключа может включать любые другие идентификационные сведения.

Чтобы внести в сертификат иные записи с различными типами идентификации:

1. В окне PGPkeys выделите нужный ключ, в строке меню нажмите *Ключи* > *Добавить* > *Имя*.

2. В появившемся окне *Имя нового пользователя* в поле *Новое имя для добавления к ключу* введите своё имя и в поле *Новый адрес для добавления к ключу* – идентификационные сведения. Если добавляете свой номер ICQ для шифрования переговоров при помощи плагина, укажите ID в следующем формате: *ICQ:номер*. Нажмите *OK*.

3. Введите ключевую фразу и снова *OK*.

Не забудьте обновить ключ на сервере.

В PGP 6.0 и выше вы также можете добавить в сертификат ключа типа DH/DSS фотографическое удостоверение.

Никогда не опирайтесь на фото-удостоверения для определения подлинности полученного открытого ключа! Используйте их только для первичной идентификации.

Чтобы добавить фото-удостоверение:

1. В окне PGPkeys выделите нужный ключ, в строке меню нажмите *Ключи* > *Добавить* > *Фотографию* (рисунок 2.17).

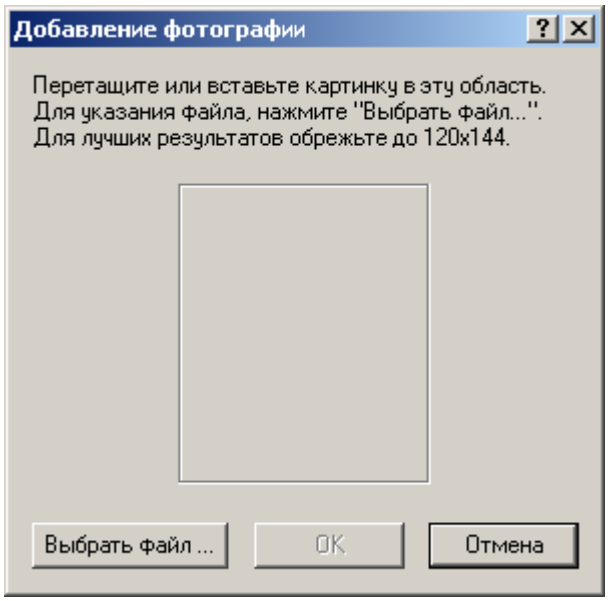



Рис. 2.17

2. Можете добавить фотографию в появившееся окно *Добавление фотографии* тремя разными способами: её можно копировать и вставить (используя клавиши *Ctrl+C / Ctrl+V*), можно перетащить графический файл из Проводника, можно нажать кнопку *Выбрать файл* и выбрать его вручную. Так или иначе, используйте картинку в формате jpeg или bmp (в последнем случае программа конвертирует файл в jpeg автоматически) и, для лучшего качества, с габаритами 120x144 пикселей.

3. Выбрав картинку нажмите *OK*.

4. Введите ключевую фразу и снова *OK*.

Фотография будет добавлена к сертификату в виде отдельной записи. Теперь обновите ключ на сервере, чтобы каждый пользователь мог её увидеть в окне свойств полученной им копии вашего ключа.

Если хотите заменить текущую фотографию (при замене будут потеряны все подписи, заверяющие текущее фото-удостоверение):

1. В окне PGPkeys разверните список записей сертификата нужного ключа. Найдите запись вида "Фотография".

2. Выделите эту запись, в строке меню нажмите *Правка* > *Удалить*.

3. Добавьте новую фотографию, как было описано выше. По окончании не забудьте обновить ключ на сервере.

### 2.3.5 Аннулирование ключа

Если по какой-то причине у вас возникнет подозрение или станет доподлинно известно, что ваша ключевая пара была скомпрометирована, нужно немедленно уведомить всех текущих и будущих корреспондентов не использовать данный открытый ключ для обмена информацией с вами, ибо велик шанс её попадания в чужие руки. Наиболее быстрый и удобный способ сделать это – выпустить сертификат аннулирования ключа (Key Revocation Certificate, KRC). Он будет присоединён к открытому ключу и аннулирует его, а после импортирования этой копии ключа на связку корреспондент не сможет использовать его для зашифрования информации.

Аннулированная ключевая пара не может использоваться для зашифрования и подписания информации. Но ей можно продолжать пользоваться для расшифрования и сверки ЭЦП (в последнем случае вы всякий раз будете получать предупреждение, что ключ аннулирован).

Кроме аннулирования своих ключей вы можете отзывать с чужих ключей собственные сертифицирующие подписи, например, если посчитаете, что ключ скомпрометирован и вы более не можете гарантировать его целостность и принадлежность только изначальному

владельцу, или если по иным причинам не захотите, чтобы другие пользователи полагались на вашу подтверждающую подпись. Аннулированная подпись никогда не берётся в расчёт при вычислении достоверности ключа.

Чтобы аннулировать свою ключевую пару или отозвать подтверждающую подпись с чужого сертификата:

1. В окне PGPkeys выделите нужный ключ или свою ЭЦП, и в строке меню нажмите *Ключи* > *Аннулировать*.

2. На просьбу подтвердить свои намерения ответьте *Да*, если действительно хотите это сделать.

3. Введите ключевую фразу (при отзыве подписи – ключевую фразу того ключа, которым ставили эту подпись) и нажмите *OK*.

Ключевая пара или подтверждающая подпись будет аннулирована и отмечена иконкой  или  соответственно. Обязательно обновите ключ на сервере и разошлите уведомления с копиями ключа всем своим постоянным корреспондентам!

Но может сложится и иная ситуация. Допустим, вы забудете свою ключевую фразу или потеряете закрытый ключ (например, после серьёзного системного сбоя). Без закрытого ключа и ключевой фразы вы не сможете издать KRC, чтобы аннулировать открытый ключ и не допустить шифрование им информации, которую теперь тоже невозможно прочитать. Если вы не резервировали свой закрытый ключ, чтобы восстановить его в случае потери, описанный сценарий безнадёжен.

В качестве меры предосторожности можно уполномочить одного или нескольких доверенных человек в чрезвычайной ситуации аннулировать ваш ключ. Эти "отменители" смогут издать сертификат KRC собственными закрытыми ключами без всякого вмешательства с вашей стороны. (Эта функция поддерживается только в PGP 6.0 и выше для ключей типа DH/DSS.)

Чтобы добавить "отменителя":

1. В окне PGPkeys выделите нужный ключ, и в строке меню нажмите *Ключи* > *Добавить* > *Аннулирование*.

2. В появившемся списке ключей выделите те из них, владельцам которых хотите дать полномочия аннулирования. Нажмите *OK*.

3. На просьбу подтвердить свои намерения ответьте *Да*, если действительно хотите это сделать.

4. Введите ключевую фразу и нажмите *OK*.

Владельцы указанных вами ключей получат полномочия аннулирования и смогут аннулировать ваш ключ, как и любой собственный. Обязательно передайте им обновлённую копию своего ключа, а также отправьте его на сервер.

Также нужно отметить один крайне важный нюанс. Если ваш ключ был аннулирован "отменителем", то, чтобы у стороннего пользователя он выглядел таковым (), и ваш открытый ключ, и открытый ключ "отменителя" должны присутствовать на его связке. Если ключа "отменителя" на связке пользователя нет, ваш аннулированный ключ будет казаться ему нормальным, и он будет продолжать шифровать им информацию. Поэтому ключ "отменителя" должен находиться в относительно широком распространении и, по меньше мере, его копия должна храниться на общественном сервере-депозитарии.

Если уполномоченный отменитель недостаточно добросовестен и есть опасение, что он может злонамеренно аннулировать ваш ключ без всякой на то необходимости, можно поступить иначе. Небезынтересна такая схема: вы создаёте новую ключевую пару, которую добавляете к своему главному ключу в качестве доверенного отменителя. Открытый ключ этой новой пары вы отправляете на сервер, закрытый разделяете на несколько долей, каждую из которых отдаёте на хранение относительно доверенному человеку. В форс-мажорной ситуации все они по вашей просьбе реконструируют этот закрытый ключ и аннулируют им ваш собственный.

### 2.4 Работа с буфером обмена и активным окном

Хотя шифрование электронной почты более удобно осуществлять с помощью плагинов, далеко не все мэйл-клиенты поддерживают их, да и сами плагины отсутствуют в бесплатной freeware-версии PGP. Однако программа предоставляет ничуть не более сложный способ криптографирования текста – это работа с активным окном и с содержимым буфера обмена через PGPtray. Через PGPtray можно легко зашифровать, расшифровать или подписать любой текст, будь то электронное письмо или содержимое любого текстового файла, а использование комбинаций "горячих клавиш" сделает выполнение этих операций совершенно необременительным.

Два способа работы с текстом через PGPtray – активное окно и буфер обмена – в целом равнозначны. Но если для зашифрования текста в буфере обмена этот текст предварительно нужно туда скопировать, работа с содержимым активного окна более автоматизирована. Немного попрактикуйтесь, и вы сами почувствуете разницу и определите применимость каждого способа для решения тех или иных задач.

#### 2.4.1 Зашифрование и подписание текста

Как правило, удобнее и проще шифровать текст с помощью функции активного окна. Если вам нужно зашифровать или подписать не всё содержимое окна, а только фрагмент

находящегося там текста, достаточно его выделить и, оставив окно в фокусе, выполнить те же инструкции, что и для содержимого окна целиком.

1. Напишите своё письмо, как вы делаете это в обычных условиях. Можно использовать любой текстовый редактор, мэйл-клиент и даже веб-интерфейс почтовой службы. (Желательно отправлять важные сообщения с пустым заголовком темы, чтобы не давать потенциальному злоумышленнику даже малейшей информации о содержании письма.)

2. Составив письмо, выполните одно из следующих действий – они равноправны:

- оставьте окно текстового редактора активным и нажмите на иконку PGPtray ( ) > *Текущее окно* > *Зашифровать* (чтобы только зашифровать), *Подписать* (чтобы только подписать) или *Зашифровать и подписать* (чтобы одновременно подписать и зашифровать своё письмо);
- оставьте окно текстового редактора активным и нажмите комбинацию "горячих клавиш", соответствующую требуемой операции с текстом;
- выделите и копируйте текст в буфер обмена (Ctrl+C), нажмите на иконку PGPtray ( ) > *Буфер обмена* > *требуемая операция с текстом* (опция *Очистить* так же позволяет очистить буфер обмена, а *Редактировать* – отредактировать его содержимое).

3. Если вы шифруете текст, а не только подписываете его, то в открывшемся окне выбора ключей получателей *Выбор ключа* (рисунок 2.18) укажите, для каких корреспондентов хотите зашифровать своё сообщение. Не удивляйтесь количеству пунктов в верхней части окна – там представлены не отдельные открытые ключи с вашей связки, а все записи сертификатов этих ключей, которых может быть намного больше. Поэтому для каждого получателя сообщения достаточно указать всего одну запись с его ключа.

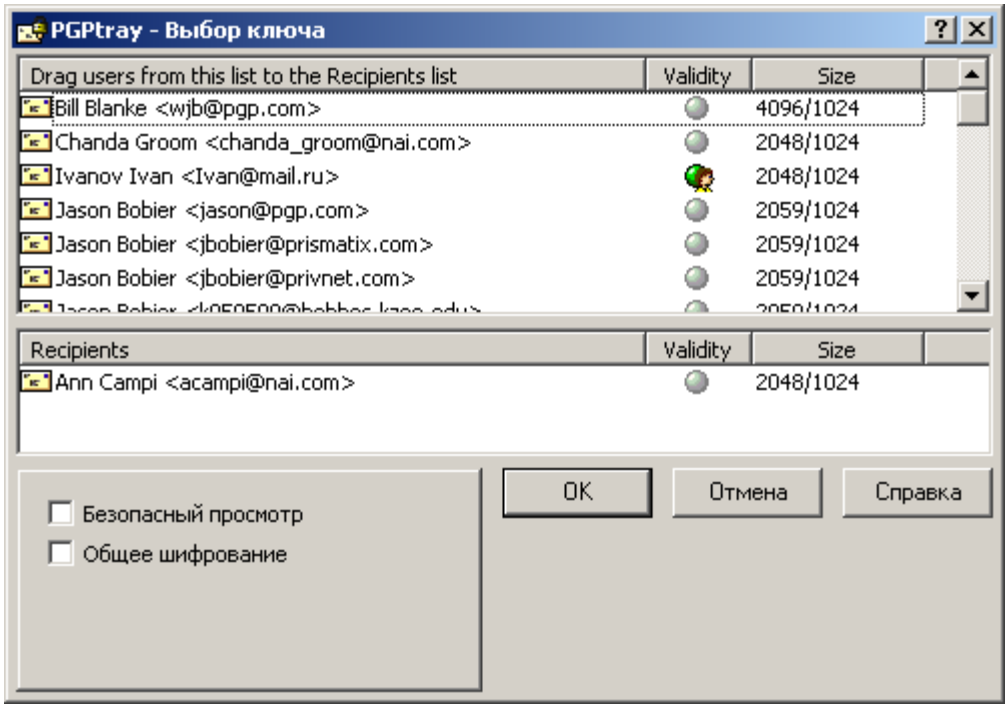


Рис. 2.18

Перетащите в нижнюю часть окна те из них, для кого вы хотите зашифровать своё послание (можно не перетаскивать, а дважды щёлкнуть по любой записи, чтобы переместить её вниз или вверх). Если у вас выбран ключ "по умолчанию", то он изначально будет присутствовать в числе получателей сообщения. Не стоит его убирать, иначе впоследствии вы сами не сможете расшифровать отправленное письмо, чтобы, скажем, его перечитать.

Индикатор *Validity* показывает степень достоверности каждой из идентификационных записей. Крайне нежелательно шифровать сообщение теми ключами (и отправлять на те адреса), которые отмечены как недостоверные. Проведите хотя бы самую элементарную и минимальную проверку подлинности данного ключа и соответствующей записи и подпишите её.

4. При необходимости отметьте дополнительные опции шифрования и нажмите *OK*:

- *Безопасный просмотр* – отображать у получателя расшифрованный текст письма в специальном окне *Безопасный просмотр*, используя шрифт, предотвращающий так называемую TEMPEST-атаку (удалённый съём информации по электромагнитному излучению монитора); кроме того, в этом случае сообщение невозможно будет сохранить в виде открытого текста. Разумно использовать для сообщений крайней секретности, но не для повседневных писем (ещё и потому, что этот поставляемый с PGP TEMPEST-защитный шрифт не имеет кириллических символов, и, соответственно, письмо придётся писать латиницей). Также имейте в виду, что в PGP до 6.0 поддержка функции *Безопасный просмотр* отсутствует, и если получатель использует более раннюю версию программы, она выбранную вами опцию просто проигнорирует.
- *Общее шифрование* – симметричное шифрование паролем вместо открытого ключа. При выборе этой опции программа предложит ввести ключевую фразу, которая потребуется и для расшифрования текста. Понятно, что использовать эту функцию для пересылки электронной почты нерационально – криптография с открытым ключом для этой цели практичнее и удобнее. Однако шифрование простым паролем может пригодиться для защиты документов, хранящихся на вашем собственном диске. (С технической точки зрения программа использует введённый пароль для шифрования сеансового ключа, которым шифруется само сообщение по алгоритму, указанному как *Назначенный алгоритм* в настройках PGP.)

5. Если вы электронно подписываете текст, а не только шифруете его, программа попросит ввести ключевую фразу вашего закрытого ключа (если у вас несколько ключевых пар, в меню *Ключи подписи* можно выбрать ключ для подписания).

Учтите, что если у вас выбран ключ "по умолчанию", и его ключевая фраза в данный момент хранится в кэше, этот запрос не появится – PGP автоматически подпишет текст вашим основным ключом. Чтобы выбрать другой ключ вам потребуется предварительно удалить ключевую фразу из оперативной памяти (*PGPtray* > *Буфер обмена* > *Очистить*).

PGP зашифрует / подпишет текст и заменит оригинал криптографированным материалом (рисунок 2.19). (Если вместо работы с активным окном вы предпочли работу с буфером обмена, вам самим придётся вставить обработанный текст в нужное приложение.)

```
-----BEGIN PGP MESSAGE-----
Version: PGPfreeware 6.5.8 for non-commercial use <http://www.pgp.com>
Comment: Так будет выглядеть зашифрованное сообщение

qANQR1DBwU4DJdJ0oint1icQCADpr4Q6iSkbMZz0MTfTHSGFfpiFv7nPMUmO90El
olIbO8y1d7i2qqCE3PvcWd8jGEvQrtOk0pW2ACslJaVfLaVr45CAE7YX/BCGismx
rq9fvZd10RhlyeVcbqyAn5i4RRVJzKugQRyVxYajfMrJpObqVfbj76JElfNQZTFV
bR0bQd2JLLz/6mRN/zqAZf/LLJRVPoAhjM6JQQ1jZ+PmIID9tpX1WWCJ0sHuHgzE
qJDtGChTlIA1QtCgssmPQwIAOgcPI+laCeJ7b7ZR/agyAGlk2TXifnBch/8wyiLN
EbLeywjxbbkWSR11/Ce2/Kzg7z5mhGKjr7ddrLrN+DG7VrJ7B/9Lo3fgeehFMJ7o
iteuOS7xVflSKbMUMRrPBAEb0mOmRJyMgzNFxJLY3raaTIPSwjmAlZn/4rnFYYxr
yIm8r2Vts0C/50PD1N5j59UEXWI5jbJbb4Tn/49jAISTiEHrUmAG2SQSU8GMIafr
JFyYrLOutvhdPR4DR2o/K2zjT23YooWuH2Cqw05SSnex2I84IZMt8OljfQ6NshKV
NCXvJ0DA1gUKKbs0o/7GdKfdb7D/TIAKrptBrujYNlli/OARaeA9p7rygZXXy0gj
j16vPmQ9hw8phjENM21PnxRTWS5rKcC6mcs+eRQoTsL9GtyLn4gzrhrNRLTt23pF
cDK1qP60ycGhMO7aJLo2aLVruBYu5rX1kqkgCox/r1bexHmWqBEpYqRZ8+wRhgdu
nk4RFFe4/qSVK343CeHZiedOIDBCXAi3a20arH6XU+gZQQ+1IKNSws6vw8bOnf9S
WZ3f/IuZTZDpZbU6FymkPvRv+6sSsbAugff4asW5PD8rEXBrE74EZNUSMPTzyWxO
IbkCD/s7nTbOlVQQJu0iiNHxza2eU3Qs19CjfADzFYehVkpGWv/CP4KrhzFYFuZR
yTKtPqaiu5NzYlS/hDxcjYTYfnAja3RLLgC2JWNSIqJ0kX7vweNo8oApI+nLxlaO
SvZ8yoheelMcU4TK02jWRKXSSKMQwLYfLiHWiiTU6zHbeFGpvqkhKTVtSe1QrNG6
nIPgyYB3/33psJgBUCq0IhlrvYIU09gmyjsDNB/VX0EgCWKmOakduUWbREEDgXNr
Jxdj5ZDmBBnfBMCEg6Jgo40hiYroh+Z1IrhLTGNd9iKCENlCz6Tpv5FI6vi1wYpi
9GZtepAkD9RSdC6Puu2esi4uGWHmGkb/d17DKn2zZ9xMxzjI8kViIYzsKxVzDb/M
bNFQL24pQndFzwkKdDIi2sXAEn/fZradtbs7caSsxC2dBu+wc7UAnGoTbWp6p+r7
m0VL2ioUwPodvc09zAxB3TdLPGu9/n4qFh0fZHjSpw+Hom77aQerE1KhbkQs34KT
X67eVp4Upm0OIPWJgQW3U8VMksYxFgCuUrHGZWaV6N3ZtFUCqSAF52zdHgOYV1GJ
38US8ztJqQ3nkwIC6wJCJX3NOSAjqZaR1TGT7NCtfx+JV6NYSBRxv5wa
=G8km
-----END PGP MESSAGE-----
```

Рис. 2.19

### 2.4.2 Расшифрование и сверка ЭЦП

Расшифрование текста и сверка цифровой подписи особенно легки с использованием "горячих клавиш" – достаточно пары нажатий. В остальных случаях, как и с шифрованием, можно использовать PGPtray. Если вы хотите расшифровать сообщение через буфер обмена, нужно выделить весь блок шифртекста вместе с заголовками типа “-----BEGIN PGP MESSAGE-----”, “-----END PGP SIGNATURE-----” и др. и целиком копировать его в буфер обмена.

Как правило, попытка расшифровать сообщение через активное окно прямо со страницы веб-сайта приводит к ошибке. Так случается потому, что веб-страницы обычно содержат графику и множество других нетекстовых элементов. Но чтобы не копировать шифртекст в буфер обмена можно пойти на маленькую хитрость: достаточно выделить шифртекст в окне браузера и затем нажать комбинаю клавиш для расшифрования или указать эту же команду через меню работы с активным окном в PGPtray.

Чтобы расшифровать текстовое сообщение и/или сверить его электронную подпись:

1. Откройте сообщение в своём мэйл-клиенте (если это письмо), текстовом редакторе или веб-браузере. Если оно зашифровано, а не только подписано, вы увидите лишь нечитаемый шифртекст.
2. Выполните одно из следующих действий – они равноправны:

- оставьте окно текстового редактора активным и нажмите на иконку PGPtray (  ) > *Текущее окно* > *Расшифровать и Проверить* (чтобы расшифровать сообщение и/или сверить ЭЦП);
- оставьте окно текстового редактора активным и нажмите комбинацию "горячих клавиш", соответствующую операции расшифрования;
- выделите блок шифртекста вместе с заголовками и копируйте его в буфер обмена (Ctrl+C), нажмите на иконку PGPtray (  ) > *Буфер обмена* > *Расшифровать и Проверить*.

3. Появится окно *Введите пароль* со списком открытых ключей, которыми зашифровано сообщение. Если сообщение предназначено вам, программа попросит ввести ключевую фразу одного из ваших закрытых ключей. Если же вместо поля для ввода ключевой фразы в окошке указана ошибка *"Невозможно расшифровать данное сообщение ..."*, причина этого в том, что у вас на связке нет нужного для расшифрования закрытого ключа (он мог быть удалён, либо отправитель намеренно или случайно не зашифровал письмо вашим открытым ключом).
4. Введите ключевую фразу и нажмите *OK*.

Программа расшифрует сообщение и отобразит результат в окошке *Просмотр текста*. Если сообщение было подписано, там же будет указано состояние цифровой подписи.

Если при зашифровании отправитель отметил опцию *Безопасный просмотр*, PGP выдаст предупреждение, что письмо предназначено только для ваших глаз и его стоит читать с соблюдением максимальных мер предосторожности. Когда будете готовы открыть сообщение, нажмите *OK*. Текст будет выведен в окне *Безопасный просмотр* с помощью специального TEMPEST-защитного шрифта. (Имейте в виду, что ни копировать его, ни сохранить в расшифрованном виде вам не удастся.)

Если полученное сообщение было подписано, программа также сообщит вам некоторые сведения о цифровой подписи (рисунок 2.20).

```
*** СТАТУС ПОДПИСИ PGP: хороший
*** Подписыватель: Ivanov Ivan <Ivan@mail.ru>
*** Подписано: 17.12.04 13:21:52
*** Проверено: 19.12.04 5:58:28
*** НАЧАЛО РАСШИФРОВАННОГО/ПРОВЕРЕННОГО СООБЩЕНИЯ PGP ***

Текст подписанного сообщения

*** КОНЕЦ РАСШИФРОВАННОГО/ПРОВЕРЕННОГО СООБЩЕНИЯ PGP ***
```

Рис. 2.20

Это выглядит как набор заголовков, где в строке *Подписано* указана дата подписания (относительно вашего часового пояса), в *Проверено* – дата сличения подписи (т.е. текущий момент), в *Подписыватель* – имя владельца ключа, которым была поставлена подпись, а в *Статус подписи PGP* – собственно, состояние подписи:

- *Good* – информация получена вами ровно в том виде, в каком была подписана и отправлена автором.
- *Bad* – подписанная информация была каким-то образом изменена (искажена). Причиной тому могло послужить не только злонамеренное вмешательство, но и более тривиальные вещи, например, плохое качество связи, повлекшее искажение информации в процессе передачи, случайное редактирование сообщения автором уже после подписания, изменение, внесённое почтовой программой отправителя или вашей. В любом случае, к подобного рода сообщениям следует относиться с большой осторожностью; желательно также в кратчайшие сроки выяснить причину происшедшего.
- *Unknown* – это говорит о том, что на вашей связке ключей отсутствует тот, которым информация была подписана, и, следовательно, программа не может сверить подпись. В таких ситуациях PGP пытается самостоятельно связаться с сервером-депозитарием, чтобы найти соответствующий открытый ключ (если в настроках программы во вкладке *Серверы* включена опция *Удостоверение*).
- *Invalid* – так PGP уведомит вас о том, что ключ автора сообщения есть на вашей связке, но не признан подлинным, и, соотственно, программа не может оценить целостность подписанной информации. Вам нужно проверить достоверность ключа и заверить его.

При сличении подписи обязательно проверяйте, чтобы дата/время, указанные в строке *Проверено*, совпадали с текущими показаниями системных часов! Если вы не будете этого делать либо будете делать недостаточно тщательно, злоумышленник сможет одурачить вас, подсунув сформированное определённым образом составное сообщение, при расшифровании выглядящее так, словно было подписано одним из ваших доверенных

корреспондентов. Но поскольку мошенник не может доподлинно знать с точностью до секунд, в какой момент времени вы откроете письмо, указанная им в строке *Проверено* дата будет иметь расхождение с реальной датой расшифрования сообщения (т.е. с текущим моментом).

Учтите, что метка времени, стоящая в строке *Подписано*, указывает время системного таймера отправителя. Отправителю эту метку крайне легко сфальсифицировать – достаточно перед подписанием перевести системные часы.

### 2.5 Защита файлов

PGP позволяет шифровать не только текст, но и файлы для их безопасного хранения на диске или для пересылки в качестве вложений к электронным письмам. Зашифрованный файл можно без опасений размещать и в Интернете, поскольку никто кроме владельца соответствующего закрытого ключа не сможет узнать его содержание.

При шифровании папки она не будет зашифрована целиком; напротив, PGP индивидуально зашифрует находящиеся в ней файлы. Чтобы зашифровать папку с сохранением структуры каталогов, стоит предварительно упаковать её в архив (например, с помощью WinZip) и уже затем зашифровать сам архивный файл.

Плагин PGP в некоторых мэйл-клиентах не способен автоматически зашифровывать и расшифровывать вложения электронной почты. Поэтому чтобы безопасно переслать файл или извлечь его из полученного письма вам придётся вручную выполнить с ним описанные ниже действия.

Зашифрование и подписание файлов можно производить двумя способами: через контекстное меню в Проводнике Windows или с помощью утилиты PGPtools, которую можно вызвать через PGPtray. Расшифровывать же файлы проще всего в Проводнике, просто дважды щёлкнув на имя зашифрованного файла; вам понадобится только ввести нужную ключевую фразу, и в том же каталоге появится расшифрованная копия этого файла.

Чтобы выполнить ту или иную операцию над файлом с помощью PGPtools, можно либо нажать на соответствующую кнопку и указать этот файл в меню *Обзор*, либо перетащить этот файл из Проводника на нужную кнопку инструмента. Кроме того, в меню *Обзор*, вызываемом с помощью этих кнопок, присутствует опция *Буфер обмена*, позволяющая выполнить данную операцию над содержимым буфера обмена. Назначение кнопок инструмента следующее (рисунок 2.4, слева направо):

- *PGPkeys* – открыть менеджер ключей;
- *Encrypt* – зашифровать файл;

- *Sign* – подписать файл;
- *Encrypt and Sign* – подписать и зашифровать файл;
- *Decypt / Verify* – расшифровать файл и / или сверить цифровую подпись;
- *Wipe* – стереть файл с диска (уничтожить без возможности восстановления);
- *Freespace Wipe* – очистить диск от фрагментов прежде удалённых файлов.

Нажав в верхнем левом углу окошка и выбрав *Stay On Top*, вы заставите инструмент находиться поверх остальных окон.

Если вы зашифровываете файл, а не только подписываете его, то откроется окно выбора ключей получателей *Выбор ключа* (рисунок 2.21), где нужно указать, для каких корреспондентов вы хотите зашифровать этот файл. Не удивляйтесь количеству пунктов в верхней части окна – там представлены не отдельные открытые ключи с вашей связки, а все записи сертификатов этих ключей, которых может быть намного больше. Поэтому для каждого получателя файла достаточно указать всего одну запись с его ключа.

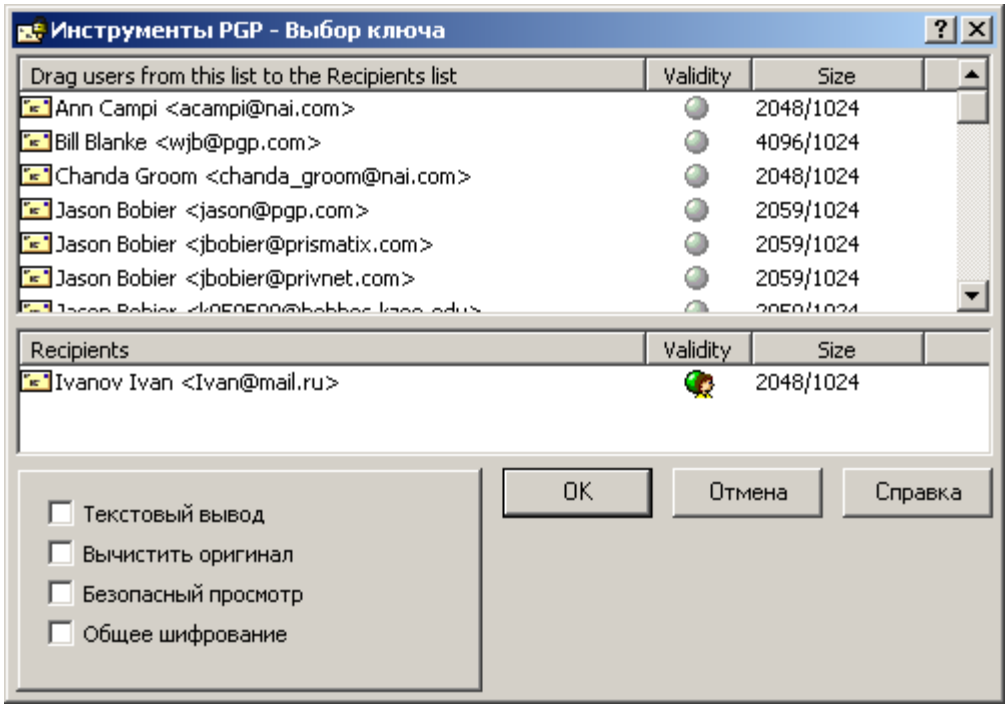



Рис. 2.21

Перетащите в нижнюю часть окна те из них, для кого вы хотите зашифровать файл (можно не перетаскивать, а дважды щёлкнуть по любой записи, чтобы переместить её вниз или вверх). Если у вас выбран ключ "по умолчанию", то он изначально будет присутствовать в числе получателей. Не стоит его убирать, иначе впоследствии вы сами не сможете расшифровать отправленный файл, и ни в коем случае не убирайте его, если шифруете файл для сохранения у себя на диске (только если ни собираетесь заменить его другим своим ключом).

Индикатор *Validity* показывает степень достоверности каждой из идентификационных записей. Крайне нежелательно шифровать файл теми ключами (и отправлять на те адреса), которые отмечены как недостоверные. Проведите хотя бы самую элементарную и минимальную проверку подлинности данного ключа и соответствующей записи и подпишите её.

При необходимости отметьте дополнительные опции шифрования и нажмите *OK*:

- *Текстовый вывод* – сохранить шифртекст не в двоичном, а в ASCII-формате (в текстовом виде). Некоторые старые мэйл-клиенты не позволяют пересылать двоичный код, и эта опция может оказаться полезной. Кроме того, таким образом можно отправлять файл не вложением, а прямо в теле письма, если открыть зашифрованный файл любым текстовым редактором и скопировать содержимое в письмо. Учтите, однако, что использование этой опции увеличит объём файла примерно на 30% (в сравнении с шифрованием с выключенной опцией, а не с исходным файлом).
- *Вычистить оригинал* – уничтожить исходный файл с открытым текстом после зашифрования, перезаписав его на диске случайными данными. Так, файл останется только в виде шифртекста, а оригинал будет более недоступен.
- *Безопасный просмотр.*
- *Общее шифрование* – симметричное шифрование паролем вместо открытого ключа. При выборе этой опции программа предложит ввести ключевую фразу, которая потребуется и для расшифрования файла. Понятно, что использовать эту функцию для пересылки файла по электронной почте нерационально – криптография с открытым ключом для этой цели практичнее и удобнее. Однако шифрование простым паролем может пригодиться для защиты файлов, сохраняемых на вашем собственном диске. (С технической точки зрения программа использует введённый пароль для шифрования сеансового ключа, которым шифруется файл по алгоритму, указанному как *Назначенный алгоритм* в настройках PGP.)

Если вы электронно подписываете файл, а не только шифруете его, программа попросит ввести ключевую фразу вашего закрытого ключа (если у вас несколько ключевых пар, в меню *Ключи подписи* можно выбрать ключ для подписания). Учтите, что если у вас выбран ключ "по умолчанию", и его ключевая фраза в данный момент хранится в кэше, этот запрос не появится – PGP автоматически подпишет файл вашим основным ключом. Чтобы выбрать другой ключ вам потребуется предварительно удалить ключевую фразу из оперативной памяти (*PGPtray > Буфер обмена > Очистить*).

Если вы только подписываете файл, окно *Введите пароль* будет содержать несколько дополнительных опций:

- *Нарушенная подпись* – изготовить "съёмную" цифровую подпись. Если опция включена (а она включена по умолчанию), цифровая подпись будет сохранена в виде отдельного крохотного файла, имеющего такое же имя, что и у подписанного файла, но с расширением.sig. Такой файл-подпись можно передавать и публиковать отдельно от подписанного, дабы не осложнять использование подписанного файла людям, не пользующимся PGP. Если опцию выключить, файл будет сохранён, как при обычном шифровании, и использовать его без сверки ЭЦП будет невозможно.
- *Текстовый вывод* – сохранить "съёмную" ЭЦП или подписанный файл (в зависимости от предыдущей настройки) не в двоичном, а в ASCII-формате (в текстовом виде). Некоторые старые мэйл-клиенты не позволяют пересылать двоичный код, и эта опция может оказаться полезной. Кроме того, таким образом можно отправлять файл не вложением, а прямо в теле письма, если открыть зашифрованный файл любым текстовым редактором и скопировать содержимое в письмо. Учтите, однако, что использование этой опции увеличит объём подписанного файла примерно на 30% (в сравнении с шифрованием с выключенной опцией, а не с исходным файлом); для "съёмной" ЭЦП это несущественно.

PGP зашифрует / подпишет файл и сохранит эту копию в том же каталоге, что и исходный файл (если при зашифровании была отмечена опция *Вычистить оригинал*, PGP уничтожит исходную копию с открытым текстом). В зависимости от характера содержимого зашифрованного файла он будет представлен одним из трех значков (таблица 2.5).

Таблица 2.5

| | |
|---|---|
|  | Файл, зашифрованный с опцией *Текстовый вывод* (шифртекст в ASCII-формате, asc-файл). |
|  | Обычный зашифрованный файл (шифртекст в двоичном формате, pgp-файл). |
|  | "Съёмная" цифровая подпись (sig-файл). |

Чтобы расшифровать файл и/или сверить ЭЦП, достаточно дважды щёлкнуть в Проводнике на имя зашифрованного файла или на sig-файл. Если файл был зашифрован, появится окно *Введите пароль* со списком открытых ключей получателей. Если файл предназначен вам, программа попросит ввести ключевую фразу одного из ваших закрытых ключей. Если же вместо поля для ввода ключевой фразы в окошке указана ошибка *"Невозможно расшифровать данное сообщение ..."*, причина этого в том, что у вас на связке нет нужного для расшифрования закрытого ключа (он мог быть удалён, либо отправитель намеренно или случайно не зашифровал файл вашим открытым ключом). Введите ключевую

фразу и нажмите *OK*. Программа расшифрует исходный файл и сохранит его в одном каталоге с шифртекстом.

Если файл был только подписан, вы сразу увидете окно отчёта PGPlog, содержащее некоторые сведения о цифровой подписи. Так, в столбце *Name* указано имя подписанного файла, в *Signer* – имя владельца ключа, которым была поставлена подпись, в *Validity* – степень достоверности ключа подписания, а в *Signed* – состояние ключа подписания (дезактивирован, аннулирован и т.п.) и самой ЭЦП: если подпись корректна, и файл был получен ровно в том виде, в как был подписан отправителем, здесь будет указана дата подписания (относительно вашего часового пояса), в иных случаях будет отмечено одно из следующих значений:

- *Bad signature* – подписанный файл был каким-то образом изменён (искажён). Причиной тому могло послужить не только злонамеренное вмешательство, но и более тривиальные вещи, например, плохое качество связи, повлекшее искажение информации в процессе передачи, случайное редактирование файла автором уже после подписания, изменение, внесённое почтовой программой отправителя или вашей. В любом случае, к подобного рода файлам следует относиться с большой осторожностью; желательно также в кратчайшие сроки выяснить причину происшедшего.
- *Unknown signing key* – это говорит о том, что на вашей связке ключей отсутствует тот, которым файл был подписан, и, следовательно, программа не может сверить подпись. В таких ситуациях PGP пытается самостоятельно связаться с сервером-депозитарием, чтобы найти соответствующий открытый ключ (если в настроках программы во вкладке *Серверы* включена опция *Удостоверение*).
- *Invalid key* – так PGP уведомит вас о том, что ключ отправителя файла есть на вашей связке, но не признан подлинным, и, соотственно, программа не может оценить целостность подписанной информации. Вам нужно проверить достоверность ключа и заверить его.

Учтите, что метка времени, стоящая в строке *Signed*, указывает время системного таймера отправителя. Отправителю эту метку крайне легко сфальсифицировать – достаточно перед подписанием перевести системные часы.

### 2.6 Уничтожение данных

Создавая и удаляя важные документы обычными средствами операционной системы, вы оставляете информацию, содержавшуюся в удалённых файлах, лежать в освободившемся пространстве жёсткого диска. Когда вы удаляете файл, помещая его в Корзину, он по сути просто перемещается из одного каталога в другой. Но и очистив Корзину, вы не сотрёте

файл с диска окончательно, пока ОС не перезапишет высвобожденные сектора (это может случиться очень нескоро). Более того, многие программы и почти все текстовые процессоры создают в ходе работы множество резервных копий редактируемых документов. Хотя эти копии удаляются программой по завершении работы, содержавшаяся в них информация по-прежнему остаётся записанной на диске. В общем смысле, ценные файлы никогда не исчезают полностью, и при наличии должных инструментов могут быть восстановлены в первоначальный вид.

Если вам нужно безвозвратно стереть файл с лица жёсткого диска, используйте утилиту PGP Wipe. Она удаляет файл, многократно перезаписывая сектора диска, в которых он находился, случайными данными ("мусором") так, что его не удастся восстановить даже самыми совершенными коммерческими средствами.

Для очистки всего диска от остатков прежде удалённых файлов предназначена утилита PGP Freespace Wipe. Во-первых, она перезаписывает все свободные сектора диска, уничтожая фрагменты невостребованной информации, во-вторых, очищает частично занятые сектора диска в "хвостах" хранящихся на диске файлов (так называемый slack space).

Эти файловые системы сохраняют в своей специальной внутренней области резервные копии всех записей, вносимых ОС в файловую систему – ведут журнал изменений. Такой журнал представляет собой последовательное описание всех изменений, произведённых на диске, и служит цели надёжного восстановления ФС и содержимого диска после системных сбоев, однако, и усложняет задачу надёжного уничтожения данных. Стирание файла с помощью PGP Wipe не способно удалить все журнальные записи, вероятно сделанные файловой системой.

Обе утилиты можно вызвать из PGPtools с помощью соответствующих кнопок в правой части инструмента:  для PGP Wipe и  для Freespace Wipe. Кроме того, функция PGP Wipe доступна из контекстного меню в Проводнике Windows по нажатии правой кнопки на имени файла или папки, а также через интерфейс шифрования файлов.

Чтобы надёжно стереть файл с жёсткого диска:

1. Выделите в Проводнике файлы и/или папки, подлежащие уничтожению.

2. Нажмите правой кнопкой мыши на выделенные объекты, выберите в контекстном меню пункт *PGP > Wipe*.

3. В появившемся окне с перечнем удаляемых файлов / папок нажмите *Да*, чтобы подтвердить свой выбор, или *Нет*, чтобы отказаться от уничтожения этих файлов. Не забывайте, это последняя возможность передумать.

Ту же операцию можно проделать с помощью PGPtools: для этого нажмите кнопку *Wipe* (), укажите файлы, подлежащие уничтожению (или перетащите файлы на эту кнопку из Проводника), и подтвердите свой выбор, нажав *Да*.

Чтобы очистить свободное пространство диска от остатков удалённых файлов с помощью утилиты PGP Freespace Wipe:

1. В окне PGPtools нажмите кнопку *Freespace Wipe* (). Появится окно мастера с приветственным сообщением (рисунок 2.22).

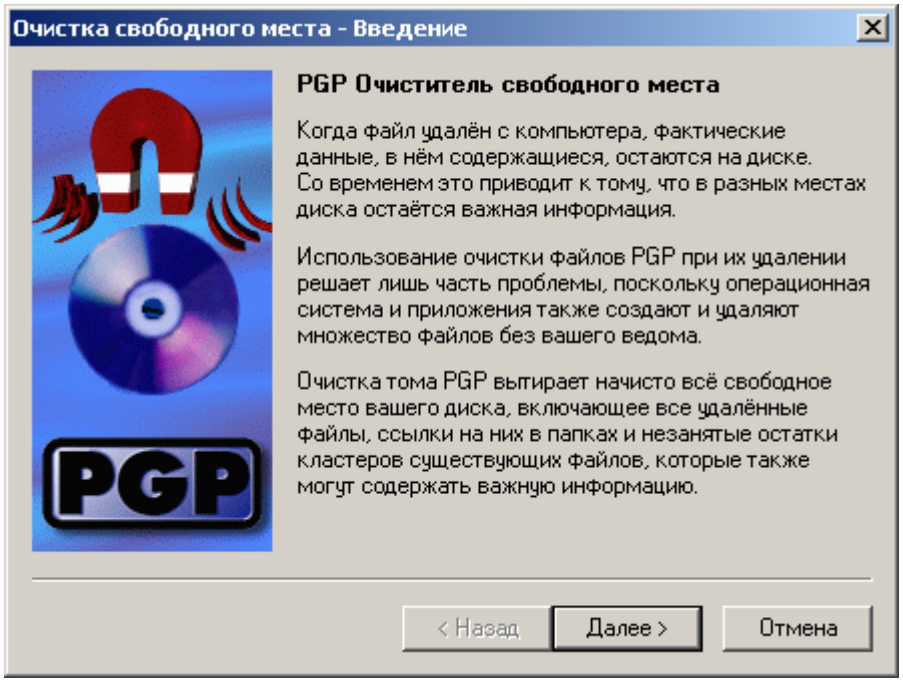



Рис. 2.22

2. Нажмите *Далее*.

3. Укажите параметры данного сеанса очистки (рисунок 2.23). В поле *Очистить диск* выберите диск, подлежащий очистке, и введите число проходов очистки (количество перезаписей свободного пространства диска).

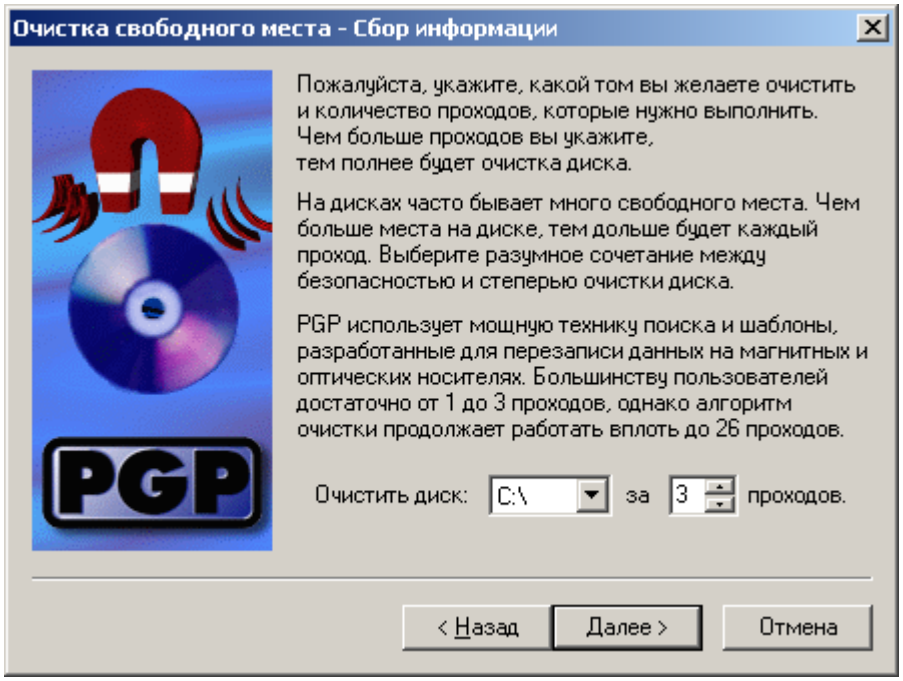



Рис. 2.23

4. Чтобы продолжить, нажмите *Далее*.

На следующей странице мастера (рисунок 2.24) будут отображены технические сведения о выбранном для очистки разделе диска и график выполнения операции.

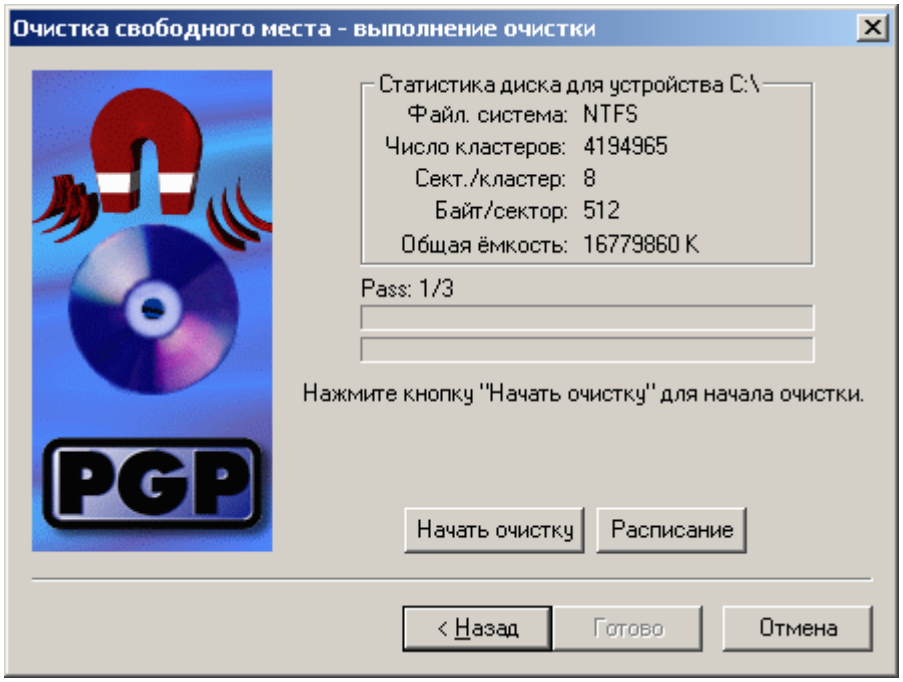



Рис. 2.24

5. Нажмите кнопку *Начать очистку*, чтобы приступить к очистке свободного пространства. Ход очистки можно прервать в любой момент, нажав кнопку *Отмена*. Однако это оставит на диске не перезаписанные фрагменты файлов.

По окончании процесса очистки в нижней части окна появится сообщение *Поздравляем! Диск был очищен*.

6. Для завершения работы мастера нажмите *Готово* (рисунок 2.25).

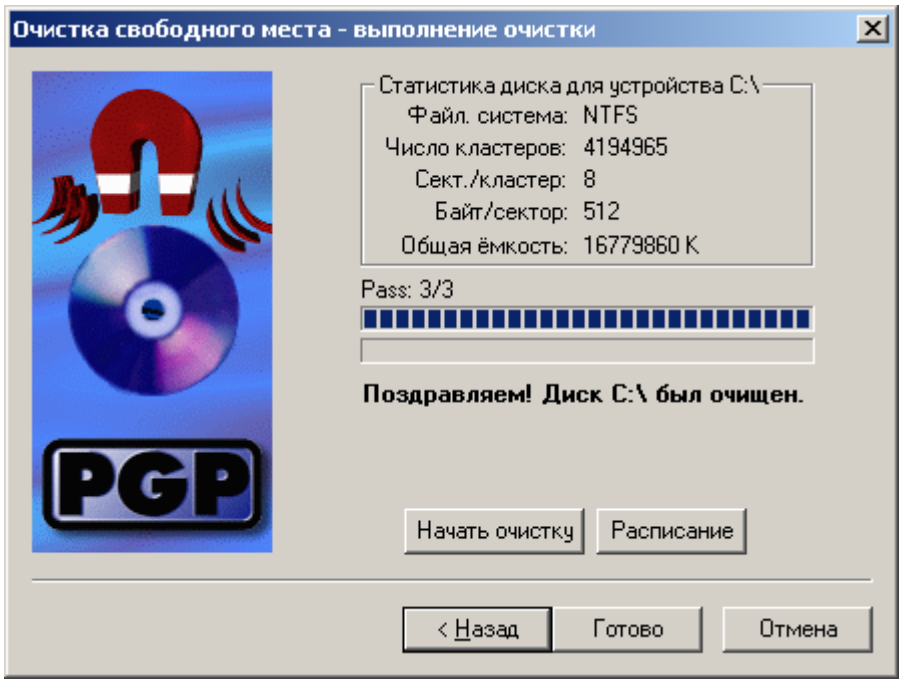



Рис. 2.25

С помощью утилит PGP Wipe и Freespace Wipe и Планировщика Windows можно создать ряд заданий для регулярной очистки свободного пространства тех или иных дисков или уничтожения содержимого определённых папок.

Чтобы запланировать регулярную очистку свободного пространства диска с помощью PGP Freespace Wipe:

1. В окне PGPtools нажмите кнопку *Freespace Wipe* ( ).
2. В окне мастера очистки нажмите *Далее*.
3. В поле *Очистить диск* выберите диск, подлежащий регулярной очистке, введите число проходов очистки
4. Чтобы продолжить, нажмите *Далее*.
5. На странице *Очистка свободного места – выполнение очистки* нажмите кнопку *Расписание*.
6. Если хотите запланировать регулярную очистку свободного пространства выбранного диска с указанными настройками, то в ответ на предупреждение нажмите *OK*.

Работая в Windows NT вам потребуется ввести свой логин и пароль. Сделайте это в появившемся окошке.

7. В открывшемся окне Планировщика заданий Windows (рисунок 2.26) укажите периодичность выполнения операции (ежедневно, еженедельно, при простое и т.д.) и, если нужно, время начала выполнения очистки.

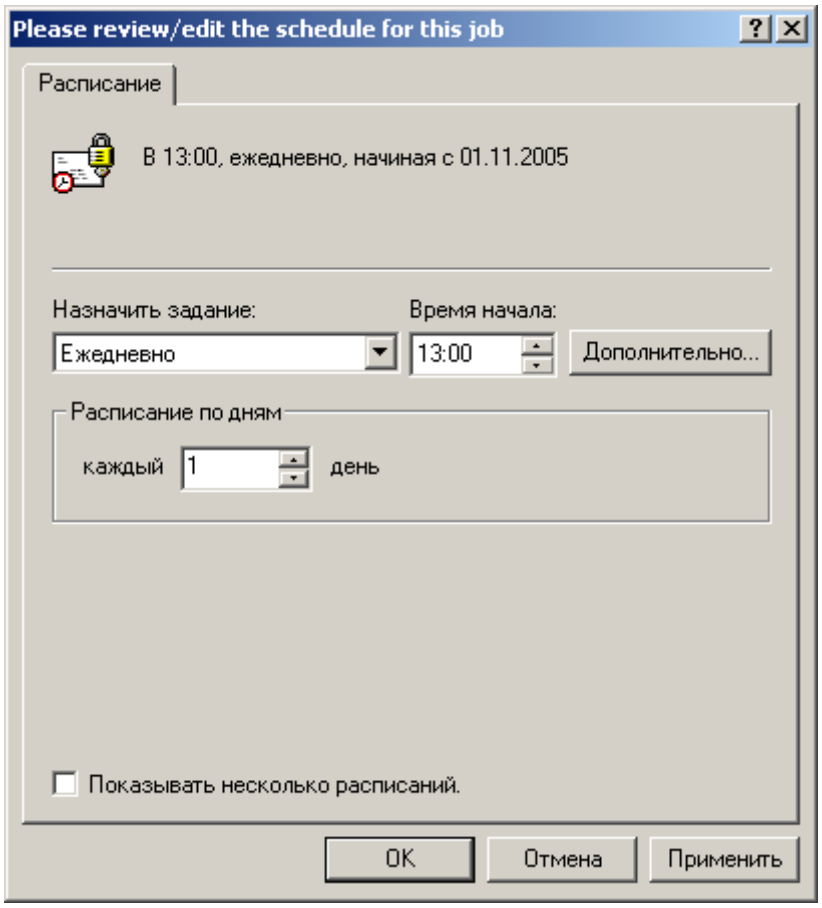



Рис. 2.26

8. В разделе *Дополнительных* настроек можете указать некоторые расширенные параметры выполнения задания, в частности, дату начала, дату окончания выполнения задания, график повторов и пр.

9. Закончив планирование задания нажмите *OK*.

Если в дальнейшем вам потребуется изменить порядок выполнения задания или отменить его, откройте Планировщик, находящийся в системном трее по соседству с PGPtray.

**3 Задание на лабораторную работу**

1. Изучите вкладки окна “Настройки PGP”.
2. Создайте с помощью менеджера PGPkeys ключи шифрования двух типов: RSA и DH/DSS.
3. Сохраните полученные ключи (открытые и секретные) в отдельный файл.

4. Назначьте ключ DH/DSS используемым по умолчанию.
5. Дезактивируйте ключевую пару RSA.
6. Активируйте ключевую пару RSA.
7. Аннулируйте ключевую пару RSA.
8. Изучите свойства ключевой пары DH/DSS:

8.1. измените пароль;

8.2. добавьте подключ;

8.3. аннулируйте созданный подключ;

8.4. добавьте фото-удостоверение.

9. Обменяйтесь с другим студентом открытыми ключами DH/DSS.
10. Импортируйте/вставьте полученный ключ на связку.
11. Установите подлинность полученного ключа с помощью его отпечатка.
12. Установите степень доверия к владельцу полученного ключа на максимальный уровень.
13. Зашифруйте произвольное сообщение/файл и обменяйтесь полученным результатом с другим студентом. Расшифруйте полученное сообщение.
14. Подпишите произвольное сообщение/файл и обменяйтесь полученным результатом с другим студентом. Проверьте достоверность источников полученного сообщения.
15. Подпишите и зашифруйте произвольное сообщение/файл и обменяйтесь полученным результатом с другим студентом. Расшифруйте полученное сообщение и проверьте достоверность его источников.
16. Уничтожьте все ненужные файлы, используя утилиту PGP Wipe.
17. Сделайте отчет по проделанной работе. Отчет должен содержать

17.1. цель работы;

17.2. описание выполненных действий по каждому пункту задания;

17.3. открытые и секретные ключи, полученные в ходе выполнения работы;

17.4. открытый ключ, полученный от другого студента;

17.5. результаты шифрования/расшифрования, подписи/верификации сообщений/файлов;

17.6. выводы по проделанной работе.

## 4 Контрольные вопросы

1. Что такое асимметричная криптографическая система? В чем ее преимущества перед симметричной системой? В чем недостатки?

2. Какие проблемы безопасности позволяет решить криптографическая защита информации? В чем они заключаются?
3. Что такое цифровая подпись? В чем ее отличие от рукописной подписи?
4. Какие задачи позволяет решить цифровая подпись?
5. Какие функции входят в состав PGP?
6. Какие типы ключей используются в PGP?
7. В чем различие между аннулированием и удалением ключа?
8. Что такое “отпечаток ключа” и для чего он используется?
9. Что такое “имплицитное доверие”?
10. Какую информацию может содержать сертификат открытого ключа PGP?
11. Каким образом в PGP производится надёжно удаление файлов с жёсткого диска?

## 9. Компьютерный практикум

**Система анализа рисков и проверки политики информационной безопасности предприятия**

**Основные определения**

*Безопасность (защищенность) информации в компьютерных системах (КС)* - это такое состояние всех компонент КС, при котором обеспечивается защита информации от возможных угроз на требуемом уровне. Компьютерные системы, в которых обеспечивается безопасность информации, называются защищенными [1].

Информационная безопасность достигается проведением руководством соответствующего уровня *политики информационной безопасности***.** Основным документом, на основе которого проводится политика информационной безопасности, является *программа информационной безопасности***.** Этот документ разрабатывается и принимается как официальный руководящий документ высшими органами управления организацией. В документе приводятся цели политики информационной безопасности и основные направления решения задач защиты информации в КС. В программах информационной безопасности содержатся также общие требования и принципы построения систем защиты информации в КС.

Под *системой защиты информации в КС* понимается единый комплекс правовых норм, организационных мер, технических, программных и криптографических средств, обеспечивающий защищенность информации в КС в соответствии с принятой политикой безопасности.

*Угроза безопасности* - потенциально возможное происшествие, которое может оказать воздействие на информацию в системе.

*Уязвимость* - некая неудачная характеристика системы, которая делает возможным возникновение угрозы.

*Атака* - действие по использованию уязвимости КС; атака - это реализация угрозы.

*Угроза конфиденциальности* - угроза раскрытия информации.

*Угроза целостности* - угроза изменения информации.

*Угроза доступности* - угроза нарушения работоспособности системы при доступе к информации.

*Ущерб* - стоимость потерь, которые понесет компания в случае реализации угроз конфиденциальности, целостности, доступности по каждому виду ценной информации. Ущерб зависит только от стоимости информации, которая обрабатывается в автоматизированной системе. Ущерб является характеристикой информационной системы и не зависит от ее защищенности.

*Риск* - вероятный ущерб, который зависит от защищенности системы. По определению риск всегда измеряется в деньгах.

В сущности, для коммерческой организации задача безопасного функционирования информационной системы сводится к выработке правил и выбору защитных средств. Комбинация двух этих составляющих позволит обеспечить необходимый уровень безопасности, как для ценных ресурсов организации, так и для всей информационной системы обработки этих ресурсов. Другими словами задача защиты – это разработка эффективной политики безопасности (или правил безопасности).

Чтобы меры политики безопасности по защите отвечали реальному состоянию дел необходимо знать - что, от кого и в какой степени нужно защищать. На сегодня существует только один процесс, способный в какой то мере дать ответы на поставленные вопросы, речь идет об анализе рисков.

## 1. Обзор программных продуктов в области анализа рисков и проверки организационных мер обеспечения информационной безопасности

В настоящее время имеется большое разнообразие как методов анализа и управления рисками, так и реализующих их программных средств. Приведем примеры некоторых отечественных продуктов.

### 1.1 Программный комплекс анализа и контроля рисков информационных систем компании – ГРИФ

Для проведения полного анализа информационных рисков прежде всего необходимо построить полную модель информационной системы с точки зрения ИБ. Для решения этой задачи ГРИФ, в отличие от представленных на рынке западных систем анализа рисков, которые громоздки, сложны в использовании и часто не предполагают самостоятельного применения ИТ-менеджерами и системными администраторами, ответственными за обеспечение безопасности информационных систем компаний, обладает простым и интуитивно понятным для пользователя интерфейсом. Однако за внешней простотой скрывается сложнейший алгоритм анализа рисков, учитывающий более ста параметров, который позволяет на выходе дать максимально точную оценку существующих в информационной системе рисков, основанную на глубоком анализе особенностей практической реализации информационной системы. Основная задача системы ГРИФ – дать возможность ИТ-менеджеру самостоятельно (без привлечения сторонних экспертов) оценить уровень рисков в информационной системе, оценить эффективность существующей практики по обеспечению безопасности компании и иметь возможность доказательно (в цифрах) убедить топ-менеджмент компании в необходимости инвестиций в сферу информационной безопасности компании [2].

1.1. На первом этапе система ГРИФ проводит опрос ИТ-менеджера с целью определения полного списка информационных ресурсов, представляющих ценность для компании.

1.2. На втором этапе проводится опрос ИТ-менеджера с целью ввода в систему ГРИФ всех видов информации, представляющей ценность для компании. Введенные группы ценной информации должны быть размещены пользователем на ранее указанных на предыдущем этапе объектах хранения информации (серверах, рабочих станциях и так далее). Заключительная фаза – указание ущерба по каждой группе ценной информации, расположенной на соответствующих ресурсах, по всем видам угроз.

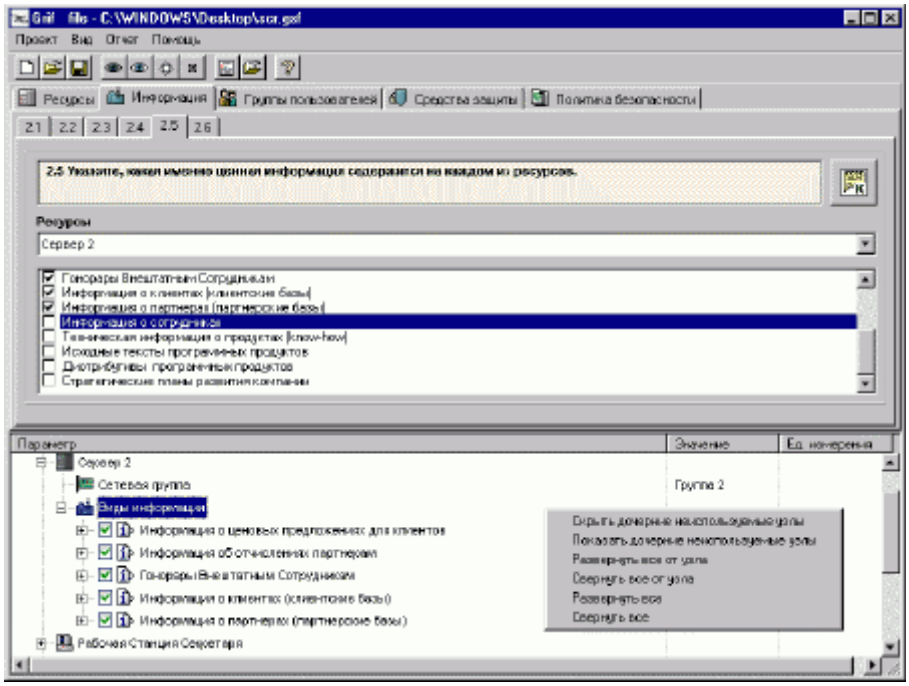



Рисунок.1.1. Интерфейс программного комплекса Гриф. Вкладка “Информация”.

1.3. На третьем этапе вначале проходит определение всех видов пользовательских групп (и число пользователей в каждой группе). Затем определяется, к каким группам информации на ресурсах имеет доступ каждая из групп пользователей. В заключение определяются виды (локальный и/или удаленный) и права (чтение, запись, удаление) доступа пользователей ко всем ресурсам, содержащим ценную информацию.

1.4. На четвертом этапе проводится опрос ИТ-менеджера для определения средств защиты информации, которыми защищена ценная информация на ресурсах. Кроме того, в систему вводится информация о разовых затратах на приобретение всех применяющихся средств защиты информации и ежегодные затраты на их техническую поддержку, а также ежегодные затраты на сопровождение системы информационной безопасности компании.

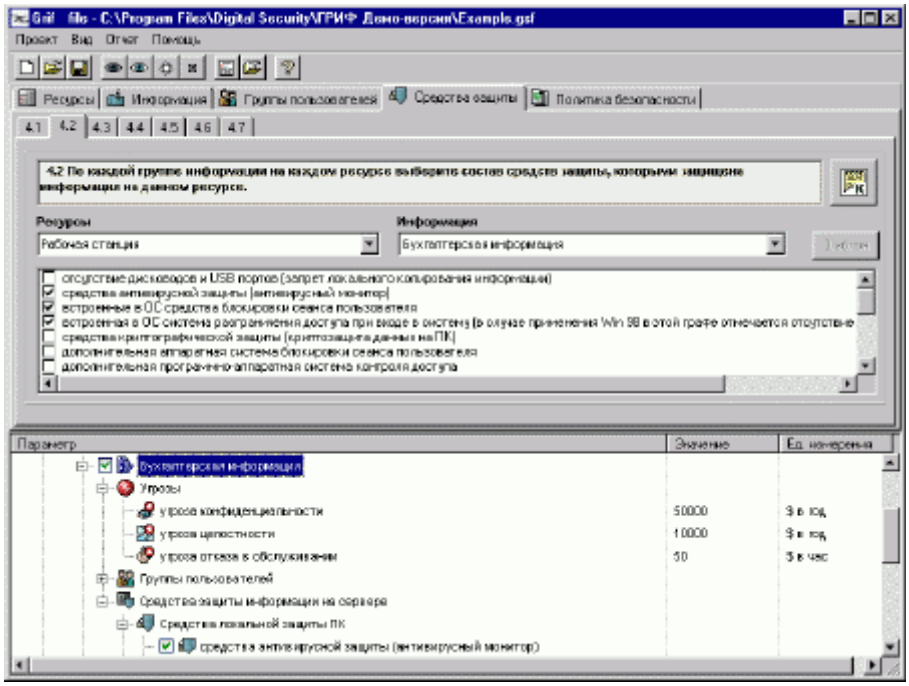



Рисунок.1.2. Интерфейс программного комплекса Гриф. Вкладка “Средства защиты”.

1.5. На завершающем этапе пользователь должен ответить на список вопросов по политике безопасности, реализованной в системе, что позволяет оценить реальный уровень защищенности системы и детализировать оценки рисков.

Наличие средств информационной защиты, отмеченных на первом этапе, само по себе еще не делает систему защищенной в случае их неадекватного использования и отсутствия комплексной политики безопасности, учитывающей все аспекты защиты информации, включая вопросы организации защиты, физической безопасности, безопасности персонала, непрерывности ведения бизнеса и так далее.

В результате выполнения всех действий по данным этапам на выходе сформирована полная модель информационной системы с точки зрения информационной безопасности с учетом реального выполнения требований комплексной политики безопасности, что позволяет перейти к программному анализу введенных данных для получения комплексной оценки рисков и формирования итогового отчета.

1.6. Отчет по системе представляет собой подробный, дающий полную картину возможного ущерба от инцидентов документ, готовый для представления руководству компании.

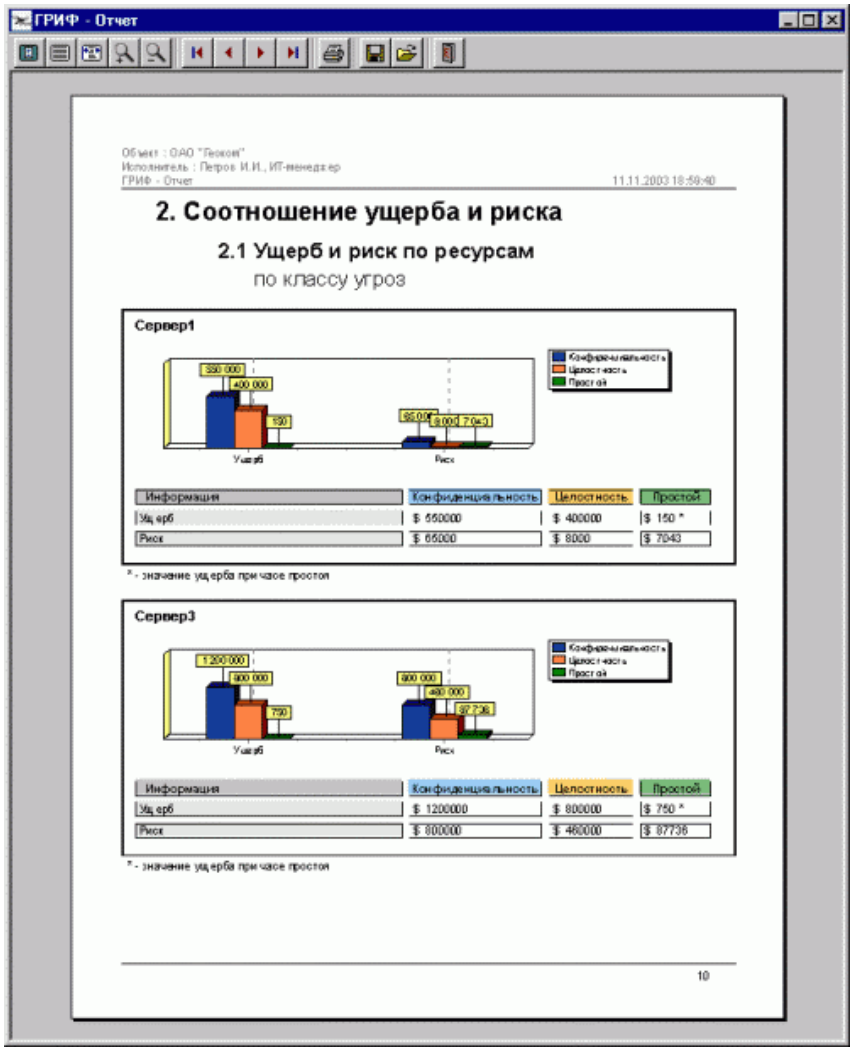



Рисунок.1.3. Интерфейс программного комплекса Гриф. Реализация отчета.

1.7. К недостаткам ГРИФ можно отнести следующее:

- отсутствует привязка к бизнес процессам (запланировано в следующей версии);
- нет возможности сравнения отчетов на разных этапах внедрения комплекса мер по обеспечению защищенности (запланировано в следующей версии);
- отсутствует возможность добавить специфичные для данной компании требования политики безопасности.

**1.2. Программный комплекс управления политикой информационной безопасности компании - КОНДОР+**

Российская компания Digital Security разработала программный продукт КОНДОР+, позволяющий специалистам (ИТ-менеджерам, офицерам безопасности) проверить политику информационной безопасности компании на соответствие требованиям международного стандарта безопасности ISO 17799.

Разработанный программный комплекс КОНДОР+ включает в себя более двухсот вопросов, ответив на которые, специалист получает подробный отчет о состоянии существующей политики безопасности, а так же модуль оценки уровня рисков соответствия требованиям ISO 17799 [3].

После регистрации пользователь получает возможность, выбрать соответствующий раздел стандарта ISO 17799 и ответить на вопросы.

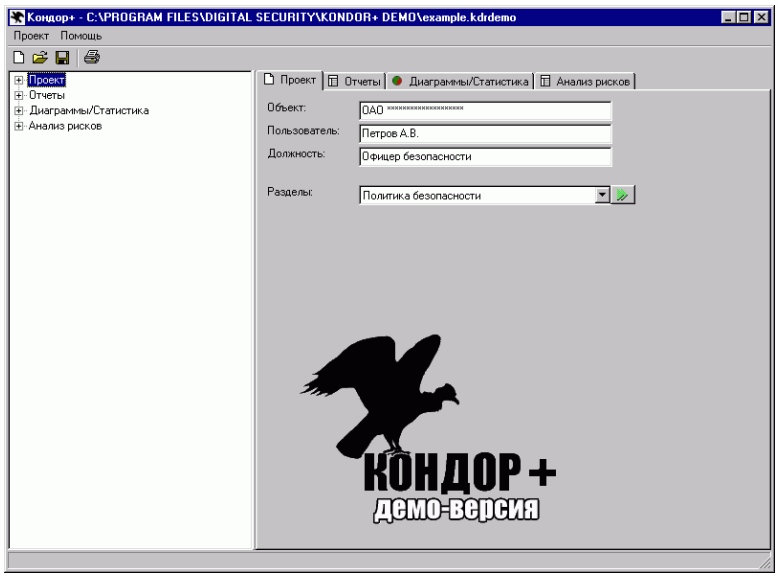



Рисунок.1.4. Интерфейс программного комплекса Кондор. Вкладка проект.

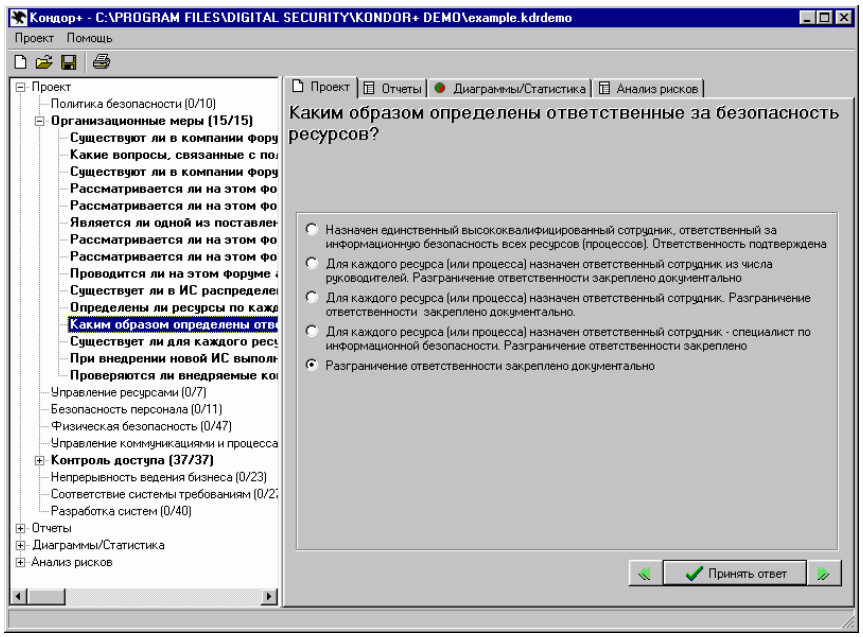



Рисунок.1.5. Интерфейс программного комплекса Кондор. Выбор раздела стандарта.

В отчете отражаются все положения политики безопасности, которые соответствуют стандарту и все, которые не соответствуют.

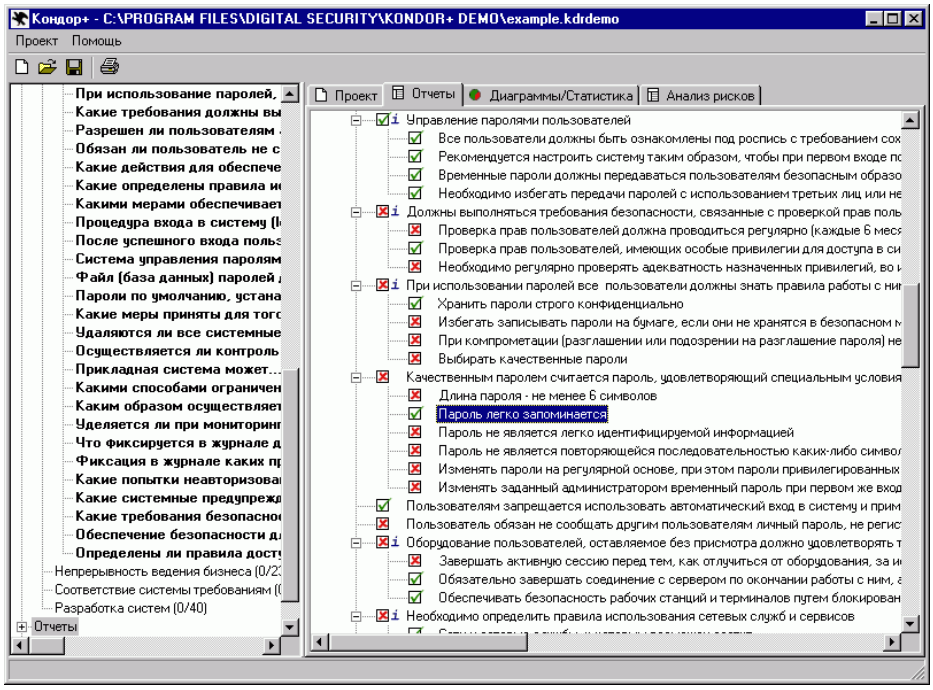



Рисунок.1.6. Интерфейс программного комплекса Кондор. Реализация отчета.

К наиболее важным элементам политики безопасности даются комментарии и рекомендации экспертов.

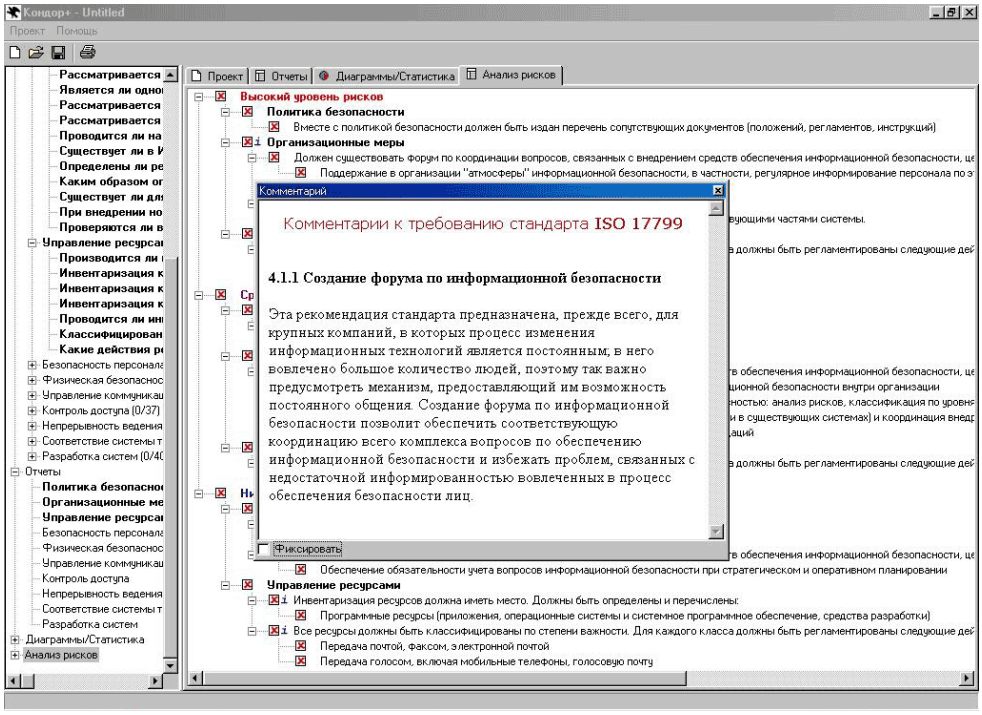



Рисунок.1.8. Интерфейс программного комплекса Кондор. Комментарии.

По желанию специалиста, работающего с программой, может быть выбрана генерация отчета, например, по какому-то одному или нескольким разделам стандарта ISO 17799, общий подробный отчет с комментариями, общий отчет о состоянии политики безопасности без комментариев для представления руководству и другие. Все варианты отчетов для большей наглядности сопровождаются диаграммами.

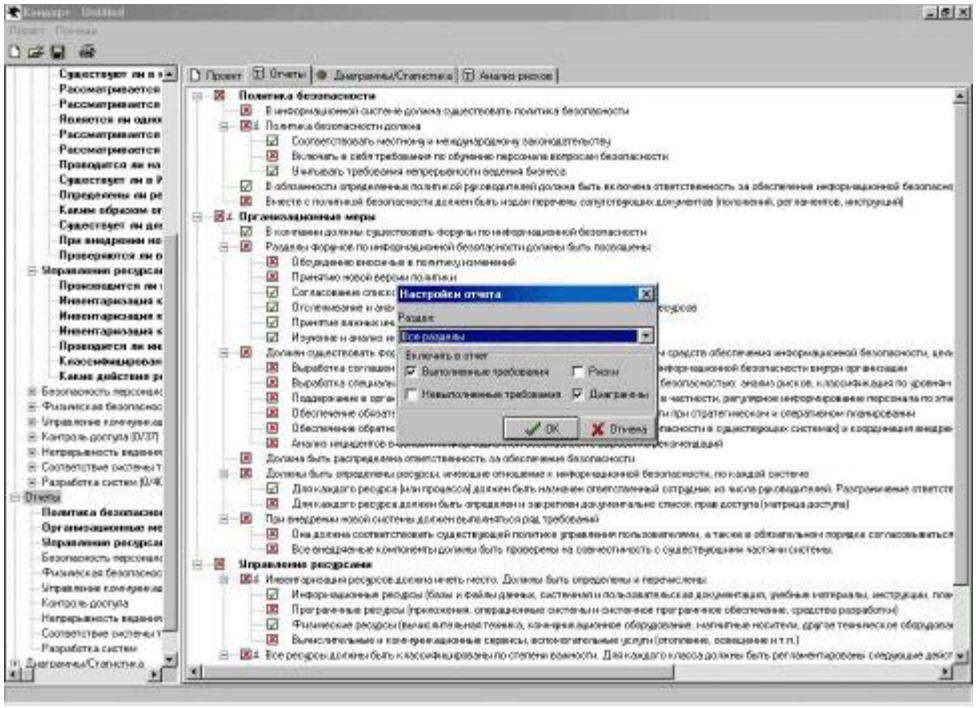



Рисунок.1.9. Интерфейс программного комплекса Кондор. Настройка отчета.

Кроме того, КОНДОР+ дает возможность специалисту отслеживать вносимые на основе выданных рекомендаций изменения в политику безопасности, постепенно приводя ее в полное соответствие с требованиями стандарта, а также иметь возможность представлять отчеты руководству, свидетельствующие о целесообразности и обоснованности инвестиций в обеспечение безопасности информационной системы компании.

Стоимость продукта составляет 225 долл. (КОНДОР) и 345 долл. (КОНДОР+ с модулем анализа рисков базового уровня).

К недостаткам КОНДОР+ можно отнести:

- отсутствие возможности установки пользователем веса на каждое требование (запланировано в следующих версиях)
- отсутствие возможности внесения пользователем комментариев (запланировано в следующих версиях)

**2. Описание системы (программного комплекса)**

При разработке системы преследовались многие цели, одна из них заключалась в том, чтобы создать программный продукт, который будет способен ввести пользователя в «курс дела» не утаивая от него ни одного этапа анализа рисков.

Необходимо было разработать максимально простое в использовании программное решение, основная задача которого - дать возможность ИТ-менеджеру самостоятельно (без привлечения сторонних экспертов) оценить уровень рисков в информационной системе, оценить эффективность существующей практики по обеспечению безопасности компании и

оптимизировать расходы и сформировать адекватный бюджет на информационную безопасность.

Система представляет интеграцию двух идей реализованных в системах Кондор и Гриф. В программном комплексе анализ рисков и политики безопасности информационной системы объединены в одном продукте. То есть данные, которые заносятся для анализа организационных мер, определяющих существующую политику безопасности компании, полностью используется при анализе рисков. Это означает что две составляющие управления информационной безопасностью - политика безопасности и анализ рисков - находятся в одном интегрированном решении. Кроме того, данный продукт может использоваться и в учебных целях как возможность изучить на практике методы и средства анализа рисков и проверки организационных мер обеспечивающих информационную безопасность. Благодаря значительно расширенной базе использованных положений стандарта ISO 17799 по сравнению с Кондором и Грифом в данной системе возможен более полный анализ организационных мер определяющих политику безопасности.

Известно, что существуют два подхода к анализу рисков - анализ рисков базового и полного уровня. В данной системе использованы сильные стороны разных методов, опирающихся на анализ рисков и на требования стандартов.

Но каким бы ни был подход, главная цель — формирование конкретных и применимых требований по безопасности к исследуемой информационной системе

В системе использован наиболее распространенный в настоящее время подход, основанный на учете различных факторов влияющих на уровни угроз и уязвимостей. Такой подход позволяет абстрагироваться от малосущественных технических деталей, учесть не только программно-технические, но и иные аспекты.

При работе система проводит анализ существующей политики безопасности на наличие так называемых дыр. Если их не устранять, то рано или поздно их обнаружат «плохие парни» и воспользуются для достижения своих, не всегда достойных целей.

В особенности отметим, что данная система позволяет также определить и экономическую эффективность системы информационной защиты.

Данный продукт окажет не заменимую помощь организациям, которые планируют получить сертификат на соответствие международному стандарту безопасности ISO 17799, так как при не выполнении каких либо требований, даются пояснения - как и что предпринять.

Ни для кого не секрет, что анализ информационных рисков является на сегодняшний день актуальной задачей для современного бизнеса - последние годы на каждой конференции по информационной безопасности в России можно услышать серьезные доклады на данную тему.

Анализ информационных рисков - это процесс комплексной оценки защищенности информационной системы с переходом к количественным или качественным показателям рисков. При этом риск - это вероятный ущерб, который зависит от защищенности системы. Под управлением рисками понимается процесс идентификации и уменьшения рисков, которые могут воздействовать на информационную систему. Результаты анализа используются при выборе средств защиты, оценке эффективности существующих и проектируемых систем защиты информации [3].

Итак, из определения следует, что на выходе алгоритма анализа риска можно получить либо количественную оценку рисков (риск измеряется в деньгах), либо - качественную (уровни риска; обычно: высокий, средний, низкий).

Кроме того, анализ рисков также отличается по используемому подходу; обычно условно выделяется анализ рисков базового и полного уровня. Для анализа рисков базового уровня достаточно проверить риск невыполнения требований общепринятого стандарта безопасности (обычно ISO 17799) с получением на выходе качественной оценки уровня рисков (высокий, средний, низкий).

Основное отличие полного анализа рисков от базового состоит в необходимости построения полной модели анализируемой информационной системы. Модель должна включать: виды ценной информации, объекты ее хранения; группы пользователей и виды доступа к информации; средства защиты (включая политику безопасности), виды угроз.

Далее после моделирования необходимо перейти к этапу анализа защищенности построенной полной модели информационной системы. И здесь мы попадаем в целый пласт теоретических и практических проблем, с которыми сталкиваются разработчики алгоритмов анализа риска полного уровня. Прежде всего, как алгоритмически (без эксперта) оценить защищенность информационной системы (заметим, что речь не идет о сканировании конкретных уязвимостей в конкретном применяемом программном обеспечении)? Следующая проблема - как алгоритмически определить все классы уязвимостей в системе защиты анализируемой системы? Как оценить ущерб от всех существующих в системе угроз безопасности и как добиться адекватной оценки совокупного ущерба по всем классам угроз (необходимо избежать избыточного суммирования ущербов)? И самая сложная проблема: риск категория вероятностная - как оценить вероятность реализации множества угроз информационной системы?

Весь вышеуказанный комплекс проблем необходимо решить при создании алгоритма.

Конечно, можно предложить пользователю самостоятельно ввести вероятность реализации угроз или оценить ее уровень, как в алгоритме RiskWatch. Но тогда мы сведем на нет весь процесс анализа.

При подсчете вероятности реализации тех или иных угроз можно опереться на некоторые статистические данные [5].

Таблица 2.1 Угрозы информационной безопасности

| Угрозы | Вероятность проявления |
|---|---|
| Небрежность | 0,188 |
| Пиратство | 0,166 |
| Нарушение целостности | 0,159 |
| Утечка данных | 0,159 |
| "Шутки" над коллегами | 0,150 |
| Наблюдение за излучением | 0,133 |
| Умышленные повреждения данных и программ | 0,129 |
| Нарушение аутентификации | 0,129 |
| Перегрузка | 0,119 |
| Неправильная маршрутизация | 0,106 |
| Аппаратные сбои | 0,090 |
| Искажение | 0,080 |
| Сетевые анализаторы | 0,074 |
| Мошенничество | 0,058 |
| Пожары и другие стихийные бедствия | 0,043 |
| Подлог | 0,033 |
| "Логические бомбы" | 0,032 |
| Кража | 0,032 |
| Блокирование информации | 0,016 |
| "Потайные ходы и лазейки" | 0,010 |

Но так как риск - это вероятный ущерб, который зависит от защищенности системы, то полученные данные будут не точными.

Из-за того что на оценку защищенности информационной системы существенным образом влияют организационные аспекты, то при анализе существующей защиты будем опираться на вопросник.

Так как на один и тот же вид информации может быть направлено сразу несколько угроз, то необходимо будет учесть так же и суммарный ущерб.

Необходимо смоделировать доступы всех групп пользователей ко всем видам информации и в зависимости от вида доступа и вида ресурса рассматривать конечное множество очевидных элементарных ситуаций, где начальную вероятность реализации угрозы можно определить достаточно просто и точно.

Далее анализируется множество опять же элементарных факторов (идет анализ комплексной защищенности объекта из вопросника) - которые так или иначе влияют на защищенность, а затем делается вывод об итоговых рисках.

**2. 1. Определение источника угроз.**

В любой методике управления рисками необходимо идентифицировать риски, как вариант – их составляющие (угрозы и уязвимости).

Целью создания любой КС является удовлетворение потребностей пользователей в своевременном получении достоверной информации и сохранении ее конфиденциальности (при необходимости). Информация является конечным «продуктом потребления» в КС и выступает в виде центральной компоненты системы. Безопасность информации на уровне КС обеспечивают такие компоненты системы как технические, программные средства, обслуживающий персонал и пользователи. Причем эта задача должна решаться путем защиты от внешних и внутренних неразрешенных (несанкционированных) воздействий. Особенности взаимодействия компонент заключаются в следующем. Внешние воздействия чаше всего оказывают несанкционированное влияние на информацию путем воздействия на другие компоненты системы. Следующей особенностью является возможность несанкционированных действий, вызываемых внутренними причинами, в отношении информации со стороны технических, программных средств, обслуживающего, персонала и пользователей. В этом заключается основное противоречие взаимодействия этих компонент с информацией. Причем, обслуживающий персонал и пользователи могут сознательно осуществлять попытки несанкционированного воздействия на информацию. Таким образом, обеспечение безопасности информации в КС должно предусматривать защиту всех компонент от внешних и внутренних воздействий (угроз) [4].

Под **угрозой безопасности информации** понимается потенциально возможное событие, процесс или явление, которые могут привести к уничтожению, утрате целостности, конфиденциальности или доступности информации.

Все множество потенциальных угроз безопасности информации в КС может быть разделено на два класса (рис 2.1).


Рисунок. 2.1. Угрозы безопасности информации в компьютерных системах

**Случайные угрозы**

Угрозы, которые не связаны с преднамеренными действиями злоумышленников и реализуются в случайные моменты времени, называют *случайными* или *непреднамеренными***.**

Реализация угроз этого класса приводит к наибольшим потерям информации (по статистическим данным - до 80% от ущерба, наносимого информационным ресурсам КС любыми угрозами). При этом могут происходить уничтожение, нарушение целостности и доступности информации. Реже нарушается конфиденциальность информации, однако при этом создаются предпосылки для злоумышленного воздействия на информацию.

*Стихийные бедствия и аварии* чреваты наиболее разрушительными последствиями для КС, т.к. последние подвергаются физическому разрушению, информация утрачивается или доступ к ней становится невозможен.

*Сбои и отказы* сложных систем неизбежны. В результате сбоев и отказов нарушается работоспособность технических средств, уничтожаются и искажаются данные и программы, нарушается алгоритм работы устройств. Нарушения алгоритмов работы от дельных узлов и устройств могут также привести к нарушению конфиденциальности информации. Например, сбои и отказы средств выдачи информации могут привести к несанкционированному доступу к информации путем несанкционированной ее выдачи в канал связи, на печатающее устройство и т. п.

*Ошибки при разработке КС, алгоритмические и программные* ошибки приводят к последствиям, аналогичным последствиям сбоев и отказов технических средств. Кроме того,

такие ошибки могут быть использованы злоумышленниками для воздействия на ресурсы КС. Особую опасность представляют ошибки в операционных системах (ОС) и в программных средствах защиты информации.

Согласно данным Национального Института Стандартов и Технологий США (NIST) 65% случаев нарушения безопасности информации происходит в результате *ошибок пользователей и обслуживающего персонала.* Некомпетентное, небрежное или невнимательное выполнение функциональных обязанностей сотрудниками приводят к уничтожению, нарушению целостности и конфиденциальности информации, а также компрометации механизмов защиты.

Характеризуя угрозы информации в КС, не связанные с преднамеренными действиями, в целом, следует отметить, что механизм их реализации изучен достаточно хорошо, накоплен значительный опыт противодействия этим угрозам. Современная технология разработки технических и программных средств, эффективная система эксплуатации КС, включающая обязательное резервирование информации, позволяют значительно снизить потери от реализации угроз этого класса.

**Преднамеренные угрозы**

Второй класс угроз безопасности информации в КС составляют преднамеренно создаваемые угрозы.

Данный класс угроз изучен недостаточно, очень динамичен и постоянно пополняется новыми угрозами. Угрозы этого класса в соответствии с их физической сущностью и механизмами реализации могут быть распределены по пяти группам:

- традиционный или универсальный шпионаж и диверсии;
- несанкционированный доступ к информации;
- электромагнитные излучения и наводки;
- модификация структур КС;
- вредительские программы.

**Традиционный шпионаж и диверсии**

В качестве источников нежелательного воздействия на информационные ресурсы по-прежнему актуальны методы и средства шпионажа и диверсий**,** которые использовались и используются для добывания или уничтожения информации на объектах, не имеющих КС. Эти методы также действенны и эффективны в условиях применения компьютерных систем. Чаще всего они используются для получения сведений о системе защиты с целью проникновения в КС, а также для хищения и уничтожения информационных ресурсов.

К методам шпионажа и диверсий относятся:

- подслушивание;
- визуальное наблюдение;
- хищение документов и машинных носителей информации;
- хищение программ и атрибутов системы защиты;
- подкуп и шантаж сотрудников;
- сбор и анализ отходов машинных носителей информации;
- поджоги;
- взрывы.

Для *подслушивания* злоумышленнику не обязательно проникать на объект. Современные средства позволяют подслушивать разговоры с расстояния нескольких сотен метров. Так прошла испытания система подслушивания, позволяющая с расстояния 1 км фиксировать разговор в помещении с закрытыми окнами. В городских условиях дальность действия устройства сокращается до сотен и десятков метров в зависимости от уровня фонового шума. Принцип действия таких устройств основан на анализе отраженного луча лазера от стекла окна помещения, которое колеблется от звуковых волн. Колебания оконных стекол от акустических волн в помещении могут сниматься и передаваться на расстояния с помощью специальных устройств, укрепленных на оконном стекле. Такие устройства преобразуют механические колебания стекол в электрический сигнал с последующей передачей его по радиоканалу. Вне помещений подслушивание ведется с помощью сверхчувствительных направленных микрофонов. Реальное расстояние подслушивания с помощью направленных микрофонов составляет 50-100 метров.

Разговоры в соседних помещениях, за стенами зданий могут контролироваться с помощью стетоскопных микрофонов. Стетоскопы преобразуют акустические колебания в электрические. Такие микрофоны позволяют прослушивать разговоры при толщине стен до 50-100 см. Съем информации может осуществляться также и со стекол, металлоконструкций зданий, труб водоснабжения и отопления.

Аудиоинформация может быть получена также путем высокочастотного навязывания. Суть этого метода заключается в воздействии высокочастотным электромагнитным полем или электрическими сигналами на элементы, способные модулировать эти поля, или сигналы электрическими или акустическими сигналами с речевой информацией. В качестве таких элементов могут использоваться различные полости с электропроводной поверхностью, представляющей собой высокочастотный контур с распределенными параметрами, которые меняются под действием акустических волн. При совпадении частоты такого контура с частотой высокочастотного навязывания и при наличии воздействия акустических волн на поверхность полости контур переизлучает и модулирует внешнее поле (высокочастотный электрический сигнал). Чаще всего этот метод прослушивания реализуется с помощью

телефонной линии. При этом в качестве модулирующего элемента используется телефонный аппарат, на который по телефонным проводам подается высокочастотный электрический сигнал. Нелинейные элементы телефонного аппарата под воздействием речевого сигнала модулируют высокочастотный сигнал. Модулированный высокочастотный сигнал может быть демодулирован в приемнике злоумышленника.

Одним из возможных каналов утечки звуковой информации может быть прослушивание переговоров, ведущихся с помощью средств связи. Контролироваться могут как проводные каналы связи, так и радиоканалы. Прослушивание переговоров по проводным и радиоканалам не требует дорогостоящего оборудования и высокой квалификации злоумышленника.

*Дистанционная видеоразведка* для получения информации в КС малопригодна и носит, как правило, вспомогательный характер.

Видеоразведка организуется в основном для выявления режимов работы и расположения механизмов защиты информации. Из КС информация реально может быть получена при использовании на объекте экранов, табло, плакатов, если имеются прозрачные окна и перечисленные выше средства размещены без учета необходимости противодействовать такой угрозе.

Видеоразведка может вестись с использованием технических средств, таких как оптические приборы, фото-, кино- и телеаппаратура. Многие из этих средств допускают консервацию (запоминание) видеоинформации, а также передачу ее на определенные расстояния.

В прессе появились сообщения о создании в США мобильного микроробота для ведения дистанционной разведки. Пьезокерамический робот размером около 7 см и массой 60 г способен самостоятельно передвигаться со скоростью 30 см/с в течение 45 мин. За это время «микроразведчик» способен преодолеть расстояние в 810 метров, осуществляя транспортировку 28 г полезного груза (для сравнения - коммерческая микровидеокамера весит 15 г).

Для вербовки сотрудников и физического уничтожения объектов КС также не обязательно иметь непосредственный доступ на объект. Злоумышленник, имеющий доступ на объект КС, может использовать любой из методов традиционного шпионажа.

Злоумышленниками, имеющими доступ на объект, могут использоваться миниатюрные средства фотографирования, видео - и аудиозаписи. Для аудио- и видеоконтроля помещений и при отсутствии в них злоумышленника могут использоваться закладные устройства или «жучки». Для объектов КС наиболее вероятными являются закладные устройства, обеспечивающие прослушивание помещений. Закладные устройства делятся на проводные и излучающие. Проводные закладные устройства требуют значительного времени на

установку и имеют существенный демаскирующий признак - провода. Излучающие «закладки» («радиозакладки») быстро устанавливаются, но также имеют демаскирующий при знак - излучение в радио или оптическом диапазоне. «Радиозакладки» могут использовать в качестве источника электрические сигналы или акустические сигналы. Примером использования электрических сигналов в качестве источника является применение сигналов внутренней телефонной, громкоговорящей связи. Наибольшее распространение получили акустические «радиозакладки». Они воспринимают акустический сигнал, преобразуют его в электрический и передают в виде радиосигнала на дальность до 8 км. Из применяемых на практике «радиозакладок» подавляющее большинство (около 90%) рассчитаны на работу в диапазоне расстояний 50 - 800 метров.

Для некоторых объектов КС существует *угроза вооруженного нападения террористических или диверсионных групп.* При этом могут быть применены средства огневого поражения.

**Несанкционированный доступ к информации**

Термин «несанкционированный доступ к информации» (НСДИ) определен как доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств вычислительной техники или автоматизированных систем.

Под правилами разграничения доступа понимается совокупность положений, регламентирующих права доступа лиц или процессов (субъектов доступа) к единицам информации (объектам доступа).

Право доступа к ресурсам КС определяется руководством для каждого сотрудника в соответствии с его функциональными обязанностями. Процессы инициируются в КС в интересах определенных лиц, поэтому и на них накладываются ограничения по доступу к ресурсам.

Выполнение установленных правил разграничения доступа в КС реализуется за счет создания системы разграничения доступа (СРД).

Несанкционированный доступ к информации возможен только с использованием штатных аппаратных и программных средств в следующих случаях:

- отсутствует система разграничения доступа;
- сбой или отказ в КС;
- ошибочные действия пользователей или обслуживающего персонала компьютерных систем;
- ошибки в СРД;
- фальсификация полномочий.

Если СРД отсутствует, то злоумышленник, имеющий навыки работы в КС, может получить без ограничений доступ к любой информации. В результате сбоев или отказов средств КС, а также ошибочных действий обслуживающего персонала и пользователей возможны состояния системы, при которых упрощается НСДИ. Злоумышленник может выявить ошибки в СРД и использовать их для НСДИ. Фальсификация полномочий является одним из наиболее вероятных путей (каналов) НСДИ.

**Электромагнитные излучения и наводки**

Процесс обработки и передачи информации техническими средствами КС сопровождается электромагнитными излучениями в окружающее пространство и наведением электрических сигналов в линиях связи, сигнализации, заземлении и других проводниках. Они получили названия *побочных электромагнитных излучений и наводок (ПЭМИН)***.** С помощью специального оборудования сигналы принимаются, выделяются, усиливаются и могут либо просматриваться, либо записываться в запоминающих устройствах. Наибольший уровень электромагнитного излучения в КС присущ работающим устройствам отображения информации на электронно-лучевых трубках. Содержание экрана такого устройства может просматриваться с помощью обычного телевизионного приемника, дополненного несложной схемой, основной функцией которой является синхронизация сигналов. Дальность удовлетворительного приема таких сигналов при использовании дипольной антенны составляет 50 метров. Использование направленной антенны приемника позволяет увеличить зону уверенного приема сигналов до 1 км. Восстановление данных возможно также путем анализа сигналов излучения неэкранированного электрического кабеля на расстоянии до 300 метров.

Наведенные в проводниках электрические сигналы могут выделяться и фиксироваться с помощью оборудования, подключаемого к этим проводникам на расстоянии в сотни метров от источника сигналов. Для добывания информации злоумышленник может использовать также «просачивание» информационных сигналов в цепи электропитания технических средств КС.

«Просачивание» информационных сигналов в цепи электропитания возможно при наличии магнитной связи между выходным трансформатором усилителя и трансформатором выпрямительного устройства. «Просачивание» также возможно за счет падения напряжения на внутреннем сопротивлении источника питания при прохождении токов усиливаемых информационных сигналов. Если затухание в фильтре выпрямительного устройства недостаточно, то информационные сигналы могут быть обнаружены в цепи питания. Информационный сигнал может быть выделен в цепи питания за счет зависимости значений

потребляемого тока в оконечных каскадах усилителей (информационные сигналы) и значений токов в выпрямителях, а значит и в выходных цепях.

Электромагнитные излучения используются злоумышленниками не только для получения информации, но и для ее уничтожения. Электромагнитные импульсы способны уничтожить информацию на магнитных носителях. Мощные электромагнитные и сверхвысокочастотные излучения могут вывести из строя электронные блоки КС. Причем для уничтожения информации на магнитных носителях с расстояния нескольких десятков метров может быть использовано устройство, помещающееся в портфель.

**Несанкционированная модификация структур**

Большую угрозу безопасности информации в КС представляет *несанкционированная модификация алгоритмической, программной и технической структур системы***.** Несанкционированная модификация структур может осуществляться на любом жизненном цикле КС. Несанкционированное изменение структуры КС на этапах разработки и модернизации получило название «закладка». В процессе разработки КС «закладки» внедряются, как правило, в специализированные системы, предназначенные для эксплуатации в какой-либо фирме или государственных учреждениях. В универсальные КС «закладки» внедряются реже, в основном для дискредитации таких систем конкурентом или на государственном уровне, если предполагаются поставки КС во враждебное государство. «Закладки», внедренные на этапе разработки, сложно выявить ввиду высокой квалификации их авторов и сложности современных КС.

Алгоритмические, программные и аппаратные «закладки» используются либо для непосредственного вредительского воздействия на КС, либо для обеспечения неконтролируемого входа в систему. Вредительские воздействия «закладок» на КС осуществляются при получении соответствующей команды извне (в основном характерно для аппаратных «закладок») и при наступлении определенных событий в системе. Такими событиями могут быть: переход на определенный режим работы (например, боевой режим системы управления оружием или режим устранения аварийной ситуации на атомной электростанции т. п.), наступление установленной даты, достижение определенной наработки и т. д.

Программные и аппаратные «закладки» для осуществления неконтролируемого входа в программы, использование привилегированных режимов работы (например, режимов операционной системы), обхода средств защиты информации получили название «люки».

**Вредительские программы**

Одним из основных источников угроз безопасности информации в КС является использование специальных программ, получивших общее название «вредительские программы».

В зависимости от механизма действия вредительские программы делятся на четыре класса:

- «логические бомбы»;
- «черви»;
- «троянские кони»;
- «компьютерные вирусы».

*«Логические бомбы»* - это программы или их части, постоянно находящиеся в ЭВМ или вычислительных системах (ВС) и выполняемые только при соблюдении определенных условий. Примерами таких условий могут быть: наступление заданной даты, переход КС в определенный режим работы, наступление некоторых событий установленное число раз и т.п.

*«Червями»* называются программы, которые выполняются каждый раз при загрузке системы, обладают способностью перемещаться в ВС или сети и самовоспроизводить копии. Лавинообразное размножение программ приводит к перегрузке каналов связи, памяти и, в конечном итоге, к блокировке системы.

*«Троянские кони»* - это программы, полученные путем явного изменения или добавления команд в пользовательские программы. При последующем выполнении пользовательских программ наряду с заданными функциями выполняются несанкционированные, измененные или какие-то новые функции.

*«Компьютерные вирусы»* - это небольшие программы, которые после внедрения в ЭВМ самостоятельно распространяются путем создания своих копий, а при выполнении определенных условий оказывают негативное воздействие на КС.

Поскольку вирусам присущи свойства всех классов вредительских программ, то в последнее время любые вредительские программы часто называют вирусами.

**Классификация злоумышленников**

Возможности осуществления вредительских воздействий в большой степени зависят от статуса злоумышленника по отношению к КС. Злоумышленником может быть:

- разработчик КС;
- сотрудник из числа обслуживающего персонала;

- пользователь;
- постороннее лицо.

*Разработчик* владеет наиболее полной информацией о программных и аппаратных средствах КС и имеет возможность внедрения "закладок" на этапах создания и модернизации систем. Но он, как правило, не получает непосредственного доступа на эксплуатируемые объекты КС. Пользователь имеет общее представление о структурах КС, о работе механизмов защиты информации. Он может осуществлять сбор данных о системе защиты информации методами традиционного шпионажа, а также предпринимать попытки несанкционированного доступа к информации. Возможности внедрения закладок пользователями очень ограничены. Постороннее лицо, не имеющее отношения к КС, находится в наименее выгодном положении по отношению к другим злоумышленникам. Если предположить, что он не имеет доступ на объект КС, то в его распоряжении имеются дистанционные методы традиционного шпионажа и возможность диверсионной деятельности. Он может осуществлять вредительские воздействия с использованием электромагнитных излучений и наводок, а также каналов связи, если КС является распределенной.

Большие возможности оказания вредительских воздействий на информацию КС имеют специалисты, обслуживающие эти системы. Причем, специалисты разных подразделений обладают различными потенциальными возможностями злоумышленных действий. Наибольший вред могут нанести работники службы безопасности информации. Далее идут системные программисты, прикладные программисты и инженерно-технический персонал.

На практике опасность злоумышленника зависит также от финансовых, материально-технических возможностей и квалификации злоумышленника.

## 2.2.Примеры методик анализа рисков

Концепции анализа рисков, управления рисками на всех стадиях жизненного цикла информационной технологии были предложены многими крупными организациями, занимающимися проблемами информационной безопасности. Отечественные аналитики начали использовать различные методики на практике. Несколькими российскими организациями были разработаны собственные методики анализа и управления рисками, разработано собственное программное обеспечение, которое, наряду с зарубежным, имеется на отечественном рынке [3].

### Оценка рисков

Для измерения какого-либо свойства необходимо выбрать шкалу. Шкалы могут быть разной «силы», выбор той или иной шкалы зависит как от свойств измеряемой величины, так и от имеющихся в наличии измерительных инструментов.

В качестве примера рассмотрим варианты выбора шкалы для измерения характеристического свойства «ценность информационного ресурса». Она может измеряться опосредованно в шкалах отношений, таких как стоимость восстановления ресурса, время восстановления ресурса и других. Другой вариант — определить ранговую шкалу для получения экспертной оценки, имеющую, например, три возможных значения лингвистической переменной:

1) Малоценный информационный ресурс - от него не зависят критически важные задачи, и он может быть восстановлен с небольшими затратами времени и денег;

2) Ресурс средней ценности - от него зависит ряд важных задач, но в случае его утраты он может быть восстановлен за время менее, чем критически допустимое, стоимость восстановления высокая;

3) Ценный ресурс: от него зависят критически важные задачи, в случае утраты время восстановления превышает критически допустимое, либо стоимость чрезвычайно высока.

Для измерения рисков не существует абсолютной шкалы. Риски можно оценивать по объективным либо субъективным критериям. Примером объективного критерия является вероятность выхода из строя какого-либо оборудования, например ПК за определенный промежуток времени. Примером субъективного критерия является оценка администратора информационного ресурса риска выхода из строя ПК. Для этого обычно разрабатывается ранговая шкала с несколькими градациями, например: низкий, средний, высокий уровни.

Существует ряд подходов к измерению рисков. Рассмотрим наиболее распространенные: оценка по двум факторам и оценка по трем факторам.

**Оценка рисков по двум факторам.**

В простейшем случае используется оценка двух факторов: вероятность происшествия и тяжесть возможных последствий. Обычно считается, что риск тем больше, чем больше вероятность происшествия и тяжесть последствий. Общая идея может быть выражена формулой:

РИСК=Рпроисшествия X ЦЕНА ПОТЕРИ (2.1.)

Если переменные являются количественными величинами, риск — это оценка математического ожидания потерь.

Если переменные являются качественными величинами - то операция умножения не определена. Таким образом, в явном виде эта формула использоваться не должна.

Рассмотрим вариант использования качественных величин (наиболее часто встречающаяся ситуация).

Сначала должны быть определены значения лингвистической переменной вероятности событий, например такой шкалы:

- A - событие практически никогда не происходит;
- B - событие случается редко;
- C - вероятность события за рассматриваемый промежуток времени — около 0,5;
- B - скорее всего, событие произойдет;
- E - событие почти обязательно произойдет.

Кроме того, определяется лингвистическая переменная; серьезности происшествий, например:

N (Negligible) — воздействием можно пренебречь.

Mi (Minor) — незначительное происшествие - последствия легко устранимы, затраты на ликвидацию последствий невелики, воздействие на информационную технологию незначительно;

Mo (Moderate) — происшествие с умеренными результатами - ликвидация последствий не связана с крупными затратами, воздействие на информационную технологию невелико и не затрагивает критически важные задачи;

S (Serious) — происшествие с серьезными последствиями: ликвидация последствий связана со значительными затратами, воздействие на информационные технологии ощутимо, воздействует на выполнение критически важных задач;

C (Critical) — происшествие приводит к невозможности решения критически важных задач.

Для оценки рисков определяется переменная из трех значений: низкий риск, средний риск, высокий риск.

Риск, связанный с определенным событием, зависит от двух факторов и может быть определен как показано в таблице 2.2.

Шкалы факторов риска и сама таблица могут быть определены иначе, иметь другое число градаций.

Таблица.2.2. Определение риска в зависимости от двух факторов

| | Negli | Minor | Moder | Seriou | Critica |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | gible | | ate | s | l |
| | Низкий риск | Низкий риск | Низкий риск | Средний риск | Средний риск |
| | Низкий риск | Низкий риск | Средний риск | Средний риск | Высокий риск |
| | Низкий риск | Средний риск | Средний риск | Средний риск | Высокий риск |
| | Средний риск | Средний риск | Средний риск | Средний риск | Высокий риск |
| | Средний риск | Высокий риск | Высокий риск | Высокий риск | Высокий риск |

Подобный подход к оценке рисков достаточно распространен. При разработке (использовании) методик оценки рисков необходимо учитывать следующие особенности:

- значения шкал должны быть четко определены (словесное описание) и пониматься одинаково всеми участниками процедуры экспертной оценки;
- требуются обоснования выбранной таблицы. Необходимо убедиться, что разные инциденты, характеризующиеся одинаковыми сочетаниями факторов риска, имеют с точки зрения экспертов одинаковый уровень рисков.

Подобные методики широко применяются при проведении анализа рисков базового уровня.

**Оценка рисков по трем факторам.**

В большинстве методик, рассчитанных на более высокие требования, чем базовый уровень, используется модель оценки риска с тремя факторами: угроза, уязвимость, цена потери. Угроза и уязвимость определяются следующим образом.

*Угроза* — совокупность условий и факторов, которые могут стать причиной нарушения целостности, доступности, конфиденциальности информации.

*Уязвимость* — слабость в системе защиты, которая делает возможным реализацию угрозы.

*Цена потери* — это качественная или количественная оценка степени серьезности происшествия.

Вероятность происшествия, которая в данном подходе может быть объективной либо субъективной величиной, зависит от уровней (вероятностей) угроз и уязвимостей:

Рпроисшествия = Ругрозы Х Руязвимости (2.2.)

Соответственно, риск определяется следующим образом:

РИСК = Ругрозы Х Руязвимости Х ЦЕНА ПОТЕРИ (2.3.)

Данное выражение можно рассматривать как математическую формулу, если используются количественные шкалы, либо как формулировку общей идеи, если хотя бы одна из шкал - качественная. В последнем случае используются различного рода табличные методы для определения риска в зависимости от трех факторов.

Например, показатель риска измеряется в шкале от 0 до 8 со следующими определениями уровней риска:

1) Риск практически отсутствует. Теоретически возможны ситуации, при которых событие наступает, но на практике это случается редко, а потенциальный ущерб сравнительно невелик:

2) Риск очень мал. События подобного рода случались достаточно редко, кроме того, негативные последствия сравнительно невелики;

. . .

8) Риск очень велик. Событие, скорее всего, наступит, и последствия будут чрезвычайно тяжелыми.

Матрица может быть определена следующим образом (табл.2.3). В данной таблице уровни уязвимости Н, С, В означают соответственно низкий, средний и высокий уровни.

Подобные таблицы используются как в «бумажных» вариантах методик оценки рисков, так и в различного рода инструментальных средствах анализа рисков.

Таблица.2.3. Определение риска в зависимости от трех факторов

| Степень серьезности происшествия (цена потери) | Уровень угрозы | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | Низкий | | | Средний | | | Высокий | | |
| | Уровни уязвимостей | | | Уровни уязвимостей | | | Уровни уязвимостей | | |
| | Н | С | В | Н | С | В | Н | С | В |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Незначительна | 0 | 1 | 2 | 1 | 2 | 3 | 2 | 3 | 4 |
| я Несущественная | 1 | 2 | 3 | 2 | 3 | 4 | 3 | 4 | 5 |
| Умеренная | 2 | 3 | 4 | 3 | 4 | 5 | 4 | 5 | 6 |
| Серьезная | 3 | 4 | 5 | 4 | 5 | 6 | 5 | 6 | 7 |
| Критическая | 4 | 5 | 6 | 5 | 6 | 7 | 6 | 7 | 8 |

Практические сложности в реализации этого подхода следующие.

Во-первых, должен быть собран весьма обширный материал о происшествиях в этой области.

Во-вторых, применение этого подхода оправдано далеко не всегда. Если информационная система достаточно крупная (содержит много элементов, расположена на обширной территории), имеет давнюю историю, то подобный подход, скорее всего, применим. Если система сравнительно невелика, использует новейшие элементы технологии (для которых пока нет достоверной статистики), оценки угроз и уязвимостей могут оказаться недостоверными.

### 2.3. Выбор методика анализа рисков

Как уже упоминалась выше для оценки угроз и уязвимостей используются различные методы, в основе которых могут лежать [6]:

- Экспертные оценки.
- Статистические данные.
- Учет факторов, влияющих на уровни угроз и уязвимостей.

Мы же, выбрали наиболее распространенный в настоящее время подход, основанный на учете различных факторов, влияющих на уровни угроз и уязвимостей. Такой подход позволяет абстрагироваться от малосущественных технических деталей, учесть не только программно-технические, но и иные аспекты.

Нам необходимо оценит следующие вероятности:

вероятность уровня(степени) угрозы и вероятность уровня уязвимости .

Для оценки угроз выберем следующие косвенные факторы:

- Статистика по зарегистрированным инцидентам.
- Тенденции в статистке по подобным нарушениям.
- Наличие в системе информации, представляющей интерес для потенциальных внутренних или внешних нарушителей.
- Моральные качества персонала.
- Возможность извлечь выгоду из изменения обрабатываемой в системе информации.

- Наличие альтернативных способов доступа к информации.

Для оценки уязвимостей выберем следующие косвенные факторы:

- Количество рабочих мест (пользователей) в системе.
- Размер рабочих групп.
- Осведомленность руководства о действиях сотрудников (разные аспекты).
- Характер используемого на рабочих местах оборудования и ПО.
- Полномочия пользователей.

Далее мы берем подготовленный список вопросов, составленный при изучении разделов стандарта ISO 17799, и делим его на две части, влияющих на уровень угроз и влияющих на уровень уязвимости. Напротив фиксированных вариантов ответов поставим определенное количество баллов, определяющих уровень критичности.

Для определения факторов влияющих на уровень угроз, приведем следующий вопрос с вариантами ответов:

*Может ли сокрытие информации принести прямую финансовую или иную выгоду сотрудникам?*

Варианты ответов:

а) Да 15

б) Нет 0

Для определения факторов влияющих на уровень уязвимости, приведем следующий вопрос с вариантами ответов:

*Есть ли у сотрудников возможность осуществить несанкционированный доступ к информации (например, когда их непосредственно не контролируют, по вечерам и т.п.)?*

а) Да 20

б) Нет 0

Итоговая оценка угрозы и уязвимости данного класса будет определяться суммированием баллов. Программный код сам оценит степень угрозы и уязвимости по количеству накопленных балов.

Таблица 2.4.Степень угрозы при количестве баллов.

| | |
|---|---|
| До 60 | Очень низкая |
| От 60 до 150 | Низкая |
| От 150 до 250 | Средняя |
| От 250 до 400 | Высокая |

| | |
|---|---|
| 400 и более | Очень высокая |

Таблица 2.5. Степень уязвимости при количестве баллов.

| | |
|---|---|
| До 100 | Низкая |
| От 100 до 300 | Средняя |
| 300 и более | Высокая |

Эта методика проста и дает владельцу информационных ресурсов ясное представление, каким образом получается итоговая оценка и что надо изменить, чтобы улучшить показатели.

Далее используя метод оценка рисков по трем факторам произведем расчет по формуле 2.3.

В результате проделанной работы по оценки рисков мы получим качественные показатели. А при использовании оценки ущерба в случае реализации угроз конфиденциальности, целостности и доступности– мы сможем получить и некоторые количественные результаты.

### 2.4. Методика проверки организационных мер на соответствие положениям международного стандарта безопасности ISO 17799.

Политика информационной безопасности компании является важнейшим нормативным документом, определяющим комплекс мер и требований по обеспечению информационной безопасности бизнеса. Политика безопасности должна описывать реальное положение дел в информационной системе компании и являться обязательным руководством к действию для всего персонала компании. На сегодняшний день общепризнанным стандартом при создании комплексной политики безопасности компании является международный стандарт управления информационной безопасностью ISO 17799, созданный в 2000 году Международной организацией по стандартизации и Международной электротехнической комиссией на основе разработок Британского института стандартов [7].

Ниже приведены основные разделы стандарта ISO 17799:

1. *Политика безопасности*
2. *Организационные меры по обеспечению безопасности*

- Управление форумами по информационной безопасности
- Координация вопросов, связанных с информационной безопасностью
- Распределение ответственности за обеспечение безопасности

3. *Классификация и управление ресурсами*

- Инвентаризация ресурсов
- Классификация ресурсов

4. *Безопасность персонала*

- Безопасность при выборе и работе с персоналом
- Тренинги персонала по вопросам безопасности
- Реагирование на секьюрити инциденты и неисправности

5. *Физическая безопасность*

6. *Управление коммуникациями и процессами*

- Рабочие процедуры и ответственность
- Системное планирование
- Защита от злонамеренного программного обеспечения (вирусов, троянских коней)
- Управление внутренними ресурсами
- Управление сетями
- Безопасность носителей данных
- Передача информации и программного обеспечения

7. *Контроль доступа*

- Бизнес требования для контроля доступа
- Управление доступом пользователя
- Ответственность пользователей
- Контроль и управление удаленного (сетевого) доступа
- Контроль доступа в операционную систему
- Контроль и управление доступом к приложениям
- Мониторинг доступа и использования систем

8. *Разработка и техническая поддержка вычислительных систем*

- Требования по безопасности систем
- Безопасность приложений
- Криптография
- Безопасность системных файлов
- Безопасность процессов разработки и поддержки

9. *Управление непрерывностью бизнеса*

- Процесс управления непрерывного ведения бизнеса
- Непрерывность бизнеса и анализ воздействий
- Создание и внедрение плана непрерывного ведения бизнеса
- Тестирование, обеспечение и переоценка плана непрерывного ведения бизнеса

*10. Соответствие системы основным требованиям*

- Соответствие требованиям законодательства
- Анализ соответствия политики безопасности
- Анализ соответствия техническим требованиям
- Анализ соответствия требованиям системного аудита

После изучения русской редакции ISO 17799 был разработан вопросник, ответив на вопросы которого получаем подробный отчет о состоянии дел в существующей политики безопасности организации.

Алгоритм работы данного раздела поясним на следующем примере.

При выборе раздела стандарта “Политика безопасности. Организационные меры” пользователю предлагается ответить на следующий вопрос с вариантами ответов:

Существует ли в компании разработанная политика информационной безопасности, все положения которой на практике внедрены в информационную систему?

а) Да

б) Нет

в) Положения политики внедрены частично.

После обработки ответа в таблицу базы данных записывается следующее:

При ответе “Нет” - “Необходимо разработать и внедрить комплексную политику информационной безопасности”.

При ответе “ Положения политики внедрены частично”- Необходимо добиться полного внедрения всех положений политики безопасности в информационную систему компании.

При ответе на остальные вопросы происходят те же действия.

### 2.5. Разработка функциональных схем элементов автоматизированной системы.

С позиции обеспечения безопасности информации в КС такие системы целесообразно рассматривать в виде единства трех компонент, оказывающих взаимное влияние друг на друга:

- информация;
- технические и программные средства;
- обслуживающий персонал и пользователи.

*Поэтому на первом этапе идет* определения вида ресурсов, представляющих ценность для компании

Осуществляем выполнение следующего алгоритма:

Вводим блок опроса, предназначенный для получения нашей системой данных, которые в последствии понадобятся для оценки рисков. Блок опроса при взаимодействии с пользователем определяет информацию, функционирующую в данной информационной системе, пользователей системы и аппаратные средства, предназначенные для обработки и хранения информации. Далее все это заноситься в файл базы данных Access. Это самый первый, и наверно даже ключевой этап работы, после проведения которого мы имеем в базе данных определенное количество таблиц , каждая из которых соответствует тому или иному ресурсу.

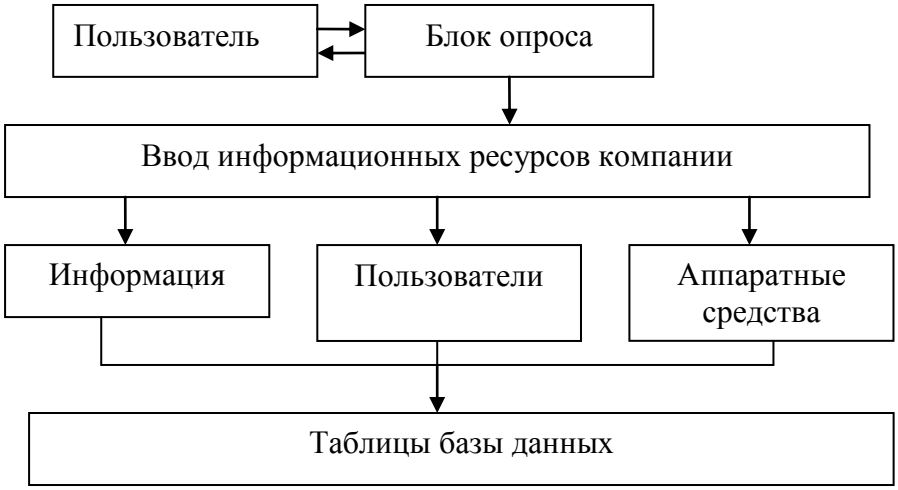



Рисунок 2.1. Схема функционирования блока опроса по выявлению ресурсов компании.

Следующий этап работы позволяет определить места хранения информации (Осуществить привязку данных) и оценить ущерб, который понесет компания в случае реализации одной из трех классических угроз, направленных на информацию. Речь идет об угрозах: конфиденциальности (право на чтение), целостности (право на запись) и отказа в обслуживании (нарушение работоспособности ресурса, на котором хранится ценная информация).

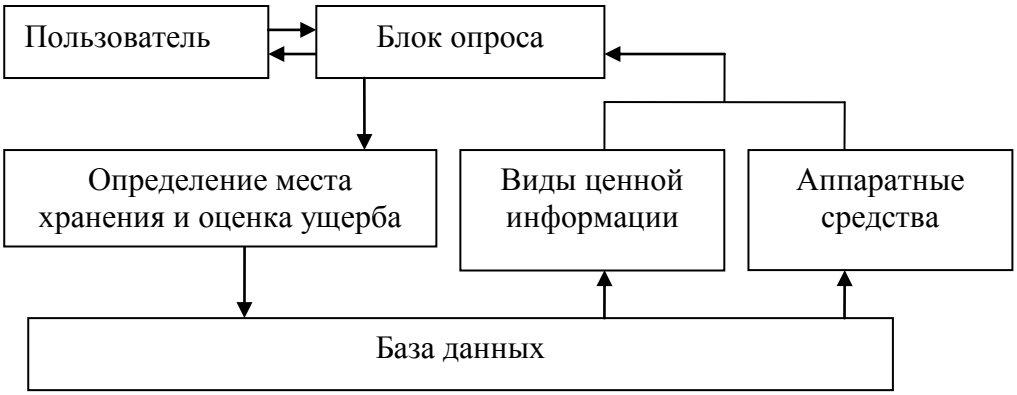



Рисунок 2.2. Схема функционирования блока опроса по привязке данных и оценки ущерба.

Из сформированных таблиц базы данных выводиться информация, циркулирующая в данной системе и аппаратные средства, предназначенные для ее хранения. Блок опроса определяет место хранения и одновременно оценивает ущерб. Полученные данные формируют очередную таблицу.

На следующем этапе работы происходит определение уровня угроз и уровня уязвимости.

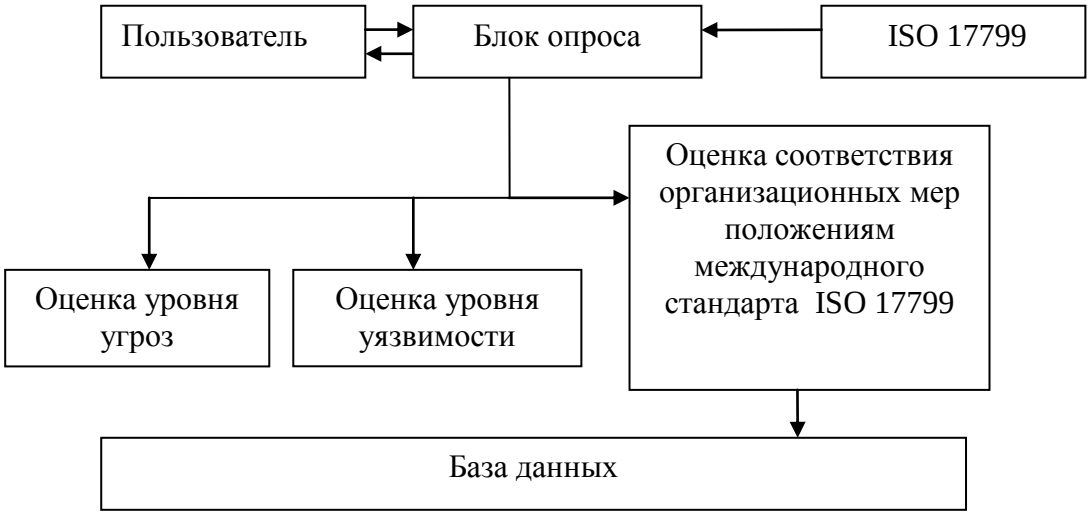



Рисунок 2.3. Схема функционирования блока опроса по оценкам уровня уязвимости, угроз и существующей политики безопасности.

Блок опроса, учитывая ответы на вопросы, оценивает уровни уязвимости и угрозы. Кроме этого происходит формирование в базе данных очередной таблицы с комментариями о не выполненных положениях стандарта.

Теперь осталось заполнить таблицы доступом субъектов системы к объектам системы. Это необходимо для того - чтобы программа, при расчете рисков знала какая категория пользователей (или кто из пользователей) к какому ресурсу имеет доступ, а к какому – нет. Кроме самого доступа, блок опроса определяет и права (чтение, запись, удаление). Блок опроса при взаимодействии с пользователем определяет доступ к ресурсам. Данные о ресурсах и пользователях выводятся на суд пользователю из уже сформированных таблиц базы данных. Полученные данные позволяют пересмотреть оценку уровня угрозы.

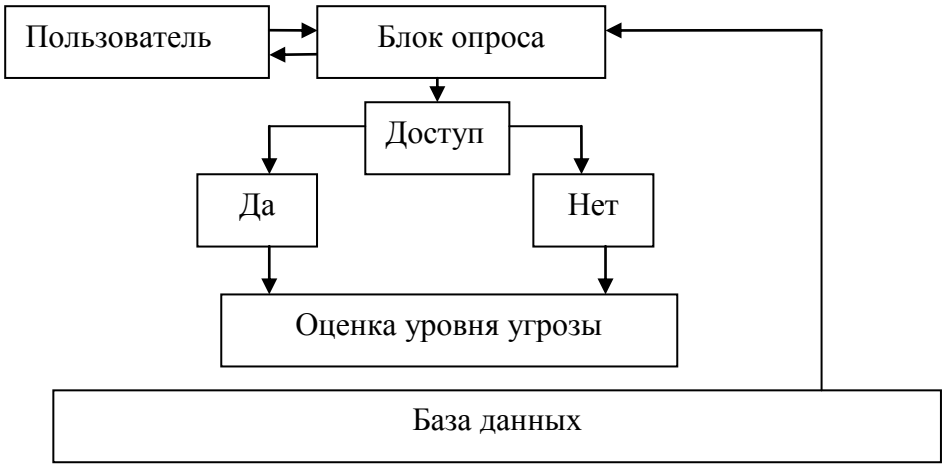



Рисунок 2.4. Схема функционирования блока опроса по выявлению доступа субъектов системы к объектам

Далее с целью  определение эффективности системы защиты информации требуется определить и внести в систему полную стоимость затрат на обеспечение информационной безопасности в год.

Блок опроса при взаимодействии с пользователем определяет полную стоимость затрат на обеспечение информационной безопасности. Полученные данные сохраняются в память.

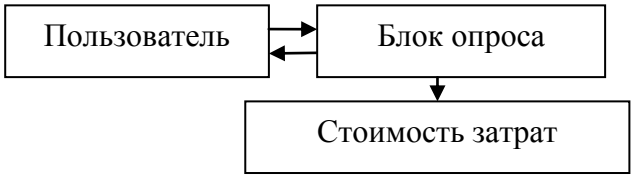



Рисунок 2.5. Схема функционирования блока опроса по выявлению эффективности системы защиты информации.

Следующий этап работы системы происходит  анализ рисков.

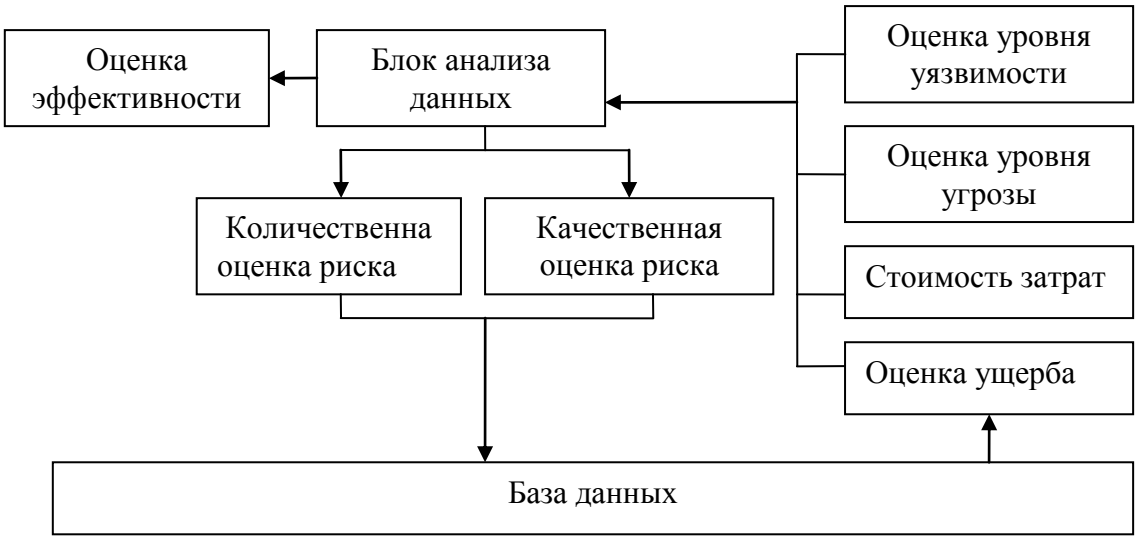



Рисунок 2.6. Схема функционирования блока анализа рисков.

В блок анализа данных поступает информация об оценках уровни уязвимости и угроз и информации о затратах на поддержании системы безопасности. В нем  по выбранной методики происходит анализ рисков , и выдаются качественная и количественная оценки рисков. Полученные данные отображаются в отчете .

## 2.5. Разработка алгоритма и интерфейса программы анализа информационных рисков.

Из существующих функциональных схем анализа и контроля рисков и проверки политики информационной безопасности компании можно построить алгоритм работы всей системы анализа.

На этом этапе необходимо определить взаимосвязь отдельных функциональных схем в самой системе анализа. Необходимо создать такой алгоритм  который позволит с минимальными вложением сил реализовать нашу систему в программном коде. Это позволить проверить правильность построения, верность функционирования и определить эффективность проведенной работы.

На анализе выше стающих функциональных схем и структурной схемы был построен следующий алгоритм.

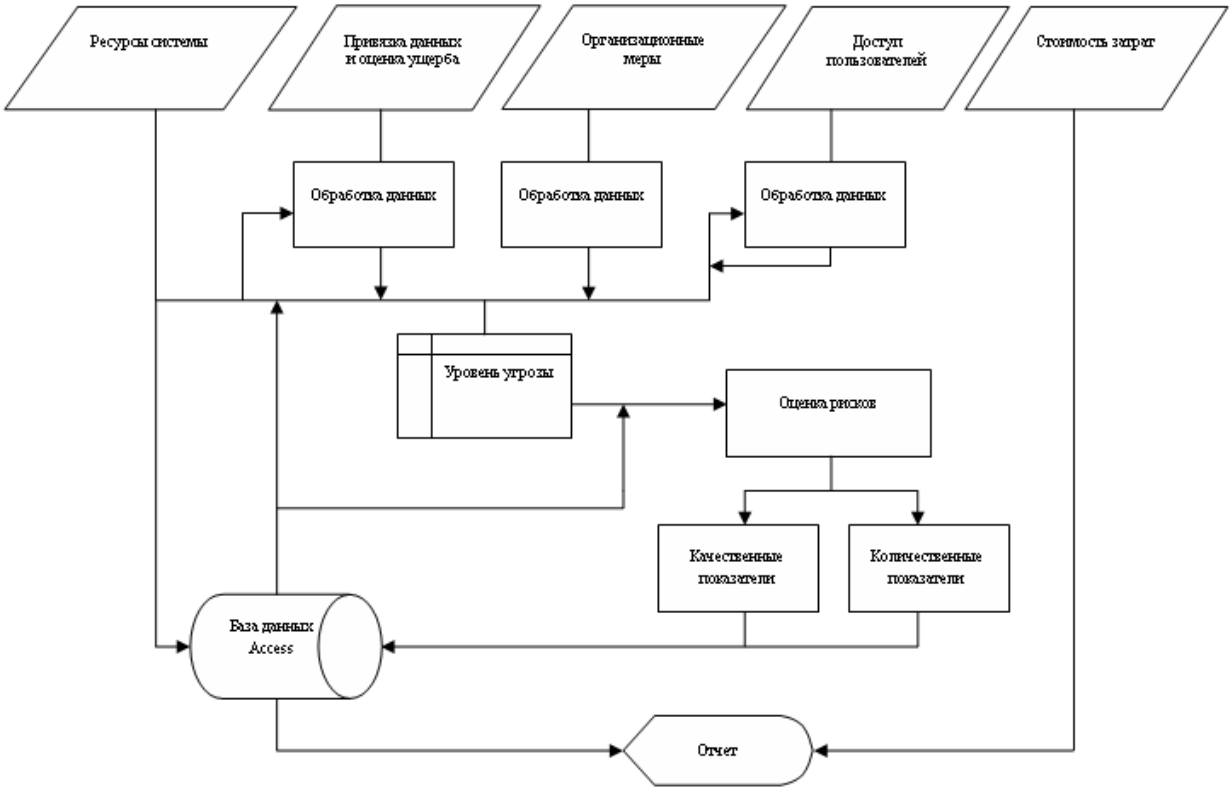



Рисунок 2.7. Алгоритм интерфейса программы анализа информационных рисков.

**Этапы функционирования**

Первым этапом работы всей системы – является получение необходимой информации для анализа. С помощью блока опроса и дальнейшей обработки , информация заноситься в базу данных. В результате – на начальном этапе заполняются данными три таблицы. В этих таблицах храниться:

1. Таблица”Inform”. Информация об основных категориях информационных ресурсов организации.
2. Таблица”Polzovateli”. Информация о пользователях.
3. Таблица”Server”. Информация о серверах.
4. Таблица”Stanzii”. Информация о рабочих станциях.

На втором этапе данные, после привязке и оценки ущерба заносятся в таблицу ”Stoimost”.

На третьем этапе происходит проверка организационных мер на соответствие положениям международного стандарта безопасности ISO 17799. Полученные данные записываются в таблицу “ISO17799”.

На третьем и четвертом этапах формируются данные о доступе, правах доступа и оценки ежегодные затраты на обеспечения информационной безопасности организации, которые поступают в “Блок анализа данных” где после запроса необходимой информации из базы данных Access происходит процесс анализа информационных рисков.

Пятый заключительный этап работы программы, полученные данные используются для формирования отчета.

**3. Интерфейс системы.**

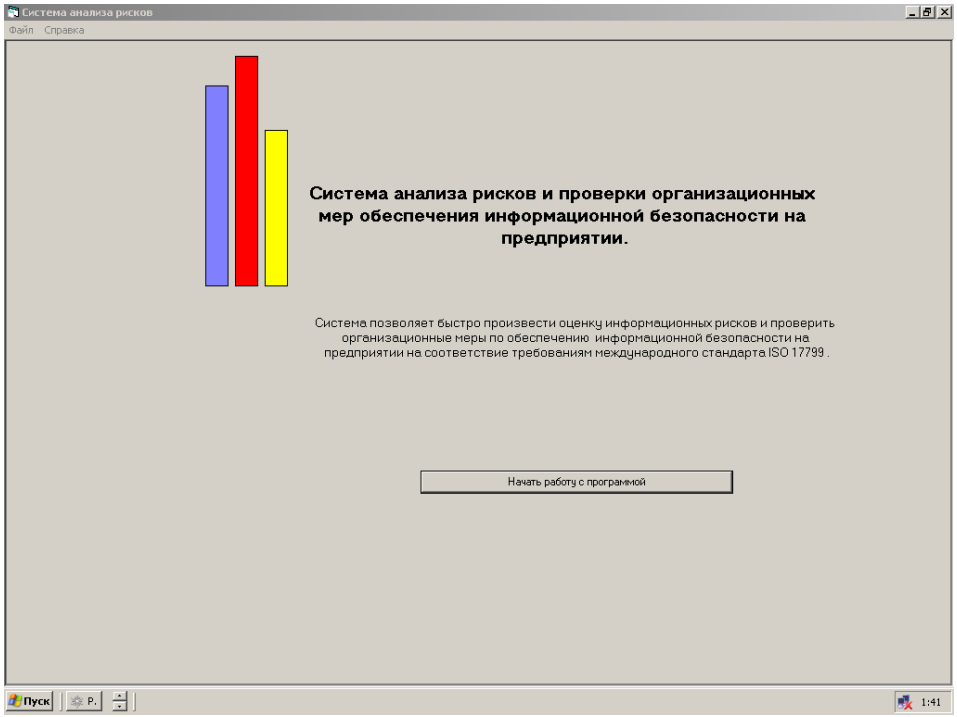



Рисунок.3.1 Главное окно программы

**Первым этап.** Определения полного списка информационных ресурсов, представляющих ценность для компании.

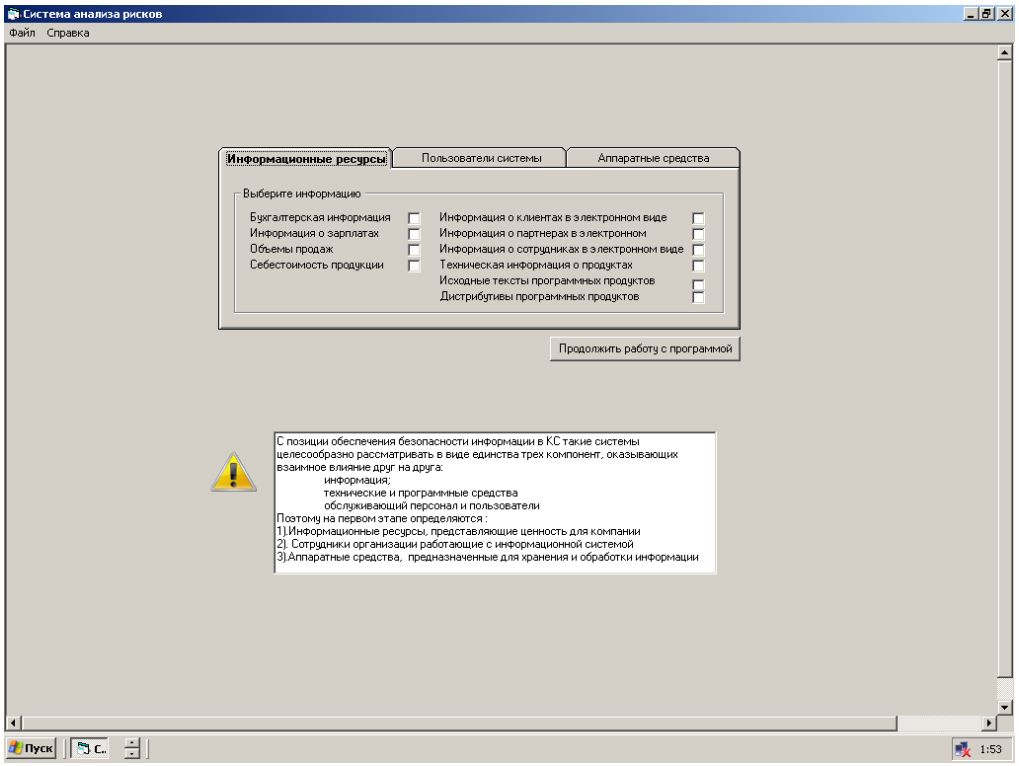


Рисунок 3.2. Интерфейс программы. Вкладка “Информационные ресурсы”.

Данная вкладка позволяет отметить виды информации, циркулирующие в системе:

Это может быть:

- Финансовая информация
- Бухгалтерская информация
- Информация о зарплатах
- Объемы продаж
- Себестоимость продукции

Ценная информация

- Информация о клиентах в электронном виде
- Информация о партнерах в электронном виде
- Информация о сотрудниках в электронном виде
- Техническая информация о продуктах
- Исходные тексты программных продуктов
- Дистрибутивы программных продуктов ( в том числе и собственные)
- Стратегические планы развития компании в электронном виде

Вкладка “Пользователи системы” дает возможность выбрать из приведенного списка тех пользователей, которые имеют отношение к данной информационной системе.

Это могут быть:

- Системные администраторы
- Офицеры безопасности
- Менеджеры
- Операторы или обычные пользователи

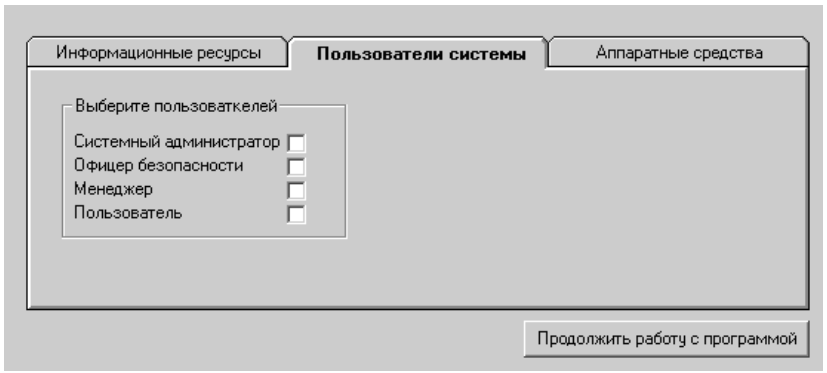



Рисунок 3.3 Интерфейс программы. Вкладка “Пользователи системы”.

Вкладка “Аппаратные средства” позволяет определить, место хранение и обработки информации.

Это могут быть:

- Сервера
- Рабочие станции
- Твердые копии

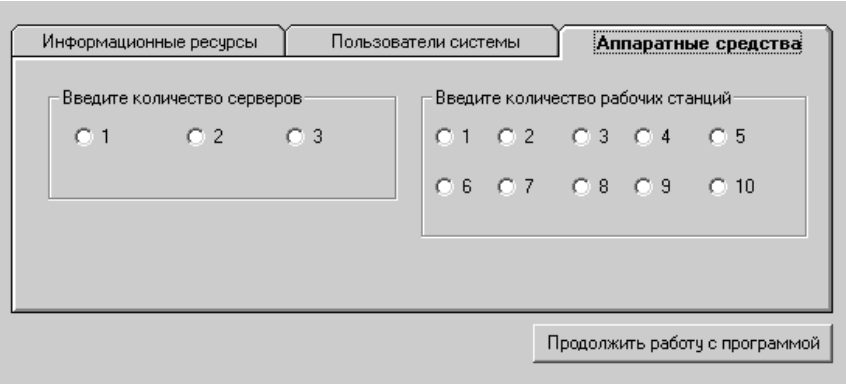



Рисунок 3.4. Интерфейс программы. Вкладка “Аппаратные средства”.

На вкладке приведенной ниже происходит привязка данных. Требуется расположить на каждом из ранее введенных ресурсов все указанные ранее виды ценной информации.

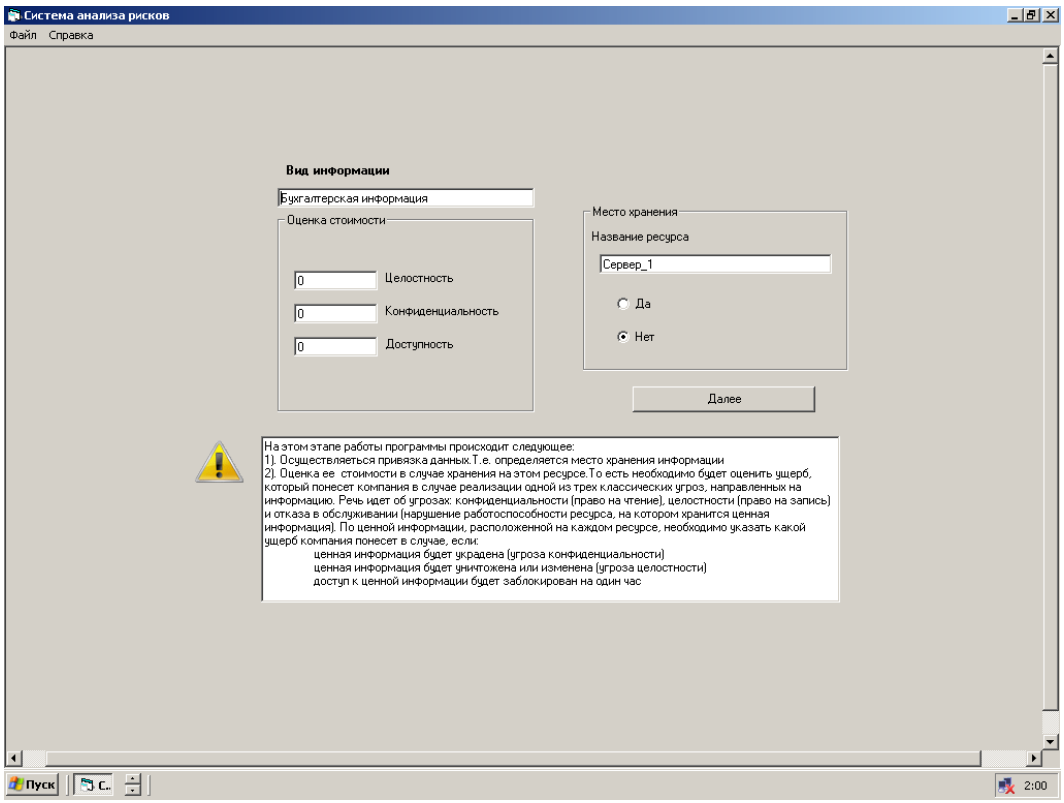


Рисунок 3.5. Интерфейс программы. Вкладка ”Привязка данных”.

Кроме этого на этом этапе работы необходимо еще определить стоимость информации. То есть необходимо оценить ущерб, который понесет компания в случае реализации одной из трех классических угроз, направленных на информацию. Речь идет об угрозах: конфиденциальности (право на чтение), целостности (право на запись) и отказа в обслуживании (нарушение работоспособности ресурса, на котором хранится ценная информация). По ценной информации, расположенной на каждом ресурсе, необходимо указать какой ущерб компания понесет в случае, если:

- ценная информация будет украдена (угроза конфиденциальности)
- ценная информация будет уничтожена или изменена (угроза целостности)
- доступ к ценной информации будет заблокирован на один час

Оценивая ущерб от реализации угроз, необходимо учитывать:

- цену ресурса - затраты на производство;
- стоимость восстановления или создания (покупку) нового ресурса;
- стоимость восстановления работоспособности организации (при работе с искаженным ресурсом, без него, при дезинформации);
- стоимость вынужденного простоя;
- стоимость упущенной выгоды (потерянный контракт);
- стоимость выплаты неустоек, штрафов (за невыполнение обязательств контракта);
- стоимость затрат на реабилитацию подмоченной репутации, престижа, имени фирмы;
- стоимость затрат на поиск новых клиентов, взамен более не доверяющих фирме;
- стоимость затрат на поиск (или восстановление) новых каналов связи, информационных источников.

Часто люди реально даже не представляют , чем владеют. Однако за владельцев оценить информацию не возможно. Предполагаемый злоумышленник может, конечно, оценить туже информацию иначе. Значить кто-то тут ошибается: владелец или злоумышленник. Конечно же , речь идет о приблизительной оценки. Точно оценить информацию очень сложно.

После проделанной работы мы переходим к следующему этапу, этапу “Проверки организационных мер обеспечения информационной безопасности на соответствие положением МСБ ISO 17799.

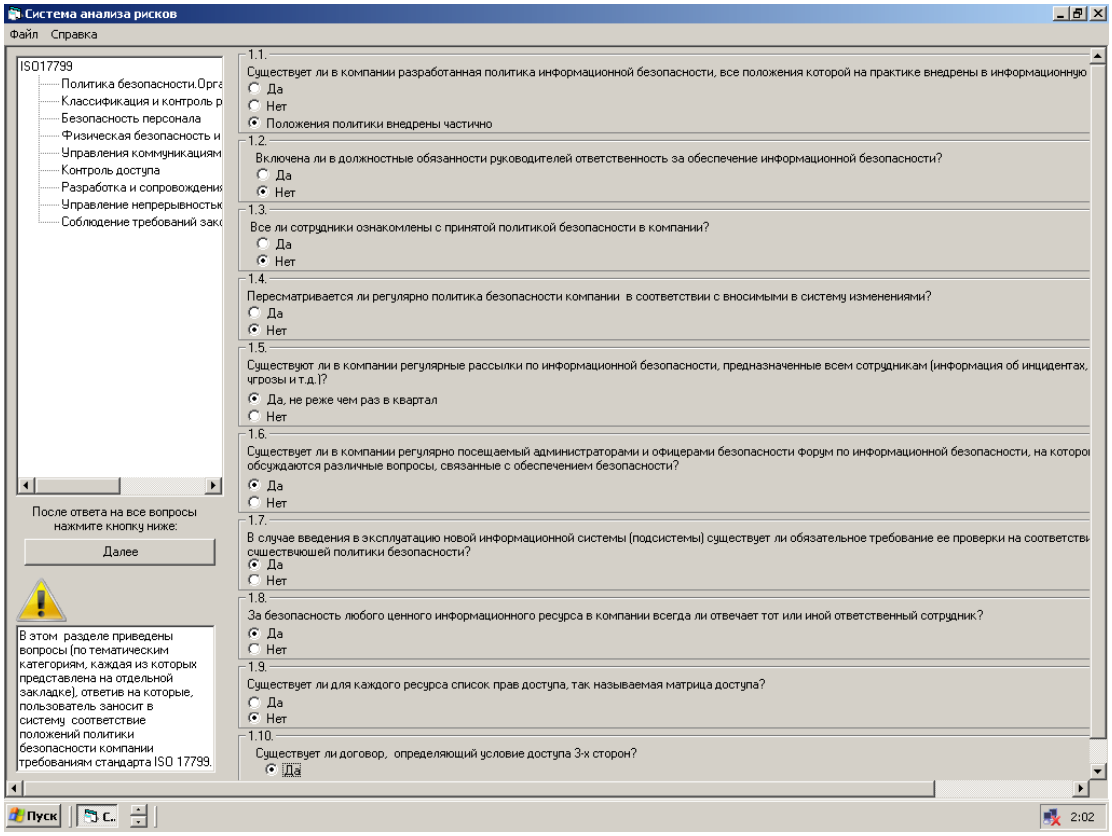



Рисунок 3.6. Интерфейс программы. Вкладка ”Организационные меры”.

Пользователю предлогается ответить на вопросы, разработанные после изучение положений МБО. Вопросы структурированы по разделам стандарта. Выбор раздела осуществляется в левой части экрана щелчком правой кнопки мыши. Вопросы отображаются в правой части. Это форма , как и все остальные , снабжена подсказками.

После ответа на все вопросы, пользователь нажимает кнопку далее и программа переходит к следующему окну.

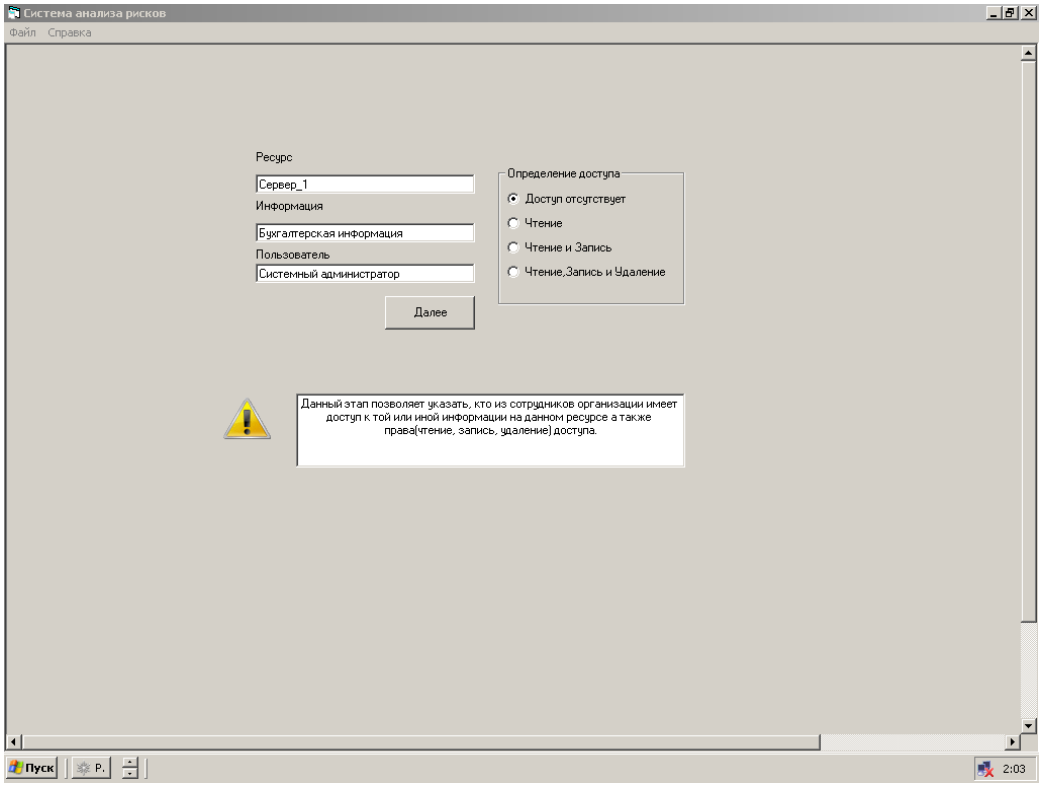



Рисунок 3.7. Интерфейс программы. Вкладка “доступ”.

Здесь необходимо определить доступ пользователей и его права (чтение, запись, удаление) ко всем ресурсам, содержащим ценную информацию. Переходим к следующему окну.

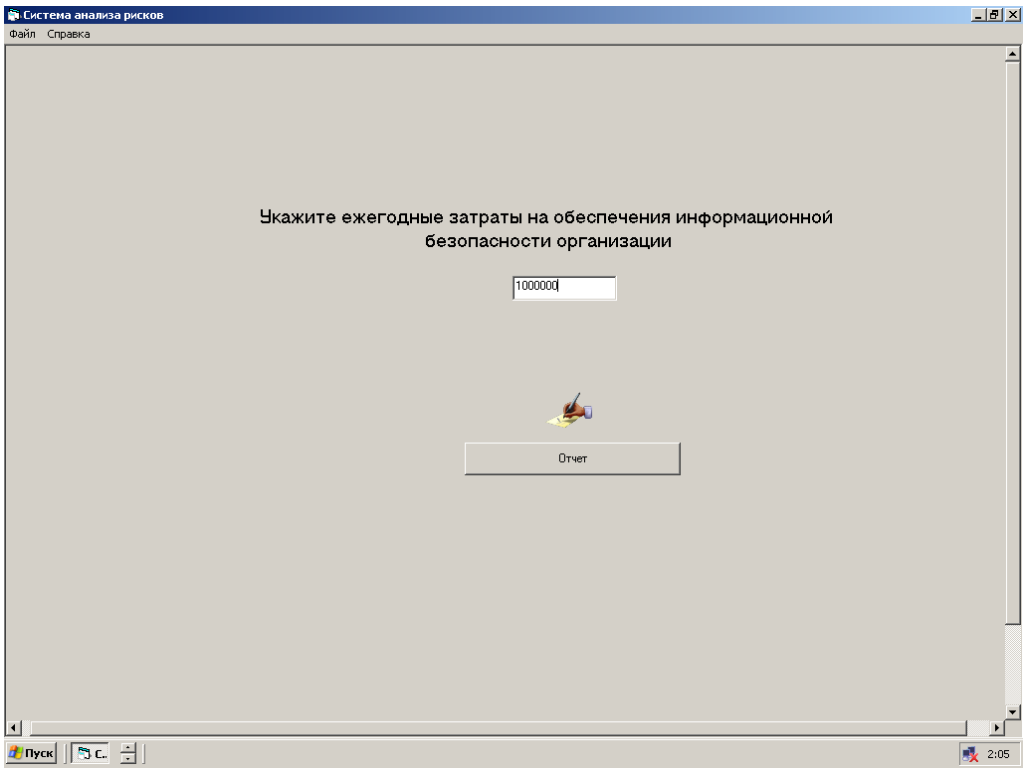


Рисунок 3.8. Интерфейс программы. Оценка затрат на поддержание системы безопасности.

На данном этапе работы с целью  определение эффективности системы защиты информации требуется определить и внести в систему полную стоимость затрат на обеспечение информационной безопасности.

В этом случае эффективность можно определить как отношение затрат к потерям которые понесет компания в случае реализации угроз безопасности.

Это могут быть:

- *Затраты на покупку систем защиты информации.* Другими словами, это стоимость лицензии программного обеспечения. Кроме того, необходимо также учесть в данном пункте затраты на аппаратное обеспечение - стоимость одного или нескольких компьютеров, на которых развернуты компоненты системы защиты. Также необходимо учесть затраты на покупку или создание средств технической защиты. Помимо этого, часто система защиты использует дополнительное программное и аппаратное обеспечение, стоимость которого также необходимо учитывать. К такому обеспечению можно отнести базы данных, системы настройки оборудования, системы резервирования, сетевые кабели, тройники, системы бесперебойного питания и т.д. В крупных компаниях, имеющих распределенную корпоративную сеть, не стоит забывать о затратах на внедрение (включая этап предварительного аудита).
- *Затраты на поддержку и обучение* (если она не включена в стоимость системы защиты). Сюда же можно отнести и командировочные расходы IT-специалистов на поездки в удаленные офисы и настройку удаленных компонентов системы обеспечения информационной безопасности.
- *Затраты на управление* (администрирование) системой защиты, которые включают зарплату администраторов безопасности и другого персонала, связанного с системой обнаружения атак и модернизацию ее программно-аппаратного обеспечения. К этой статье расходов относится оплата за услуги аутсорсинговых компаний и реагирование на инциденты безопасности.

Теперь система генерирует отчет и выводит полученные данные на обозрение.

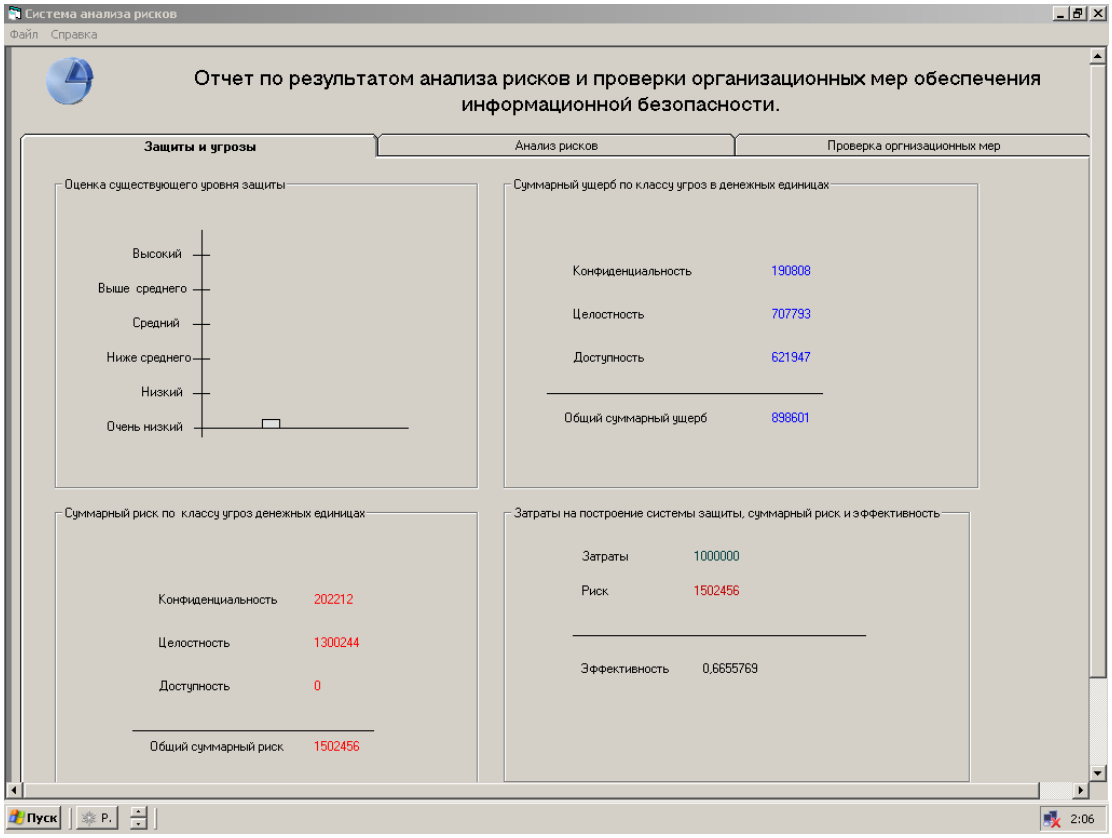



Рисунок 3.9. Интерфейс программы. Вкладка “Защита и угрозы”.

Данная вкладка позволяет пользователю визуально оценить существующий уровень информационной защиты, суммарный риск и ущерб по трем классам угроз и эффективность существующей системы защиты.

При щелчке мыши по вкладке “Анализ рисков” появляются еще две вкладки , демонстрирующие качественные и количественные показатели рисков

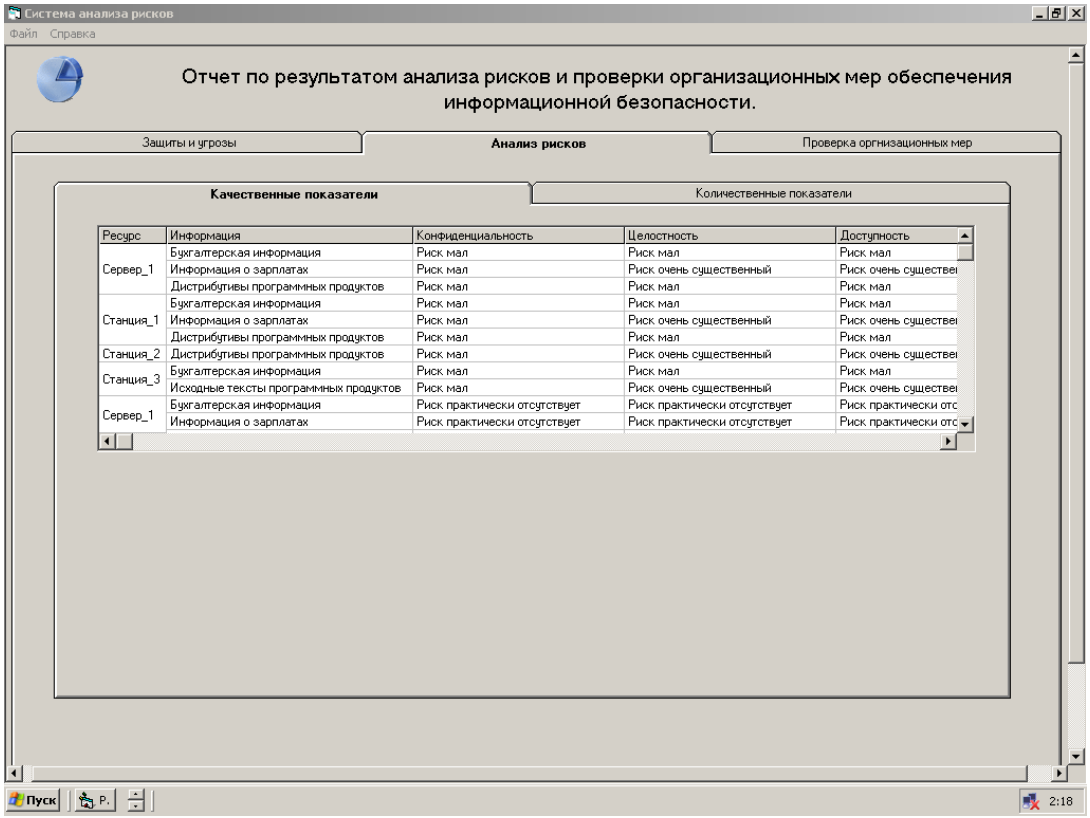



Рисунок 3.10. Интерфейс программы. Вкладка “Анализ рисков. Качественные показатели”.

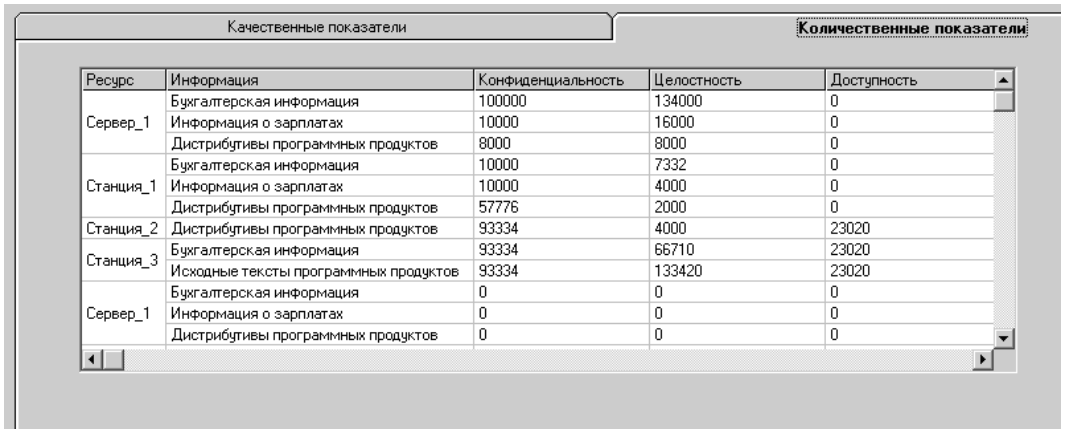



Рисунок 3.11. Интерфейс программы. Вкладка “Анализ рисков. Количественные показатели”.

Последняя вкладка “Проверка организационных мер ” демонстрирует пользователю , количество не соответствующих организационных мер положениям МБО и выводит пояснение.

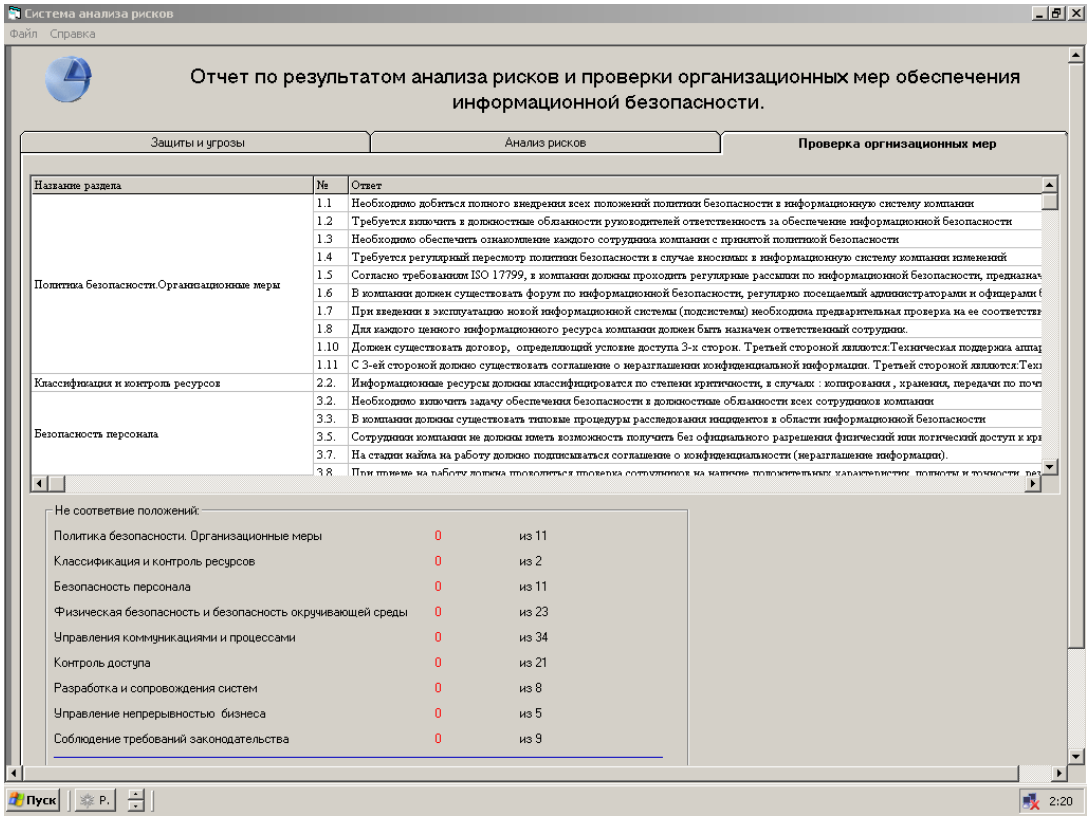



Рисунок 3.12. Интерфейс программы. Вкладка “ Проверка организационных мер ”.

## 4. Тестирование системы

Данный пункт необходим для проведения проверки верного функционирования расчетного блока программного кода (его части). Тестирование направленно на изучение зависимости потерь организации от некоторых факторов ( от классификация злоумышленника, права доступа пользователей системы и организационных мер обеспечения информационной безопасности**).**

Используемая при тестировании программного продукта информация не основывается на конкретных значениях, для конкретного предприятия – это абстрактные данные об абстрактном предприятии, необходимые для процесса тестирования.

Таблица 4.1.Исходные данные для исследования.

| | |
|---|---|
| Виды информации | Бухгалтерская информация<br>Информация о зарплатах<br>Информация о клиентах в электронном виде<br>Исходные тексты программных |

| | |
|---|---|
| | продуктов<br>Дистрибутивы программных продуктов ( в том числе и собственные)<br>Информация о партнерах в электронном виде |
| Пользователи системы | Системный администратор<br>Офицеры безопасности<br>Пользователь |
| Аппаратные средства | Сетевая группа:<br>Один сервер<br>Три рабочих станции |

Теперь осуществим привязку данных. Расположим на каждом из ранее введенных ресурсов указанные виды ценной информации.

Таблица 4.2. Привязка данных

| | |
|---|---|
| Сервер | Исходные тексты программных продуктов<br>Дистрибутивы программных продуктов (в том числе и собственные) |
| Рабочая станция один | Бухгалтерская информация<br>Информация о зарплатах |
| Рабочая станция два | Бухгалтерская информация<br>Информация о зарплатах |
| Рабочая станция три | Информация о клиентах в электронном виде<br>Информация о партнерах в электронном виде |

Для определения стоимости информации, необходимо оценить ущерб, который понесет компания в случае реализации трех классических угроз.

В предыдущем шаге мы разместили один и тот же тип информации на двух рабочих станциях. В этом шаге мы еще и оценим их одинаково. В конце тестов мы посмотрим результат и оценим, на сколько правильно работает алгоритм системы.

Таблица 4.3. Оценка информации

| Ресурс | Информация | Ущерб, в случае угрозы конфиденциальности, руб. | Ущерб, в случае угрозы целостности, руб. | Ущерб, в случае угрозы доступности, руб. |
|---|---|---|---|---|
| Сервер | Исходные тексты программных продуктов | 80 000 | 50 000 | 120 000 |
| | Дистрибутивы программных продуктов | 110 000 | 80 000 | 170 000 |
| Рабочая станция один | Бухгалтерская информация | 5 000 | 140 000 | 120 000 |
| | Информация о зарплатах | 130 000 | 260 000 | 100 000 |
| Рабочая станция два | Бухгалтерская информация | 5 000 | 140 000 | 120 000 |
| | Информация о зарплатах | 130 000 | 260 000 | 100 000 |
| Рабочая станция три | Информация о клиентах в электронном виде | 150 000 | 170 000 | 250 000 |
| | Информация о партнерах в электронном виде | 160 000 | 145 000 | 300 000 |

Определение доступа мы произведем по следующей схеме:

1) Ограничим доступ всех пользователей к информации, хранящейся на первой рабочей станции.

2) К тем же видам информации на второй рабочей станции права доступа оценим по разному.

Таблица 4.4.Определение прав доступа пользователей на рабочей станции два

| Пользователи | Информация | Права доступа |
|---|---|---|

| | | |
|---|---|---|
| Системный администратор | Бухгалтерская информация | Чтение , запись, удаление |
| | Информация о зарплатах | Чтение и запись |
| Офицер безопасности | Бухгалтерская информация | Чтение , запись, удаление |
| | Информация о зарплатах | Чтение и запись |
| Пользователь | Бухгалтерская информация | Чтение и запись |
| | Информация о зарплатах | Чтение |

3) Укажем доступ к информации, хранящейся на сервере и на третей рабочей станции в хаотичном порядке.

Таблица4.5. Определение прав доступа пользователей на рабочей станции три

| Пользователи | Информация | Права доступа |
|---|---|---|
| Системный администратор | Информация о клиентах в электронном виде | Чтение , запись, удаление |
| | Информация о партнерах в электронном виде | Чтение |
| Офицер безопасности | Информация о клиентах в электронном виде | Доступ отсутствует |
| | Информация о партнерах в электронном виде | Чтение, запись |
| Пользователь | Информация о клиентах в электронном виде | Доступ отсутствует |
| | Информация о партнерах в электронном виде | Чтение |

Таблица 4.6. Определение прав доступа пользователей на сервере

| Пользователи | Информация | Права доступа |
|---|---|---|
| Системный администратор | Исходные тексты программных продуктов | чтение |

| | | |
|---|---|---|
| | Дистрибутивы программных продуктов (в том числе и собственные) | Чтение и запись |
| Офицер безопасности | Исходные тексты программных продуктов | Чтение, запись, удаление |
| | Дистрибутивы программных продуктов (в том числе и собственные) | Чтение и запись |
| Пользователь | Исходные тексты программных продуктов | Доступ отсутствует |
| | Дистрибутивы программных продуктов (в том числе и собственные) | Доступ отсутствует |

Далее, для проверки организационных мер, осуществим невыполнение большинства требования международного стандарта ISO 17799. Это позволит увеличить уровень уязвимости системы. С помощью ответов на вопросы связанных с тем, на сколько сотрудники заинтересованы в неправомерных действиях, мы увеличим уровень угроз.

Оценим ежегодные затраты на обеспечения информационной безопасности в 500 тысяч рублей. Процесс тестирования дал следующие результаты.

Таблица 4.7.Результат расчета количественной характеристики рисков

| Ресурс | Информация | Риск связанный с угрозой конфиденциальности, руб. | Риск связанный с угрозой целостности, руб. | Риск связанный с угрозой доступности, руб. |
|---|---|---|---|---|
| Сервер | Исходные тексты программных продуктов | 480 000 | 400 000 | 960 000 |
| | Дистрибутивы программных продуктов | 660 000 | 640 000 | 1 020 000 |

| | | | | |
|---|---|---|---|---|
| Рабочая станция один | Бухгалтерская информация | 30000 | 840000 | 720000 |
| | Информация о зарплатах | 780000 | 1560000 | 600000 |
| Рабочая станция два | Бухгалтерская информация | 40000 | 1120000 | 960000 |
| | Информация о зарплатах | 1040000 | 2080000 | 600000 |
| Рабочая станция три | Информация о клиентах в электронном виде | 900000 | 1020000 | 1500000 |
| | Информация о партнерах в электронном виде | 960000 | 870000 | 1800000 |

Таблица 4.8. Результат расчета качественной характеристики рисков

| Ресурс | Информация | Риск связанный с угрозой конфиденциальности | Риск связанный с угрозой целостности | Риск связанный с угрозой доступности |
|---|---|---|---|---|
| Сервер | Исходные тексты программных продуктов | Риск велик | Риск очень велик | Риск очень велик |
| | Дистрибутивы программных продуктов | Риск велик | Риск очень велик | Риск очень велик |
| Рабочая станция один | Бухгалтерская информация | Риск велик | Риск велик | Риск велик |
| | Информация о зарплатах | Риск велик | Риск велик | Риск велик |
| Рабочая станция два | Бухгалтерская информация | Риск очень велик | Риск очень велик | Риск очень велик |
| | Информация о зарплатах | Риск очень велик | Риск очень велик | Риск очень велик |

| | | | | |
|---|---|---|---|---|
| Рабочая станция три | Информация о клиентах в электронном виде | Риск велик | Риск велик | Риск велик |
| | Информация о партнерах в электронном виде | Риск велик | Риск велик | Риск велик |

При этом система показала уровень системы защиты как низкий.

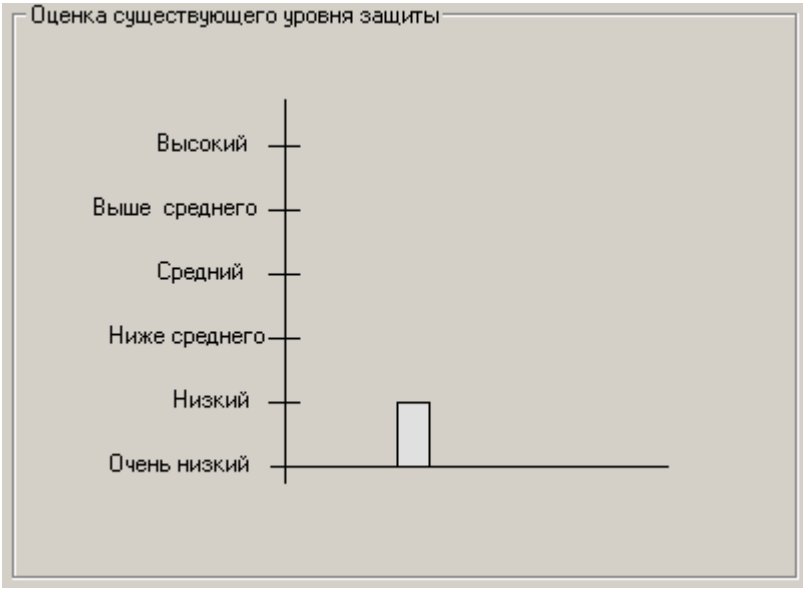



Рисунок 4.1. Оценка уровня защиты. Тест номер один.

Далее проведем следующее испытание программного комплекса. Теперь наоборот, попробуем выполнить как можно больше требований стандарта ISO17799.Это позволит увеличить уровень уязвимости системы и в некоторых случаях уровень угроз. Ответы ответов на вопросы связанные с тем, на сколько сотрудники заинтересованы в неправомерных действиях оставим такими же как и в первом тесте.

Процесс тестирования дал следующие результаты.

Таблица 4.9.Результат расчета количественной характеристики рисков

| Ресурс | Информация | Риск связанный с угрозой конфиденциальности, | Риск связанный с угрозой | Риск связанный с угрозой |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| | | руб. | целостности, руб. | доступности, руб. |
| Сервер | Исходные тексты программных продуктов | 160000 | 100000 | 240000 |
| | Дистрибутивы программных продуктов | 220000 | 240000 | 340000 |
| Рабочая станция один | Бухгалтерская информация | 10000 | 280000 | 240000 |
| | Информация о зарплатах | 260000 | 520000 | 200000 |
| Рабочая станция два | Бухгалтерская информация | 10000 | 420000 | 240000 |
| | Информация о зарплатах | 260000 | 780000 | 200000 |
| Рабочая станция три | Информация о клиентах в электронном виде | 300000 | 340000 | 500000 |
| | Информация о партнерах в электронном виде | 320000 | 290000 | 600000 |

Таблица 4.10. Результат расчета качественной характеристики рисков

| Ресурс | Информация | Риск связанный с угрозой конфиденциальности | Риск связанный с угрозой целостности | Риск связанный с угрозой доступности |
|---|---|---|---|---|
| Сервер | Исходные тексты программных продуктов | Риск мал | Риск мал | Риск мал |

| | | | | |
|---|---|---|---|---|
| | Дистрибутивы программных продуктов | Риск мал | Риск существенный | Риск существенный |
| Рабочая станция один | Бухгалтерская информация | Риск мал | Риск мал | Риск мал |
| | Информация о зарплатах | Риск мал | Риск мал | Риск мал |
| Рабочая станция два | Бухгалтерская информация | Риск мал | Риск существенный | Риск существенный |
| | Информация о зарплатах | Риск мал | Риск существенный | Риск существенный |
| Рабочая станция три | Информация о клиентах в электронном виде | Риск мал | Риск мал | Риск мал |
| | Информация о партнерах в электронном виде | Риск мал | Риск мал | Риск мал |

Организационные меры не соответствовали 23 положениям международного стандарта ISO 17799.


Рисунок 4.2. Оценка уровня защиты. Тест номер два

Из представленного материала мы видим , что произошло уменьшение риска до определенного уровня. Однако уровень угрозы со стороны сотрудников остался на определенном уровне, и это дало о себе знать. В целом система оценила уровень защиты как выше среднего.

Полученные данные говорят о том, что не соблюдение положений стандарта ISO 17799 приводит к увеличению риска связанного с угрозой конфиденциальности, целостности и доступности. Это в полнее справедливо так как, стандарт определяет базовый набор требований безопасности для широкого класса ИС, который формируется в результате обобщения мировой практики.

Мы заметили, что уровень рисков на рабочей станции два выше чем на номер один. Это говорит о том что, предоставление привилегированный прав доступа к информации, увеличивает уровень угрозы. Для борьбы с этим можно предпринять следующие меры:

Для того, чтобы понизить риск вредоносного воздействия со стороны сотрудников, необходимо уже при составлении должности максимально минимизировать количество информационных объектов, к которым пользователь будет иметь доступ впоследствии. В литературных источниках подобный принцип носит название принципа минимизации привилегий (либо прав доступа).

Потери предприятия тем меньше, чем меньше в этих потерях заинтересованы сотрудники данного предприятия. Очевидна необходимость ввода личной ответственности за собственную деятельность в отношении информационных активов компании. Личная ответственность предполагает разделение обязанностей по отношению к объектам, к которым пользователь имеет доступ. Отсюда суть второго результата тестирования: чтобы понизить риск вредоносного воздействия со стороны сотрудников, нужно следовать правилу разделения обязанностей.

При приеме на работу проводить проверку сотрудников на наличие положительных характеристик, полноты и точности резюме, подтверждение заявленного образования и профессиональной квалификации и независимую проверку документов – паспорта.

**5. Методика проведения работы**

**1. Цель работы.**

Целью данной работы является ознакомление с методикой анализа рисков, ролью анализа рисков в построении системы защиты, а также ознакомление с международным стандартом информационной безопасности ISO 17799.

**2.Теоретическая часть.**

Информацию по этому пункту вы в полном объеме найдете в меню “Справка”.

**3. Порядок выполнения работы**

1. После ознакомление с теорией получите у вашего преподавателя номер варианта на лабораторную работу. Каждый номер варианта представляет определенную модель информационной системы. Номера вариантов приведены ниже.

Таблица 5.1. Вариант 1.

| | |
|---|---|
| Название | Компания ”РеалСофт” |
| Сотрудники | Директор (сотрудник)<br>Системный администратор<br>Офицер безопасности<br>Бухгалтер (сотрудник)<br>Менеджер<br>Программисты (сотрудники) |
| Информация | Бухгалтерская информация<br>Информация о зарплатах<br>Исходные тексты программных продуктов<br>Дистрибутивы программных продуктов |
| Аппаратные средства для обработки информации | Два сервера<br>Шесть рабочих станций |
| Описание | Организация занимается разработкой программного обеспечения. Расположена в отдельном здании. На входе расположена будка с охраной. |
| Затраты на информационную | 100 000 |

| | |
|---|---|
| безопасность в год | |

Таблица 5.2. Вариант 2.

| | |
|---|---|
| Название организации | Нотариальная контора ”Парус” |
| Сотрудники | Директор<br>Бухгалтер (сотрудник)<br>Менеджер |
| Информация | Бухгалтерская информация<br>Информация о зарплатах<br>Дистрибутивы программных продуктов<br>Информация о клиентах в электронном виде |
| Аппаратные средства для обработки информации | Один сервер<br>Три рабочих станции |
| Описание | Занимается оформление договоров купли-продажи, обмена, дарения жилья, автомашин, земельных участков, копий документов. Проводит квалифицированные консультации по нотариальным вопросам<br>Арендуемое помещение на втором этаже. Кроме этой организации в здании расположено еще несколько фирм. На входе существует охрана , которую интересует целью прихода |
| Затраты на информационную безопасность в год | 10 000 |

Таблица 5.3. Вариант 3.

| | |
|---|---|
| Название организации | Страховая компания “Под крылом” |
| Сотрудники | Директор (пользователь)<br>Бухгалтер (пользователь)<br>Системный администратор<br>Менеджеры |
| Информация | Бухгалтерская информация |

| | |
|---|---|
| | Информация о зарплатах<br>Информация о клиентах в электронном виде<br>Информация о сотрудниках в электронном виде<br>Дистрибутивы программных продуктов |
| Аппаратные средства для обработки информации | Один сервер<br>Четыре рабочих станции |
| Описание | Компания занимается страхованием всех видов деятельности. Расположена в отдельном здании. На входе сидит охранник. |
| Затраты на информационную безопасность в год | 200 000 |

Таблица 5.4. Вариант 4.

| | |
|---|---|
| Название организации | Филиал нефтяной компании в Томске “РусНефть” |
| Сотрудники | Директор (сотрудник)<br>Системный администратор<br>Офицер безопасности<br>Бухгалтер (сотрудник)<br>Менеджер<br>Программисты (сотрудники) |
| Информация | Бухгалтерская информация<br>Информация о зарплатах<br>Информация о клиентах в электронном виде<br>Дистрибутивы программных продуктов<br>Объемы продаж |

| | |
|---|---|
| | Себестоимость продукции |
| | |
| Описание | Занимается транспортировкой и переработкой нефти. Расположена в отдельном здании. Существует служба безопасности. На входе охрана регистрирует цель прихода. |

Таблица 5.5. Вариант 5.

| | |
|---|---|
| Название организации | Компьютерная фирма ”Ваш компьютер” |
| Сотрудники | Директор (сотрудник)<br>Системный администратор<br>Бухгалтер (сотрудник)<br>Менеджеры |
| Информация | Бухгалтерская информация<br>Информация о зарплатах<br>Дистрибутивы программных продуктов<br>Объемы продаж<br>Информация о партнерах в электронном виде<br>Техническая информация о продуктах |
| Аппаратные средства для обработки информации | Два сервера<br>Три рабочих станции |
| Описание | Занимается продажей компьютеров, офисной техники, сетевого оборудования, программного обеспечения. Расположена в отдельном здании. Существует служба охраны. |
| Затраты на информационную безопасность в год | 1 000 000 |

2. Для того чтобы приступить к работе с “ Системой анализа рисков и проверки организационных мер обеспечения информационной безопасности на предприятия”, необходимо запустить файл Project.exe. Далее система покажет окно с предложением начать работу с программой

3. Выберите те виды информационных ресурсов которые представлены в вашем варианте. Теперь перейдите к вкладке “Пользователи системы”, где надо будет отметить пользователей информационной системы. На вкладке “Аппаратные средства” определите количество серверов и рабочих станций из вашего варианта. Нажмите кнопку ”Продолжить работу с программой”.

4. Укажите на сервере хранение двух любых видов информации из списка, а на рабочих станциях по четыре вида информационных ресурса, желательно разных и оцените предполагаемый ущерб, в случае угроз конфиденциальности, целостности и доступности. Так как данные хранятся на разных ресурсах, то предполагается, что они имеют разную ценность. В случае если информация не храниться на выбранном ресурсе, то ее оценка не имеет смысла - эти данные все равно не будут использованы. В случае затруднения обратитесь к подсказке.

5. Далее система отобразит окно, с вопросами по разделу стандарта в правой части и выбором раздела стандарта в левой части экрана. Отвечать на вопросы лучше всего, начиная с первого раздела “Политика безопасности. Организационные меры”. Оцените систему безопасности выбранной организации, учтите как можно больше недостатков,

так как полное описание организационных мер обеспечения информационной безопасности для представленных вариантов не представляется возможным. Нажмите кнопку “Далее”.

6. Перед вами окно с определением доступа пользователей к информационным ресурсам.

Ограничьте доступ к информации на первой выбранной станции. К тем же видам информации на второй рабочей станции, определите разные виды доступа пользователей.

На остальных серверах и рабочих станциях виды доступа определите сами.

7. Теперь на экране должно появиться окно для ввода затрат на информационную безопасность. Затраты можно определить из вашего варианта. Это заключительный этап сбора информации о вашей организации. Далее программа генерирует отчет по результатам анализа.

8. Ознакомьтесь с представленным отчетом. Сравните риск и ущерб по трем классам угроз. Оцените на ваш взгляд эффективность системы защиты. Перейдите к вкладке “Анализ

рисков”. Сравните данные о риске по трем классом угроз на рабочих станциях , к информации на которых был представлен доступ и к которым нет. Сделайте выводы.

9. Перейдите к вкладке “Проверка организационных мер”. Посмотрите, какое количество организационных мер соответствуют положениям стандарта, и какое нет. Далее вам предстоит ознакомиться с основными положениями международного стандарта безопасности ISO 17999.

10. Сделайте скриншоты трех вкладок отчета и сохраните их в своей отчет по лабораторной работе. Закройте окно программы. Снова откройте файл Project.exe. Повторите 3 и 4 пункт. Попытайтесь в 5 пункте соблюсти как можно больше положений МСБ ISO 17999. Далее повторите 7, 8, 9 пункт. Сделайте выводы.

**Контрольные вопросы**

1. Дайте определение понятия - Политика информационной безопасности.

2.Что такое процесс анализа рисков? Какова роль анализа рисков в процессе формирования политики безопасности компании.

3. В чем отличие полного анализа рисков от базового?

4.Что понимается под угрозой безопасности информации?

5.На какие два класса делиться все множество потенциальных угроз безопасности информации?

6.В чем заключается оценка рисков по двум факторам?

7.В чем заключается оценка рисков по трем факторам?

8. Дайте определение понятию “Уязвимость”.

9.Дайте определение понятиям “угроза конфиденциальности”, ”угроза целостности” и “угроза доступности”.

10. Назовите основные разделы стандарта ISO 17799.

## 10. ЗАДАНИЯ НА САМОСТОЯТЕЛЬНУЮ РАБОТУ

Содержание

Введение

Часть 1: Политика безопасности

1.1Политика безопасности

1.1.1 Основные положения политики обеспечения информационной безопасности

1.1.2 Анализ и обновление

1.1.3 Организационные меры по обеспечению безопасности

1.1.4 Классификация и управление ресурсами

1.2 Безопасность персонала

1.2.1 Безопасность при выборе персонала и работе с ним

1.2.2 Тренинги пользователей

1.2.3 Реагирование на инциденты в области безопасности, а также сбои и неисправности

1.2.4 Физическая безопасность

1.2.5 Безопасность кабельной системы

1.2.6 Безопасное уничтожение отработавшего оборудования

1.2.7 Безопасность рабочего места

1.3. Управление коммуникациями и процессами

1.3.1 Служебные инструкции и ответственность

1.3.2 Контроль изменений в операционной среде (среды функционирования)

1.3.3 Процедуры реагирования на инциденты

1.3.4 Разграничение ответственности путем разделения обязанностей

1.3.5 Разделение ресурсов

1.3.6 Защита от вредоносного программного обеспечения (вирусов, троянских коней)

1.3.7 Управление внутренними ресурсами

1.3.8 Управление сетью

1.3.9 Безопасность носителей данных

1.3.10 Безопасность при передаче информации и программного обеспечения

1.4 Контроль доступа

1.4.1 Политика контроля доступа

1.4.2 Управление доступом пользователя

1.4.3 Ответственность пользователей

1.4.4 Контроль и управление удаленного (сетевого) доступа

1.4.5 Контроль доступа в операционную систему

1.4.6 Контроль и управление доступом к приложениям

1.4.7 Мониторинг доступа и использования систем

1.4.8 Мобильные компьютеры и пользователи

1.5 Разработка и техническая поддержка вычислительных систем

1.5.1 Безопасность приложений

1.5.2 Средства криптографической защиты

1.5.3 Безопасность системных файлов

1.5.4 Защита рабочих данных, используемых при тестах систем

1.5.5 Контроль доступа к исходным текстам программ и библиотек

1.5.6 Процедуры контроля изменений

1.5.7 Технический обзор изменений в операционной среде

1.5.8 Ограничения на изменения прикладного ПО

1.5.9 Безопасность процессов разработки и поддержки

1.6 Управление непрерывностью бизнеса

1.6.1 Процесс управления непрерывным ведением бизнеса

1.6.2 Создание и внедрение плана непрерывности бизнеса

1.6.3 Основы планирования непрерывности бизнеса

1.6.4 Тестирование планов обеспечения непрерывности бизнеса

1.6.5 Обеспечение и переоценка планов

1.7. Соответствие системы основным требованиям

1.7.1 Соответствие требованиям законодательства

1.7.2 Соответствие политике безопасности

1.7.3 Соответствие техническим требованиям

1.7.4 Методы и средства управления системным аудитом

Часть 2: Пример типовой политики безопасности компании, имеющей выход в Интернет и обладающей ресурсами, к которым необходим доступ из Интернет

2.1 Сетевая безопасность

2.2 Локальная безопасность (безопасность рабочих станций и серверов)

2.3 Физическая безопасность

2.4 Типовые документы, основанные на стандарте безопасности ISO 17799

2.4.1 Основные требования по обеспечению внутренней ИТ- безопасности компании. Общие положения

2.4.2 Основные правила, инструкции и требования по обеспечению внутренней ИТ- безопасности компании

Часть 3: Современные методы и средства сетевой защиты

3.1 Межсетевые экраны

3.1.1 Коммутаторы

3.1.2 Пакетные фильтры

3.1.3 Шлюзы сеансового уровня

3.1.4 Посредники прикладного уровня

3.1.5 Инспекторы состояния

3.2 Системы контроля содержания

3.3 Системы контроля целостности

3.4 Системы построения VPN

3.5 Системы обнаружения атак

3.6 Системы анализа защищенности

3.7 Обманные системы

3.8 Создание типовой архитектуры безопасности корпоративной сети

Введение

Бурное развитие информационных технологий в конце 20 века привело к тому, что на сегодняшний день практически все бизнес-процессы любой компании основаны на использовании различных автоматизированных систем. Подобная тенденция к всеобщей автоматизации бизнес-процессов обусловлена конкурентной борьбой: чем ниже себестоимость продукции и, следовательно, - тем выше конкурентоспособность компании. Именно поэтому такое широкое применение в экономике нашли компьютерные сети и в том числе Internet и созданные на их базе различные распределенные вычислительные системы, позволяющие существенно сократить время, необходимое для выполнения различных технологических операций.

Однако наряду с безусловными позитивными моментами, связанными с всеобщей автоматизацией и широким применением компьютерных сетей, существуют и негативные стороны. К ним, прежде всего, необходимо отнести вновь возникающие проблемы, связанные с безопасностью обрабатываемой информации в автоматизированных системах компаний. Всего существую три классических угрозы безопасности информации - это *угрозы раскрытия, целостности и отказа в обслуживании*.

Итак, Вы - ИТ менеджер банка, финансовой или промышленной компании. Что произойдет, если информация (счета, активы клиентов, информация о поставщиках, клиентах и т.д.), обрабатываемая в Вашей информационной системе, попадет к конкурентам или к злоумышленникам - угроза раскрытия? Что случится, если произойдет несанкционированное изменение критично важных для Вашей компании электронных документов - угроза целостности? Что произойдет, если внезапно Ваша автоматизированная система будет остановлена - угроза отказа в обслуживании?

Результаты последних исследований, проведенных в 2001 г, показывают, что, несмотря на то, что большинство топ - менеджеров осознает основные угрозы для сферы обслуживания клиентов и внутренней инфраструктуры компании, они не до конца отдают себе отсчет, откуда исходит опасность, какая информация является наиболее деликатной и уязвимой, и какие действия следует предпринять, чтобы уменьшить риск взлома и иной несанкционированной деятельности. При этом топ-менеджмент из-за своей инертности запаздывает с изменением политики внутри компаний минимум на полгода. Очевидно, что смена приоритетов требует многочисленных согласований внутри корпораций, а активное общественное мнение смещает акценты, рисуя "иллюзорные" картины источников опасности: до сих большинство топ - менеджеров считает хакеров и внешние атаки наиболее опасными для бизнеса их компаний, но при этом по статистике до 80% злоупотреблений берут начало внутри компании. Также исследования показывают, что обычным фактом

является слабая приверженность организаций к аудиту информационной безопасности (35%), минимальные усилия по стимулированию легального расследования "инцидента" (17%), недостаточное понимание, откуда исходит угроза (79% до сих пор стереотипно считают, что "извне", хотя статистика показывает обратное).

Ежедневно в Интернет злоумышленниками осуществляются сотни - тысячи взломов веб-сайтов, серверов приложений и баз данных. Взлом корпоративного веб-сайта компании, являющегося ее представительством в Сети, может серьезно подорвать имидж и репутацию компании и вызвать падение ее курса акций.

Огромное число успешных вторжений из Интернет наглядно показывает незащищенность большинства ресурсов. Незащищенность сети компании, обычно, обусловлена целым рядом факторов и заблуждений:

типовые факторы**:**

- непонимание величины ущерба, который может принести успешная атака на ИТ систему компании;
- отсутствие информации об истинном уровне защиты;
- ложная уверенность о надежной собственной защите;
- отсутствие или нехватка квалифицированного персонала в отделе ИТ – безопасности;
- отсутствие разработанной стратегии и политики информационной безопасности;
- отсутствие или недостатки применяемой системы защиты ИТ – ресурсов.

типовые заблуждения:

- "мы не представляем интереса для атаки";
- "в нашей вычислительной системе нет критичной важной для компании информации";
- "наш веб-сервер выполняет только представительскую функцию и его взлом не повлечет для компании значимого ущерба";
- "у нас есть файрвол - мы надежно защищены".

Любая крупная компания обычно обладает достаточно разветвленной и сложной ИТ-инфраструктурой, которая позволяет автоматизировать решение основных бизнес процессов компании. Но чем функциональнее информационная система, тем сложнее в ней решать вопросы, связанные с обеспечением безопасности обрабатываемой в ней информации. Для того, чтобы наилучшем образом обеспечить безопасность системы и избежать избыточных расходов, прежде всего, необходимо провести комплексный анализ безопасности информационных ресурсов компании (аудит безопасности) причем желательно силами

сторонних независимых аудиторов, которые укажут на слабые места в имеющейся системе обеспечения безопасности и предложат оптимальный комплекс мер по повышению текущего уровня защищенности сети. Зачем же проводить аудит автоматизированных внутренних ресурсов компании? Во-первых, по международной статистике порядка 80% всех взломов осуществляется именно изнутри компании ее собственным персоналом. Во-вторых, только проведение полного аудита безопасности компании позволит обнаружить все слабости в существующей системе защиты, разработать и внедрить стратегию, политику и архитектуру безопасности.

На основании проведенного аудита безопасности корпоративной сети осуществляется разработка стратегии и политики информационной безопасности компании; разработка, внедрение и поддержка безопасного решения, позволяющего повысить защищенность информационных ресурсов компании до необходимого уровня

И так, безопасность любой компании начинается с независимого аудита. Следующим шагом является разработка стратегии и политики информационной безопасности. Политика безопасности компании – это краеугольный камень, с которого начинается безопасность, которую позволяет разработать полный анализ рисков ядра автоматизированных бизнес процессов. Набор необходимых правил, требований и нормативных документов для обеспечения требуемого уровня защищенности.

Необходимо определить кто будет отвечать за информационную безопасность. Какова процедура задания новых пользователей или изменения рабочей конфигурации системы. Каковы Ваши действия – что происходит в случае атаки. Какова процедура увольнения ИТ сотрудника. Весь сложнейший комплекс административно-технических вопросов должен быть регламентирован в рамках разработанной комплексной политики безопасности компании. Отсутствие разработанной политики четко показывает недостаточное внимание компании к вопросам безопасности её информационных ресурсов. И наоборот, наличие работающей политики безопасности помимо обеспечения реальной защиты придает компании серьезный имидж в глазах заказчиков и потенциальных инвесторов и выгодно сказывается на ее репутации даже среди конкурентов.

Обнаружить недостатки в системе безопасности, разработать стратегию и политику безопасности - все это является необходимым, но не достаточным условием надежной защиты сети компании. Третьим и последним условием является разработка и *внедрение* архитектуры безопасности или иными словами разработка и внедрение проекта защиты.

Проект защиты - это совокупность административных, программных и технических мер и средств, позволяющих обеспечить защиту автоматизированной системы в соответствие с требуемым уровнем. Необходимый для компании уровень защиты определяется на этапе комплексного аудита безопасности ресурсов сети.

Внедрение проекта защиты позволит компании надежно обеспечить безопасность своих автоматизированных ресурсов, контролировать работу собственного персонала, отследить и отразить возможные атаки злоумышленников и ликвидировать или минимизировать возможные потери от их действий. А статистика нарушений информационной безопасности неумолима. Согласно исследованиям американского Общества промышленной безопасности (American Society for Industrial Security) и компании PricewaterhouseCoopers корпорации, входящие в Top-1000 журнала Fortune, потеряли от краж внутренней информации 45 млрд. долл. только в 1999 году.

Часть 1

## 1.1 Политика безопасности

Необходимость разработанной соответствующей политики безопасности, на сегодняшний день является очевидным фактом для любой даже достаточно небольшой компании. Политика безопасности в целом - это совокупность программных, аппаратных, организационных, административных, юридических, физических мер, методов, средств, правил и инструкций, четко регламентирующих все аспекты деятельности компании, включая информационную систему, и обеспечивающих их безопасность. Политика безопасности является одним из важнейших, жизненно важных документов компании. К сожалению, еще встречаются отдельные руководители, которые считают, что им нечего защищать. Не будем повторять прописные истины: опыт большинства экспертов по информационной безопасности говорит, что в любой компании всегда найдется электронный ресурс, требующий того или иного уровня защиты. Напомним лишь, что разработка плана действий на случай непредвиденных обстоятельств является неотъемлемой частью любой политики безопасности. И, как показывает практика, (вспомним терракты 11 сентября в США), те предприятия, у которых был разработан и протестирован подобный план, понесли значительно меньшие убытки, чем компании, не имевшие подобного плана, задачей которого является обеспечение непрерывности ведения бизнеса.

Кроме своего прямого назначения, разработка политики безопасности дает и неожиданный, на первый взгляд, побочный эффект: в результате анализа информационных потоков, инвентаризации информационных ресурсов и ранжирования обрабатываемой информации по степени ценности руководство организации получает целостную картину одного из самых сложных объектов управления - информационной системы, что положительно влияет на качество управления бизнеса в целом, и, как следствие, улучшает его прибыльность и эффективность.

### 1.1.1 Основные положения политики обеспечения информационной безопасности

1. Определение информационной безопасности, перечень ее составляющих.
2. Положение о целях управления - поддержка целей и принципов информационной безопасности.
3. Краткое разъяснение политики безопасности, принципов ее построения и стандартов в этой области. Соответствие политики требованиям, имеющим особое значение для организации:

- соответствие положений политики местному и международному законодательству;
- обучение персонала по вопросам безопасности;
- обнаружение и блокирование вирусов и других вредоносных программ;
- непрерывность ведения бизнеса;
- последствия нарушения политики безопасности.

4. Включение в должностные обязанности руководителей ответственности за обеспечение информационной безопасности, включая отчеты об инцидентах.

5. Подробный перечень документов, которые должны быть изданы вместе с политикой безопасности (положения, инструкции, регламенты и т.п.).

Прежде всего, обратим внимание на требование стандарта перечислить все объекты информационной инфраструктуры, подлежащие защите. Это не просто сделать даже в средних компаниях, не говоря уже о крупных. Зачастую, эта задача решается с привлечением внешней аудиторской фирмы, специализирующейся на вопросах информационной безопасности.

**Соответствие законодательству** - чрезвычайно важный пункт любой политики безопасности. Развитые страны мирового сообщества имеют специфичные законы, регламентирующие применение информационных технологий на своих территориях. Примерами могут служить Франция, в которой до последнего времени запрещалось применение программного обеспечения зарубежного производства в государственных организациях; отмененные весной 2001 года экспортные ограничения США на длину ключей в средствах криптографической защиты; Россия, с ее жестким государственным контролем за использованием шифровальных средств, собственными стандартами безопасности (РД ГТК), наличием ведомственных стандартов безопасности (например, в Министерстве атомной промышленности). Поэтому при разработке политики безопасности чрезвычайно важно учесть специфику законодательства страны, где осуществляет деятельность компания. Для этого необходимо привлекать юристов, Хорошо владеющих вопросами права в области информационных технологий, телекоммуникаций и информационной безопасности.

**Последствия в случае нарушений политики безопасности.** Этот раздел требует особого внимания. Зачастую, компании забывают четко проработать моменты, связанные с наступлением той или иной ответственности в случае нарушения политики безопасности. В связи с этим, злоумышленники могут остаться безнаказанными даже в случае их обнаружения и выявления и доказательства умышленности их злонамеренных действий. В зависимости от наступивших последствий и юридического статуса нарушителя, к нему могут быть применены дисциплинарные, административные или уголовные меры воздействия.

**Определение ответственности за обеспечение информационной безопасности** - это то, о чем необходимо всегда помнить и это то, что должно проходить единым стержнем через всю политику безопасности. Определение ответственности - это краеугольный камень политики безопасности и это то, что о чем так часто забывают при ее разработке.

По сложившейся практике, за все аспекты деятельности компании персональную ответственность несет руководитель. Очевидно, однако, что он не может лично обеспечивать информационную безопасность, поэтому без конкретизации, без точного определения кто именно и за что именно несет ответственность в компании, никакая, даже самая совершенная система защиты работать соответствующим образом не будет. Поэтому необходима детальная проработка вопросов, связанных с распределением обязанностей и разграничением ответственности.

### 1.1.2 Анализ и обновление

Информационная система любой компании не вечна. "Все течет, и все изменяется" - это полной мере применимо и здесь.

Крайне редко, только у небольших компаний можно встретить статичную неизменяемую информационную систему. Обычно же информационная система представляет собой круговорот постоянных изменений и нововведений, которые необходимо учитывать и отслеживать в политике безопасности. Именно поэтому так важно соблюдение требования периодического анализа и обновления политики безопасности.

### 1.1.3 Организационные меры по обеспечению безопасности

**Создание профильных форумов по информационной безопасности и управление ими.** Эта рекомендация стандарта предназначена, прежде всего, для крупных компаний, в которых процесс изменения информационных технологий является постоянным; в него вовлечено большое количество людей, поэтому так важно предусмотреть механизм, предоставляющий им возможность постоянного общения. Создание форума по информационной безопасности позволит обеспечить соответствующую координацию всего комплекса вопросов по обеспечению информационной безопасности и избежать проблем, связанных с недостаточной информированностью вовлеченных в процесс обеспечения

Разделы форума посвящены следующим вопросам:

1. обсуждение вносимых в политику изменений, принятие новой версии политики, согласование списков ответственных лиц;

2. отслеживание и анализ важных изменений в структуре информационных ресурсов компании на предмет выявления новых угроз;

3. изучение и анализ инцидентов с безопасностью;

4. принятие важных инициатив по усилению мер безопасности.

**Форум по координации вопросов, связанных с внедрением средств обеспечения информационной безопасности** должен содержать следующие пункты:

1. Выработка соглашений о разграничении ответственности за обеспечение информационной безопасности внутри организации.

2. Выработка специальных методик и политик, связанных с информационной безопасностью: анализ рисков, классификация систем и информации по уровням безопасности.

3. Поддержание в организации "атмосферы" информационной безопасности, в частности, регулярное информирование персонала по этим вопросам.

4. Обеспечение обязательности учета вопросов информационной безопасности при стратегическом и оперативном планировании.

5. Обеспечение обратной связи (оценка адекватности принимаемых мер безопасности в существующих системах) и координация внедрения средств обеспечения информационной безопасности в новые системы или сервисы.

6. Анализ инцидентов в области информационной безопасности, выработка рекомендаций.

**Распределение ответственности за обеспечение безопасности** происходит следующим образом:

- определение ресурсов, имеющих отношение к информационной безопасности, по каждой системе;
- для каждого ресурса (или процесса) должен быть назначен ответственный сотрудник из числа руководителей. Разграничение ответственности должно быть закреплено документально;
- для каждого ресурса должен быть определен и закреплен документально список прав доступа (матрица доступа).

**Процесс внедрения новой информационной системы.** Основные моменты:

1. Новая система должна соответствовать существующей политике управления пользователями, где указываются цели и задачи пользователей, а также в обязательном

порядке согласовываться с руководителем, ответственным за обеспечение безопасности данной системы.

2. Все внедряемые компоненты должны быть проверены на совместимость с существующими частями системы.

### 1.1.4 Классификация и управление ресурсами

**Инвентаризация ресурсов**. Данный пункт акцентирует внимание на необходимость проведения инвентаризации имеющихся в компании нормативных и инструктивных документов.

Ресурсы подразделяются на:

- Информационные ресурсы: базы данных и файлы данных, системная документация, пользовательская документация, учебные материалы, инструкции по эксплуатации или по поддержке, планы по поддержанию непрерывности бизнеса, мероприятия по устранению неисправностей, архивы информации или данных;
- Программные ресурсы: приложения, операционные системы и системное программное обеспечение, средства разработки;
- Физические ресурсы: вычислительная техника (процессоры, мониторы, переносные компьютеры), коммуникационное оборудование (маршрутизаторы, телефонные станции, факсы, автоответчики, модемы), магнитные носители (кассеты и диски), другое техническое оборудование (источники питания, кондиционеры);
- Вычислительные и коммуникационные сервисы, вспомогательные услуги: отопление, освещении и т.п.

**Классификация ресурсов.** Стандарт требует классифицировать все ресурсы компании с точки зрения безопасности. Зачастую, часть, казалось бы, малозначительных ресурсов выпадает из поля зрения специалистов компании, что совершенно недопустимо - в безопасности не бывает мелочей. Например, наличие персональных модемов и потенциальная возможность их использования является одним из распространенных каналов утечки информации и требует особого контроля - такой ресурс обязан быть классифицирован как ресурс повышенной опасности, требующий специального разрешения на его применение.

Все ресурсы должны быть классифицированы по степени важности.

Для каждого класса должны быть регламентированы следующие действия:

1. копирование;

2. хранение;
3. передача почтой, факсом, электронной почтой;
4. передача голосом, включая мобильные телефоны, голосовую почту;
5. уничтожение.

### 1.2 Безопасность персонала

#### 1.2.1 Безопасность при выборе персонала и работе с ним

**Необходимо включить задачу обеспечения безопасность в должностные обязанности сотрудников.** Задача обеспечения информационной безопасности должна решаться на всех уровнях в компании - от высшего руководства до рядового сотрудника. Поэтому включение в должностные обязанности каждого сотрудника задач по обеспечению информационной безопасности является одним из важных факторов, влияющих на безопасность компании в целом. Также не менее важно обеспечить на практике (а не на словах) строгое выполнение всеми сотрудниками своих обязанностей по отношению к безопасности информации: халатное отношение к этим вопросам (так называемый человеческий фактор) может свести на нет все вложения в эту область и обречь на неудачу все попытки обеспечить безопасность компании. Классический пример, когда пользователь из-за халатного отношения к своим должностным обязанностям оставляет персональный пароль на листочке, приклеенном на экран монитора, до сих пор встречается на практике (правда, уже реже). Учет человеческого фактора - это ключ к надежной защите информационных ресурсов.

**Проверка персонала при приеме на работу**. Часто ли вы сталкивались с практикой комплексной проверки компанией персонала при приеме на работу? Наверняка нет. Обычно компании делегируют функции проверки персонала рекрутинговым компаниям и это не всегда может быть обосновано, поэтому данный пункт вынесен в отдельный подраздел стандарта. Необходима самостоятельная комплексная проверка силами отдела безопасности компании личности принимаемого на работу, его рекомендаций, указанных в резюме сведений и т.д. Важно соблюдать такую процедуру комплексной проверки не только для сотрудников, которые будут работать напрямую с секретной или конфиденциальной информацией (такие сотрудники обычно тщательно проверяются), но и для персонала, который может косвенно (или случайно) иметь дело с критичной для компании информацией.

Иногда при приеме персонала на особо важную должность, связанную с работой с секретной информацией, рекомендуется будущему сотруднику предложить пройти добровольный психологический тест на детекторе лжи.

**Заключение соглашений о соблюдении режима информационной безопасности со всеми сотрудниками.** При приеме на работу необходимо подписать специальное соглашение о конфиденциальности, запрещающее сотруднику разглашать информацию, начиная с определенного уровня (грифа) секретности. В подобном юридически проработанном соглашении, необходимо учесть степень ответственности за его невыполнение сотрудником компании, а также период действия соглашения, в том числе и после увольнения сотрудника.

**Условия работы персонала**. В соответствии со стандартом, при приеме на работу новых сотрудников необходимо, чтобы они ознакомились и подписали:

- письменную формулировку их должностных обязанностей;
- письменную формулировку прав доступа к ресурсам компании (в том числе и информационным);
- соглашение о конфиденциальности;
- специальные соглашения о перлюстрации всех видов служебной корреспонденции (мониторинг сетевых данных, телефонных переговоров, факсов и т.д.).

Пример такого соглашения компании с персоналом:

Вся информация, находящаяся на электронных носителях рабочих станций и в вычислительных сетях компании, является собственностью компании.

Подразделения и лица, уполномоченные на то руководством компании имеют право в установленном порядке, без уведомления пользователей, производить проверки соблюдения требований настоящей Инструкции, а также осуществлять контроль за данными, находящимися на электронных носителях. В целях осуществления указанных действий они могут получить доступ к любым данным пользователей, находящихся на электронных носителях рабочих станций и в сети, а пользователь обязан предоставить требуемую ими информацию.

Компания имеет право без согласия пользователя передавать информацию, хранящуюся на электронных носителях, третьим лицам, включая правоохранительные органы и иные организации, уполномоченные на это действующим законодательством.

Любые компоненты корпоративной сети могут использоваться пользователями только для выполнения своих служебных обязанностей.

Использование компонентов сети не по назначению, использование, нарушающее требования настоящей Инструкции, приказов и распоряжений руководства компании

(Директора, Технического Директора, руководителей подразделений), а также использование, которое наносит вред компании, в зависимости от тяжести наступивших последствий может повлечь за собой дисциплинарную (включая увольнение), административную или уголовную ответственность.

### 1.2.2 Тренинги пользователей

Понимая и особо выделяя важность человеческого фактора для обеспечения надежной защиты информационной системы компании, стандарт ISO 17799 подчеркивает необходимость наладить постоянный процесс повышения уровня технической грамотности и информированности пользователей в области информационной безопасности. Для этого необходимо регулярное проведение тренингов, посвященных общим правилам информационной защиты. Этим будет достигнуто постоянное напоминание пользователям основных правил и требований компании по обеспечению информационной безопасности. Особенно важно проводить подобные тренинги для вновь поступившего на работу персонала и в случае внесения в информационную систему каких-либо изменений (принятие новых технологий, прикладных автоматизированных систем, смены оборудования, ОС, ключевых приложений, принятие новых правил или инструкций и т.д.)

### 1.2.3 Реагирование на инциденты в области безопасности, а также сбои и неисправности

Обеспечение соответствующей адекватной реакции сотрудников при возникновении инцидентов с безопасностью и неисправностей в информационной системе является на сегодняшний день неотъемлемым требованием к политике безопасности компании. Необходимо разработать однозначно интерпретируемый порядок действий в случае критических ситуаций. Периодические тесты и проверки действий персонала при имитации возникновения критических ситуаций также рекомендованы данным стандартом.

Необходимы:

1. Отчеты об инцидентах.
2. Отчеты о недостатках в системе безопасности.
3. Отчеты о сбоях и неисправностях компьютерных систем.
4. Изучение инцидента.

В случае обнаружения нестандартной ситуации необходимо:

- записать все симптомы ее появления;

- компьютер должен быть изолирован и если возможно его использование приостановлено;
- о факте должно быть немедленно сообщено непосредственному руководителю и службе информационной безопасности, они же должны быть проинформированы о результатах анализа причин произошедшего.

Запрещается предпринимать самостоятельные меры без разрешения уполномоченных лиц.

5. Дисциплинарные меры (в российской специфике это, в зависимости от последствий: дисциплинарные, административные или даже уголовные). Обязательным требованием стандарта является необходимость предусмотреть дисциплинарные и другие меры ответственности в случае нарушения персоналом компании требований по обеспечению информационной безопасности, повлекшего вредные последствия. В некоторых случаях можно не предусматривать особых дисциплинарных мер и руководствоваться только гражданским или административным правом страны, в которой действует данная компания. Однако, в случаях, когда возможные действия персонала не предусматривают нарушение законодательства страны, но при этом нарушают собственные интересы компании или если законы страны не предусматривают достаточной ответственности при нарушениях в области информационных технологий, то требуется руководствоваться корпоративными нормативными актами, в которых продуманны и юридически обоснованы соответствующие меры воздействия на нарушителей.

6. Регулярное обучение персонала по вопросам безопасности.

### 1.2.4 Физическая безопасность

**Безопасность оборудования.** Оборудование должно располагаться с учетом минимизации доступа в рабочее помещение лиц, не связанных с обслуживанием этого оборудования. Расположение систем обработки и хранения информации, содержащих важные данные, для минимизации возможности случайно или специально увидеть данные в процессе их обработки, должны согласовываться с требованиями о безопасности помещений.

Политика компании должна содержать категорический запрет на прием пиши, напитков и курение вблизи оборудования. К сожалению, зачастую этот аспект совершенно выпускается из виду, в то время как последствия, например, пролитого на сервер кофе могут стать по истине катастрофическими, даже при наличии резервных копий информации. Не многие знают, во что превращаются вентиляторы блоков питания при регулярном курении в технологических помещениях. Выход оборудования из строя в результате перегрева

приводит не только к потере информации, но и к прямому материальному ущербу вследствие пожара.

Необходимость постоянного мониторинга оборудования для раннего обнаружения признаков, которые могут повлечь за собой отказ системы является очевидным требованием - видео наблюдение, постоянный контроль за пожарными датчиками позволят вовремя обнаружить возможную неисправность.

На требование использования специальных методов защиты оборудования, например, накладка на клавиатуру, необходимо обратить внимание менеджерам по информационным технологиям промышленных предприятий, в случае расположения оборудования в промышленных зонах. Подобные специальные средства защиты помогут защитить оборудование от неизбежного повышенного уровня загрязненности в таких помещениях.

Меры защиты должны быть приняты для минимизации следующих потенциальных угроз:

- кража;
- огонь;
- взрыв;
- дым;
- вода;
- пыль;
- вибрация;
- химические вещества;
- побочные электромагнитные излучения и наводки.

Требование предусмотреть возможные воздействия от происшествий на соседних объектах позволит заранее оценить возможный ущерб и спланировать контр аварийные мероприятия.

### 1.2.5 Безопасность кабельной системы

1. Силовые и телекоммуникационные линии в информационно обрабатывающую систему должны проходить под землей (если возможно). В противном случае, им требуется адекватная альтернативная защита.

2. Сетевые кабели должны быть защищены от несанкционированного подключения или повреждения. Этого можно достигнуть при помощи их прокладки вне общедоступных зон.

3. С целью снижения влияния электромагнитных помех, силовые кабели должны быть разделены с коммуникационными.

4. Для важных или особо важных систем должно быть предусмотрены следующие меры защиты:

- линии связи должны быть закрыты защитными коробами, кроссовые помещения и шкафы должны надежно запираться и опечатываться; контроль целостности должен осуществляться регулярно;
- линии связи должны быть продублированы;
- применение оптического кабеля;
- обнаружение несанкционированных подключений к линиям связи и оповещение персонала.

### 1.2.6 Безопасное уничтожение отработавшего оборудования

Безопасное уничтожение отработавшего оборудования является достаточно незаметным пунктом любой политики безопасности, но чрезвычайно важным. Не стоит недооценивать проблемы, которые возникают при отсутствии должного внимания вопросам безопасного уничтожения оборудования и остаточных данных на любом носителе. В книге "Хакеры" (Дж. Маркофф, К.Хефнер) описана технология, при помощи которой Кевин Митник добывал пароли и другую ценную информацию об интересующей его системе - он тщательно изучал выбрасываемые на помойку ненужные распечатки и другие "отходы производства".

Поэтому жесткий контроль за дальнейшей судьбой всего списываемого оборудования является просто необходимым условием любой политики безопасности. Особенно стоит обратить внимание на требование обязательного уничтожения (или безопасной перезаписи информации) устройств хранения информации, содержащих ценную информацию.

Устройства хранения информации, содержащие ценную информацию, при выведении из эксплуатации должны быть физически уничтожены, либо должно быть проведено гарантированное стирание с них остаточной информации.

Все оборудование, включая носители информации, перед передачей его другому владельцу (или списанием) должно быть проверено на предмет отсутствия в нем важной информации или лицензионного программного обеспечения.

Дальнейшая судьба поврежденных устройств хранения, содержащих важную информацию, (уничтожение или ремонт) определяется на основе заключения экспертной комиссии.

*1.2.7 Безопасность рабочего места*

1. Документы на всех видах носителей и вычислительная техника, в случае если ими не пользуются, а также в нерабочее время, должны храниться в запираемом помещении.

Требование хранения документов, важной бизнес информация в нерабочее время или в случае отсутствия их владельца в безопасном месте выглядит достаточно логичным, однако на практике выполняется редко - часто можно увидеть на столах персонала разных компаний всевозможные документы, в том числе и достаточно конфиденциальные. Кроме обеспечения сотрудников хранилищами (сейфами, металлическими шкафами, индивидуально запираемыми ячейками в общем хранилище и т.п.) могут применяться самые разные методы, вплоть до использования специальных наклонных столов, не позволяющих случайно забыть на них документ.

2. Ценная информация, когда она не используется, должна храниться в защищенном месте (огнеупорный сейф, выделенное помещение)

3. Персональные компьютеры, терминалы и принтеры не должны оставаться без присмотра во время обработки информации и должны защищаться блокираторами клавиатуры, паролями или иными методами на время отсутствия пользователя.

Не меньшую угрозу представляет и доступ к оставленной без присмотра электронной информации. Очень часто пользователи отлучаются со своего места, оставив компьютер или терминал с запущенными задачами (либо просто прошедший авторизацию в системе) без блокировки устройств ввода-вывода. В связи с этим в системе должна быть предусмотрена автоматическая блокировка (либо завершение сессии) по истечении определенного времени неактивности пользователя.

4. Должны быть приняты надежные меры, исключающие несанкционированное использование копировальной техники в нерабочее время.

5. Распечатки, содержащие ценную (конфиденциальную) информацию должны изыматься из печатающего устройства немедленно.

Своевременное изъятие распечаток из устройств вывода (принтеров, плоттеров и т.п.) также имеет важное значение. Распространенная практика печати конфиденциальной информации на удаленный принтер категорически не допустима - распечатка может быть ошибочно отправлена не на то устройство или изъята из выходного лотка другими лицами. Более того, зачастую руководитель поручает кому-либо из подчиненных доставить ему напечатанный документ, в результате чего происходит дополнительное распространение конфиденциальной информации.

Специалистам, разрабатывающим схему информационных потоков при удаленной печати, необходимо учитывать возможность возникновения такой ситуации и принять меры, по ее предотвращению

### 1.3. Управление коммуникациями и процессами

#### 1.3.1 Служебные инструкции и ответственность

Обратим внимание на требование определения (если это возможно) временного интервала работы системы. Атаки часто осуществляются в необычное время (нерабочее, например). Потому определение временного интервала легитимного функционирования системы может помочь выявить нарушителя.

Разработка инструкций, определяющих порядок действий в случае возникновения ошибок и других исключительных ситуаций, является одной из важных частей плана на случай нештатных обстоятельств. Персонал должен знать, как ему необходимо действовать в случае той или иной ситуации. Безусловно, все возможные типы исключительных ситуаций нельзя заранее учесть и продумать, но действия в случае основных возможных нештатных ситуациях должны быть продуманы, смоделированы и протестированы на практике.

Необходимо создание специальных инструкций, требований и схем обращения с конфиденциальными выходными данными. Примером последствий невнимания к важности регламентации обращения с конфиденциальными выходными данными служит взлом в 2000 году принтера в Пентагоне и перенаправление очереди на печать на один из адресов в России. Другим распространенным примером является печать конфиденциальных документов на удаленный общедоступный принтер в пределах компании.

Должностные инструкции должны включать:

- порядок обработки и обращения с информацией;
- порядок взаимодействия с другими системами, разрешенные часы доступа на рабочее место (в ночное время, в выходные);
- порядок действий в нештатных ситуациях;
- список лиц и способы связи с ними в нештатных ситуациях;
- специальные инструкции по обращению с результатами обработки информации, в том числе конфиденциальными и ошибочно обработанными;
- рестарт системы и восстановительные процедуры, необходимые в случае сбоя системы.

### 1.3.2 Контроль изменений в операционной среде (среды функционирования)

Под операционной средой в стандарте понимается рабочая среда, в которой непосредственно запущены бизнес процессы. То есть, операционная среда - это совокупность средств вычислительной техники и функционирующих на них процессов, непосредственно решающих и выполняющих бизнес задачи. Соответственно, именно операционная среда, являющаяся сердцем бизнеса компании - здесь зарабатываются деньги - требует особого внимания и контроля. Поэтому, в том случае, если копания планирует внесение каких-либо изменений в операционную среду, то в ее интересах реализовать рекомендуемый стандартом контроль изменений в операционной среде.

Основные требования:

- идентификация и запись важных изменений;
- оценка последствий таких изменений;
- формальное утверждение процедуры внесения изменений;
- взаимодействие со всеми заинтересованными лицами при внесении изменений;
- процедуры определения ответственности и возврата в исходное состояние при неудачных попытках изменений.

В перечисленных требованиях установления четкого контроля над особо важными изменениями сложно выделить какой-либо пункт - здесь важно обратить внимание на весь раздел в целом. Прежде всего, при внесении изменений выделить, идентифицировать и оценить предполагаемые особо важные изменения. Затем необходимо провести предварительную оценку потенциального воздействия таких изменений на рабочую информационную среду компании: как наиболее безболезненно внедрить эти изменения, как это сделать, по возможности, не влияя на производственный процесс и т.п. Затем необходимо получение формального одобрения у руководства процедуры предлагаемых изменений.

После внесения изменений необходимо наладить взаимодействие между всеми значимыми персонами, вовлеченными в процесс, для контроля корректности вносимых изменений. Также необходимо заранее предусмотреть процедуры отмены и восстановления системы (процедуры отката) при неудачных изменениях и заранее назначить ответственных за данный процесс лиц.

### *1.3.3 Процедуры реагирования на инциденты*

Важность процедур контроля и анализа инцидентов не вызывает сомнений. Любая компания, которая заботится о собственной безопасности, должна иметь заранее разработанную и протестированную методику, позволяющую выявить причины, из-за которых произошел инцидент, провести анализ и сохранение доказательств, следов инцидента, улик и свидетельств, а также определить порядок взаимодействия между лицами, пострадавшими из-за инцидента или вовлеченными в восстановительный процесс. При этом важно обратить внимание, что все аварийные действия обязательно должны быть детально задокументированы и о них должно быть доложено ответственным лицам.

Предварительная подготовка подобной методики, ее тестирование и обучение персонала действиям в условиях нештатных ситуаций и инцидентов позволит компании повысить общий уровень защищенности и обеспечить соответствующие условия для непрерывного ведения бизнеса - что является важнейшей частью любой политики безопасности. Особо отметим, чрезвычайно важно помнить и все время подчеркивать, что безопасность это не только нейтрализация угроз, это и обеспечение непрерывности бизнеса. К сожалению, этот момент выпадает из поля зрения высшего руководства и поэтому безопасность, зачастую, воспринимается исключительно как расходная статья бюджета. Хотя в критической ситуации все сразу вспоминают про безопасность и про непрерывность остановившегося вдруг бизнеса, но вспоминают слишком поздно - беспечность и непонимание руководством этих вопросов могут привести к серьезным убыткам.

1. Процедуры реагирования на инциденты должны предусматривать все возможные ситуации, включая:

- сбои в информационных системах;
- отказ в обслуживании;
- ошибки из-за неполных или неправильных входных данных

утечку информации.

2. В дополнении к оперативному плану восстановления процедуры должны также включать:

- анализ и определение причин инцидента;
- планирование и внедрение мер для предотвращения повторения (если необходимо);
- анализ и сохранение сведений об инциденте, которые можно представить в качестве доказательства (улики, свидетельства и т.п.);
- определение порядка взаимодействия между пострадавшими от инцидента и участниками процесса восстановления;
- обязательное информирование ответственных лиц.

3. По каждому инциденту должно быть собрано максимальное количество информации, которой также необходимо обеспечить необходимый уровень защиты для:

- последующего анализа внутренних проблем;
- использования собранных данных для привлечения виновных к дисциплинарной, административной или уголовной ответственности;
- использования при ведении переговоров о компенсациях с поставщиками аппаратного и программного обеспечения.

4. Действия по восстановлению после обнаружения уязвимостей в системе безопасности, исправлению ошибок и ликвидации неисправностей должны быть внимательно и формально запротоколированы. Процедура должна гарантировать что:

- только персонал, прошедший процедуры идентификации и аутентификации может получать доступ к "ожившим" системам и данным;
- все действия по выходу из нештатной ситуации зафиксированы в виде документа для последующего использования;
- обо всех произведенных действиях руководство было проинформировано в установленном порядке;
- целостность и работоспособность системы подтверждена в минимальные сроки.

### *1.3.4 Разграничение ответственности путем разделения обязанностей*

Классический метод, который называется "разделение обязанностей" (Segregation of Duties) всегда широко использовался человечеством на всем протяжении его существования. Этот же метод, уменьшающий риск от случайного или запланированного злоупотребления системой, сегодня активно применяется практиками для обеспечения информационной безопасности и рекомендуется данным стандартом. Это, в общем, не удивительно, так как стандарт безопасности информационных систем ISO 17799 действительно является по своей сути обобщением многолетнего опыта практической и теоретической работы огромной армии экспертов по информационной безопасности со всего мира.

Как подчеркивает стандарт, разделение зон ответственности между руководителями позволяет уменьшить возможность неавторизованной модификации или злоупотребления информацией и сервисами, что, в общем, очевидно.

Применение данного метода на практике сделает практически невозможным совершить в одиночку обман без возможности его обнаружения. Для этого стандарт рекомендует разделять действия, которые могут подразумевать сговор, а также вовлекать в любую

критичную процедуру две или более персоны для дополнительных гарантий исключения злоупотреблений. Это так называемый принцип "4 глаз".

Необходимо учесть следующие моменты:

- действия, которые могут подразумевать сговор (например, покупка товара и контроль закупленного товара), должны быть обязательно разделены;
- если есть опасность сговора, то тогда необходимо применение принципа "4 глаз".

Практическим применением данного правила является следующий пример из жизни. Как известно, во многих операционных системах существует суперпользователь, который имеет абсолютные привилегии в системе и, при желании, может выполнять любые (в том числе и несанкционированные) действия и при этом остаться незамеченным (например, изменить регистрационные журналы или удалить их). Такая ситуация, безусловно, является неприемлемой, но, к сожалению, это реальность. Да, существуют системы, в которых есть возможность ограничить права суперпользователя, но в стандартных системах такой возможности обычно не предусмотрено. Чтобы избежать подобной ситуации рекомендуется разделить пароль суперпользователя на две равные части (например, одну дать администратору безопасности, а вторую - администратору сети), что не позволит одному из них в одиночку работать в системе с наивысшими полномочиями: войти в систему с такими правами они смогут только вместе. Не правда ли это сильно напоминает два ключа, которые надо повернуть двум разным людям одновременно, для того чтобы открыть сейф банка, например. Очевидно, что свои половинки паролей они обязаны хранить в секрете друг от друга, однако это может оказаться затруднительным как с организационной точки зрения (оба должны оперативно прибыть к консоли), так и с технической (например, при смене пароля на режим enable в программном обеспечении CISCO, он отображается на экране).

### *1.3.5 Разделение ресурсов*

Говоря об этом требовании стандарта, уместно привести в пример с секретным заводом, каждый этаж которого, во-первых, строго изолирован от других этажей, и, во-вторых, имеет свой уровень секретности. Соответственно сотрудники имеют доступ строго к определенному этажу в соответствии со своим уровнем допуска. Перенося этот пример на данное требование стандарта о разделении сред, логично отметить, что информационную систему компании можно также воспринимать, как и секретный завод и делить ее на соответствующие зоны секретности. Правда, стандарт не выделяет отдельно зоны в соответствии с уровнем секретности, но подразумевает это - пример подобной архитектуры безопасности приведен в последнем разделе.

Итак, с технологической точки зрения стандарт предлагает разделить все информационные ресурсы на следующие среды:

- перспективная разработка;
- тестирование (карантин);
- непосредственное осуществление бизнес операций (операционная среда).

Это требование является, безусловно, логичным, так как, прежде всего, необходимо отделить операционную среду от остальных технологических сред, дабы не помешать производственному процессу.

Чрезвычайно важно определить правила переноса программного обеспечения из отдела разработки в отдел эксплуатации, чтобы вновь разработанное программное обеспечение попало в операционный среду только после надлежащего тестирования и комплексных проверок.

Разделение операционной среды и среды разработки должно быть очень четким. Лучше, если они будут функционировать на разном оборудовании или, хотя бы, в разных доменах и каталогах. Аналогичные требования должны предъявляться и к разделению сред перспективной разработки и тестовой.

Требования ограничение доступа (особенно из операционной среды) к компиляторам, системные редакторам и другим системным средствам выглядят весьма логично и, как правило, реализуются в защищенных ОС.

Обратим также внимание на рекомендацию применения разных систем входа для тестовых и операционных сред, выставляемую для уменьшения риска случайной ошибки. Пользователи должны иметь разные пароли для входа в такие системы и меню должно иметь соответствующее предупреждение.

Во избежание случайного или преднамеренного внесения несанкционированных изменений в операционную среду, необходимо ограничить и контролировать доступ к ней разработчиков. По меньшей мере, в этом случае стандарт рекомендует применять временные пароли.

### 1.3.6 Защита от вредоносного программного обеспечения (вирусов, троянских коней)

Вирусы, черви, троянцы являются настоящим бичом современного информационного сообщества. По некоторым прогнозам к концу 2010 года более 50% электронной почты будет заражено вирусами и электронная почта умрет в нынешнем виде - ей перестанут пользоваться. Мы не разделяем в полной мере данного прогноза, но, очевидно, что на

сегодняшний день компании необходимо иметь четкую политику относительно вирусов и иного вредоносного программного обеспечения.

Для защиты от вредоносного программного обеспечения должны быть приняты следующие меры:

- обязательность применения только лицензионного программного обеспечения и запрет использования неутвержденного программного обеспечения должны быть закреплены документально;
- с целью снижения рисков, связанных с получением программного обеспечения через сети общего пользования или на носителях, этот процесс должен быть формализован в виде соответствующего документа;
- все системы должны быть снабжены антивирусным программным обеспечением, которое должно своевременно обновляться. Сканирование всех систем должно проводиться регулярно;
- целостность программного обеспечения, занимающегося обработкой критичных данных (и самих данных) должна проверяться регулярно. По факту отклонения от эталонных значений должно проводиться служебное расследование;
- все точки, через которые в систему поступает информация в виде файлов, сообщений и т.п. должны обеспечивать антивирусный контроль входящей информации;
- в организации должен быть разработан и задокументирован механизм восстановления после вирусных атак, в частности, определены процедуры резервного копирования программного обеспечения и данных;
- мониторинг всей информации, касающейся вредоносного программного обеспечения, в частности, анализ всех публикуемых бюллетеней и предупреждений по этой теме.

### 1.3.7 Управление внутренними ресурсами

✓ *Резервное копирование информации*

Не стоит в очередной раз говорить о важности резервного копирования - это и так совершенно очевидно. Отметим здесь следующие требования стандарта, касающиеся данной процедуры:

- Резервные копии вместе с инструкциями по восстановлению должны храниться в месте, территориально отдаленном от основной копии информации. Для особо важной информации необходимо сохранять три последних копии.

- К резервным копиям должен быть применен адекватный ряд физических и организационных мер защиты, соответствующий стандартам, принятым для используемых носителей.
- Носители, на которые осуществляется резервное копирование, должны регулярно проверяться на отсутствие сбоев.
- Регулярная проверка процедур восстановления и практический тренинг персонала с целью поддержания возможности восстановления данных в установленном порядке и за гарантированный промежуток времени.

✓ *Регистрация действий операторов*

Обеспечение протоколирования действий операторов в случае ошибок является неотъемлемым условием политики безопасности. Особо стоит обратить внимание на следующие трудно реализуемые на практике требования записи в файл журнала системных ошибок и действий по их коррекции (проблема в том, что действия по коррекции часто трудно поддаются автоматическому протоколированию, поэтому здесь возможно применение протоколирования действий в ручную) и требования подтверждения корректного обращения с входными и выходными данными (речь идет о прикладных системах, а не о ОС).

Обязательной регистрации в системных журналах регистрации должны подвергаться:

- время старта и остановки системы;
- системные ошибки и действия по их исправлению;
- подтверждение корректного обращения с входными и выходными данными;
- идентификатор оператора, совершившего действие, которое повлекло запись в журнал регистрации.

✓ *Регистрация системных сбоев*

В случае восстановления системы после ее выхода из строя, рекомендуется проводить анализ существующего журнала системных сбоев для гарантии того, что сбои были удовлетворительно устранены и действия по восстановлению были авторизованы и проводились в установленном порядке.

Ведение журнала системных сбоев позволит сделать:

- анализ журнала системных сбоев на предмет корректности и завершенности процесса устранения последствий сбоев;

- анализ произведенных действий на предмет соответствия установленным процедурам.

### *1.3.8 Управление сетью*

Удаленное управление оборудованием, операционными системами и приложениями является чрезвычайно удобным средством. Но, согласно аксиоме безопасности, чем более система функциональна, тем она менее безопасна. Поэтому, предусматривая в системе удаленное управление информационными ресурсами, необходимо серьезно продумать возникающие при этом вопросы безопасности. Во-первых, необходимо четко разделить какие средства могут администрироваться только локально, а какие локально и удаленно. Во-вторых, необходимо продумать и реализовать рабочие процедуры удаленного (сетевого) управления, включая ответственность персонала за корректное выполнение каждой процедуры.

Ответственность персонала за осуществление сетевых и локальных операций должна быть разделена. Должна быть определена ответственность и установлены процедуры управления удаленным оборудованием, включая оборудование в сегментах пользователей. При передаче информации через сети общего пользования должны применяться специальные средства обеспечения целостности и конфиденциальности. Для обеспечения работоспособности сетевых компьютеров должны быть разработаны специальные процедуры.

### *1.3.9 Безопасность носителей данных*

#### ✓ *Управление съемными носителями*

Помните аксиому - в безопасности мелочей не бывает. И это действительно так, хотя, исходя из практического опыта, в компаниях эту аксиому часто забывают. Применяя эту аксиому к данному требованию стандарта, напомним, что безопасность съемных носителей является важной частью безопасности компании в целом. Возьмем для примера дискеты и компакт-диски как наиболее типичные представители армии съемных носителей. Ни для кого не секрет как часто можно в компаниях наблюдать разбросанные по всем рабочим местам дискеты, компакт-диски и т.д.. А ведь на них может находиться самая различная информация, включая конфиденциальную. И не стоит думать, что если вы обеспечили должный уровень защиты серверов и рабочих станций ( первичных носителей информации), то не стоит на том же уровне защищать и вторичные носители - то есть, съемные носители.

Поэтому в компаниях должны руководствоваться теми же требованиями к безопасности съемных носителей, которые предъявляются и к безопасности основных носителей.

В том случае, если требуется вынести съемный носитель за пределы территории компании, то необходимо получение разрешения на вынос и записи о таком выносе должны быть сохранены в соответствующей базе (журнале).

Помимо этого, необходимо, чтобы все носители, сроки годности которых прошли, были уничтожены в установленном порядке. Вполне резонным является и требование хранения носителей в безопасном месте, в соответствии с рекомендациями компании производителя. Все носители, срок эксплуатации которых истек, должны быть уничтожены в установленном порядке.

- ✓ **Хранение и обращение с носителями**

Данный пункт стандарта дополняет и уточняет предыдущий пункт, указывая, какая именно информация и носители требуют безопасного хранения и обращения, а также способы достижения этой цели.

Обратим внимание на безопасность хранения такого анахронизма как копировальная бумага - не будем забывать, что кое-где она до сих пор используется, и на ней остаются копии документов.

Следует обратить особое внимание на требование безопасного хранения листингов программ и системной документации - потеря контроля над информационной системой и ее управляемости может привести к самым тяжелым последствиям.

Листинги программ, помимо того, что сами из себя могут представлять коммерческую тайну также могут являться и источником информации, по которой можно проще вычислить уязвимость в программе для ее последующего использования. Поэтому требование ограничения доступа к ним является очевидным.

Требование безопасности системной документации еще раз встречается в данном стандарте, когда речь идет о том, что пользователям необходимо предоставлять информацию, в том числе и о функциональных возможностях системы, только в необходимых пределах. В данном случае в очередной раз стандартом подчеркивается важность служебной документации (что, зачастую, забывается) и необходимость ее безопасного хранения.

Основные положения:

1. Хранение в безопасном месте.
2. Следующие носители и информация требуют повышенной безопасности при хранении:

- бумажные документы;
- записи на кассетах;
- копировальная бумага;
- отчеты;
- картриджи;
- магнитные ленты;
- съемные диски или кассеты;
- оптические носители;
- листинги программ;
- тестовые данные;
- системная документация.

3. Процедуры обращения с информацией и ее хранения.

Анализируя данное требование стандарта, остановимся на следующих его требованиях. Продолжая предыдущие пункты, необходимо обеспечить учет и маркировку всех носителей. Кроме того, требуется обеспечить официальные записи об авторизованных получателях данных. То есть кому разрешено получать какие данные и кто и когда их получил или сдал - за этим требуется вводить контроль в случае, когда речь идет о информации уровня "конфиденциально" и выше.

Еще раз обратим внимание на требование защиты данных из спулинга (которые ожидают распечатки, например), т.к. очень часто ее отсутствие создаетодин из самых серьезных каналов утечки.

### 1.3.10 Безопасность при передаче информации и программного обеспечения

✓ **Соглашения о передаче**

Обмен и передача информации в компании является потенциальным каналом утечки информации. Поэтому требования стандарта, касающиеся передачи информации, нуждаются в особом внимании.

Прежде всего, необходимо определить ответственных за процессы передачи и приема информации и закрепить обязанности документально. Здесь еще раз напомним, как важно заранее предусмотреть и разделить ответственность при выполнении каждого критического с точки зрения безопасности действия. Требование создания корректных и четких процедур для уведомления отправителя, получателя, и процедуры приема-отправки позволят избежать многочисленных проблем в этой области. Обратим внимание на необходимость

идентификации способа доставки - в случае передачи критичной информации это стоит иметь в виду.

И последнее в данном разделе требование, о котором хотелось бы упомянуть: необходимо заранее предусмотреть возможные коллизии при передаче данных и продумать ответственность за потерю или задержку данных.

### ✓ Безопасность электронной коммерции при обмене информацией

Электронная коммерция на сегодняшний день вошла в нашу жизнь. Однако, существует ряд проблемам с безопасностью электронной коммерции.

1. Аутентификация. Какой уровень конфиденциальности должны иметь покупатели и продавцы для идентификации друг друга.
2. Авторизация. Кто выпустил прайсы и подписаны ли они? Как контрагенты могут это узнать?
3. Контракт и тендер. Какие требования для конфиденциальности, целостности, доказательства отправки и приема ключевых документов и отказа от контракта.
4. Ценовая информация. Какой уровень доверия может быть применен для целостности рекламного прайс листа и конфиденциальности для скидок.
5. Порядок расчетов. Как обеспечивается конфиденциальность и целостность расчетов, платежей, адресатов и подтверждение приема-отправки.
6. Подтверждение факта оплаты. Какова степень проверки платежной информации посланной покупателем

Все эти проблемы можно надежно решить только с применением современных стойких криптографических методов защиты информации.

### ✓ *Безопасность электронной почты*

Электронная почта сегодня практически заменила почту обычную. Ее легкость и удобство использования не вызывает сомнения у пользователей. Сегодня сложно представить компанию, сотрудники которой не пользовались бы электронной почтой. Однако, эта сервисная функция требует дополнительной регламентации и нуждается в специально разработанной политике, содержащей требования, правила и инструкции по использованию электронной почты. Обратим внимание на требование стандарта о наличии

инструкции, регламентирующей правила использования электронной почты. Некоторым сотрудникам в соответствии с должностными обязанностями или в связи с особым уровнем секретности должно быть запрещено пользоваться данным сервисом.

Необходимо предусмотреть ответственность сотрудников за нанесение вреда компании (компрометация имиджа, разглашение коммерческой тайны) в результате использования электронной почты.

Обратим также внимание на требование архивирования сообщений электронной почты, которые могут в последствии быть предъявлены в качестве доказательств в суде.

При разработке политик необходимо учитывать следующие моменты:

1. Возможные атаки на электронную почту (например: вирусы, перехват, уничтожение, искажение).
2. Защита вложений.
3. Порядок допуска персонала к использованию электронной почты.
4. Определение ответственности сотрудников за нанесение вреда компании (компрометация имиджа, разглашение коммерческой тайны) в результате использования электронной почты.
5. Порядок использование криптографии для защиты электронных сообщений.
6. Архивирование сообщений электронной почты, которые могут в последствии быть предъявлены в качестве доказательств в суде.
7. Регламентация правил проверки сообщений, которые не могут быть однозначно аутентифицированы.

- ✓ *Безопасность электронного офиса*

Данное требование стандарта рассматривает безопасность электронного офиса в целом, потому в основном здесь повторяются уже известные общие требования.

Стандарт требует учесть все возможные уязвимости информации в офисной системе, например, запись телефонных разговоров, конфиденциальность звонков, сохранение факсов, несанкционированный доступ к сообщениям электронной почты и т.д. - все эти уязвимости присутствуют в офисной системе, и требуется разработка соответствующей политики и мер по устранению данных уязвимостей.

В том случае, если система не соответствует необходимому уровню безопасности, то из нее исключаются категории секретной бизнес информации. То есть, требуется классифицировать все системы компании в соответствии с уровнем секретности обрабатываемой в них информации.

Также в офисной системе требуется ввести ограничение доступа к информации, связанной с выбором персонала (пример, персонал, работающий на засекреченные проекты). Необходимо чтобы к данной информации имел доступ строго ограниченный список лиц.

При необходимости требуется ввести ограничение на доступ к ресурсам для специальных категорий пользователей. Необходимо так же предусмотреть идентификацию статуса пользователей, резервное копирование информации, планы восстановления после сбойных ситуаций.

✓ *Безопасность других форм информационного обмена*

Компании должны рассматривать процесс обеспечения информационной безопасности в комплексе. При этом необходимо учитывать все угрозы и потенциальные каналы утечки информации. Стандарт требует учета при создании политики безопасности, угроз, связанных с передачей информации голосом, факсом и видео.

Необходимо постоянно напоминать персоналу и требовать от него соблюдения следующих элементарных мер предосторожности при телефонных звонках:

- не вести конфиденциальные разговоры по незащищенным телефонным линиям;
- учитывать близость посторонних людей при звонках и, соответственно, возможность послушать разговор;
- перехват звонков при физическом доступе к линии.

Не менее важными являются требования для персонала не проводить конфиденциальные переговоры в общественных местах, открытых офисах или офисах с тонкими стенами, так как такие разговоры могут быть прослушаны.

Обратим внимание на требование не оставлять приватных сообщений на автоответчиках. Это требование является очевидным, но про него часто забывают, как и про возможность постороннему несанкционированно прослушать автоответчик (в том числе и удаленно).

Также следует требовать от персонала выполнения требований по безопасности при работе с факсами:

- не передавать по факсу конфиденциальную информацию;
- исключить неавторизованный доступ к месту хранения сообщений (в случае использования факс сервера, например);
- учитывать возможность запланированного или случайного программирования факса для посылки сообщений по определенным номерам;
- учитывать возможность посылки сообщений по неверным номерам.

## 1.4 Контроль доступа

### 1.4.1 Политика контроля доступа

Контроль доступа - это основа любой политики безопасности. Модели доступа (дискретные, мандатные) - это то, с чего начиналась в конце 80-х наука об информационной безопасности. Выделим основные требования стандарта относительно политики контроля доступа.

Политика должна учитывать следующее:

1. Требования по безопасности отдельных бизнес приложений.
2. Идентификация всей информации, связанной с бизнес приложениями.
3. Политика распространения и авторизации информации, например, необходимо знать принципы и уровни безопасности и иметь классификацию информации.
4. Соответствие между контролем доступа и политикой классификации информации в разных системах и сетях.
5. Значимые законы о защите информационных ресурсов.
6. Стандартные профили доступа для всех типовых категорий пользователей.
7. Управление правами пользователей в распределенных системах со всеми типами соединений.

Правила контроля доступа:

1. Дифференциация между правилами, которые обязательны или необязательны.
2. Создание правил доступа по принципу "Запрещено все, что не разрешено явно".
3. Определение действий, для осуществления которых нужен администратор.

### 1.4.2 Управление доступом пользователя

- ✓ **Регистрация пользователя**

1. Использование уникального идентификатора пользователя, по которому его можно однозначно идентифицировать. Применение групповых идентификаторов может быть разрешено только там, где это требуется для выполнения работы.

2. Проверка, что пользователь авторизован ответственным за систему для работы с ней. Возможно получение отдельного разрешения для наделения правами пользователя у руководства.

3. Проверка, что уровень доступа соответствует бизнес задачам политике безопасности организации и не противоречит распределению обязанностей (ответственности).

4. Документальная фиксация назначенных пользователю прав доступа.

5. Ознакомление пользователя под роспись с предоставленными правами доступа и порядком его осуществления.

6. Все сервисы должны разрешать доступ только аутентифицированным пользователям.

7. Обеспечение формального списка всех пользователей, зарегистрированных для работы в системе.

8. Немедленное исправление (удаление) прав доступа при изменении должностных обязанностей (увольнении).

9. Периодический контроль и удаление не используемых учетных записей.

10. Обеспечение недоступности запасных идентификаторов другим пользователям.

Применение уникальных идентификаторов пользователей достаточно очевидно и не нуждается в комментариях. Применение групповых идентификаторов обычно не рекомендуется и возможно только для работы в системах обработки данных, где не требуется обеспечение особого уровня защиты и подобной меры защиты как групповой идентификатор может быть вполне достаточно.

Требование обязательной проверки легитимности каждого пользователя означает, что необходимо проверять, действительно ли данный пользователь имеет разрешение для работы с данной системой, и он был внесен в систему с разрешения ответственного за нее менеджера. Выполнение этого требования является достаточно важным условием нормальной работы больших систем. В подобных системах такую проверку рекомендуется проводить регулярно, чтобы исключить возможность случайного или целенаправленного внесения в систему неавторизованного пользователя (то есть пользователя, которого внесли в систему без разрешения руководства). Очевидно, что такую проверку должен осуществлять независимый от отдела информационных технологий или отдела безопасности аудитор.

В том случае, если в систему вносится особо привилегированный пользователь или он будет работать с какими-либо особо конфиденциальными или секретными данными, для его

внесения в систему, возможно, потребуется получение отдельного разрешения у руководства.

Особо следует отметить требование проверки соответствия уровня доступа выполняемым бизнес задачам и политике безопасности организации, а также того, что назначенный уровень доступа и не противоречит принципам разделения обязанностей (ответственности). Несмотря на то, что это требование чрезвычайно важно, оно часто нарушается на практике, когда пользователи имеют избыточные права, которые не требуются для выполнения текущих бизнес задач. В общем случае, это может привести к серьезным нарушениям безопасности системы, если правами пользователя завладеет нарушитель.

Требование документального закрепления предоставленных пользователю прав и ознакомление его под роспись с порядком их использования является обязательным и призвано помочь компании защитить свои права в случае какого-либо инцидента или судебного разбирательства с персоналом.

Требования немедленного удаления прав пользователей, служебные которых поменялись, а также периодические проверки и удаление неиспользуемых учетных записей является достаточно очевидным, но требует соответствующего внимания, особенно в крупной компании.

- ✓ **Управление привилегиями**

Многопользовательская система должна иметь следующую формализацию процесса авторизации:

1. Права доступа к каждому системному компоненту (например, ОС, СУБД и приложения) должны быть определены для всех категорий персонала, имеющих к ним доступ.
2. Привилегии индивидуальных пользователей, выдающиеся по мере необходимости или от случая к случаю должны быть минимальны - только такие, какие необходимы.
3. Доступ должен предоставляться лишь после успешного прохождения процессов идентификации и аутентификации. Факт получения доступа должен фиксироваться в системном журнале.
4. Минимизация пользовательских привилегий должна достигаться использованием системных процедур.

Управление привилегиями в многопользовательской системе важный процесс для любой автоматизированной системы. Соответственно стандарт рекомендует соблюдение данных

требований для формализации процесса авторизации пользователя в системе и предоставления ему прав. Обратим внимание на следующие требования стандарта.

Во-первых, рекомендуется разделить привилегии пользователей и предоставлять доступ не только к операционной системе в целом, но и, при необходимости, к отдельным приложениям и утилитам. Во-вторых, как уже отмечалось, необходимо наделять всех пользователей минимальными привилегиями, особенно временных пользователей, которым привилегии выдаются по мере необходимости или от случая к случаю.

- ✓ **Управление паролями пользователей**

Управление паролями пользователей является одним из ключевых факторов безопасности любой компании. Как известно, человеческий фактор является одним из самых трудно учитываемых факторов в комплексном процессе управления безопасностью компании. Пароль, как важная часть человеческого фактора, является одним из самых "тонких" мест в безопасности, так как, зачастую, злоумышленнику достаточно узнать пароль, в результате чего он сможет войти в систему с правами настоящего пользователя и будет практически не отличим от него для системы. Поэтому жизненно важно продумать механизмы управления паролями пользователей и учесть данные требования стандарта.

Согласно вышесказанному, прежде всего, необходимо соблюсти требование ознакомить пользователей под роспись с правилами парольной защиты, которые, в частности, должны включать требования сохранения конфиденциальности личных паролей и работы с групповыми паролями только внутри группы. Здесь необходимо добавить, что в данном документе требуется предусмотреть ответственность пользователей за его нарушение.

Рекомендуется настроить систему таким образом, чтобы при первом входе пользователя с назначенным ему временным паролем система сразу же требовала его сменить. Временные пароли должны передаваться пользователям безопасным образом. Необходимо избегать передачи паролей с использованием третьих лиц или незашифрованной электронной почтой. Пользователь должен подтвердить получение пароля.

- ✓ **Проверка прав пользователей**

Основное требование данного пункта стандарта заключается в необходимости периодической проверки прав пользователей. Стандарт рекомендует осуществлять регулярную проверку прав (подчеркнем слово регулярная) пользователей регулярно (каждые 6 месяцев) или после каждого внесения изменений в систему (о чем часто забывают на

практике). Для пользователей, имеющих особые привилегии доступа в систему, регулярная проверка прав должна проходить чаще - один раз 3 месяца.

### 1.4.3 Ответственность пользователей

- ✓ **Использование паролей**

Стандарт регламентирует практику использования и обращения с паролями. Обратим внимание и прокомментируем следующие требования стандарта, хотя в целом они являются достаточно очевидными.

Все пользователи должны избегать записывать пароли на бумаге, в файле, электронной записной книжке, если невозможно обеспечить их безопасное хранение. Отметим, что для обеспечения повышенного уровня безопасности не стоит вообще записывать пароль куда-либо и требуется его просто запомнить. Также стоит не пренебрегать требованием менять пароль в случае его компрометации (разглашении или подозрении на разглашение пароля, например, при его передаче в открытом виде по незащищенным каналам связи). Требованию применения качественных паролей посвящено огромное количество литературы - качество пароля это тема, обсуждаемая уже очень давно. Отметим, что с точки зрения компромисса между способностью человека запоминать символьные последовательности и современным уровнем развития вычислительных мощностей имеет смысл выбирать пароли длиной 8 символов. Более короткие пароли легче подобрать, а более длинные - сложно запомнить. Ограничение на длину пароля обычно задается "снизу" (т.е. "длина не менее 8 символов"), что позволяет, по возможности, применять и более длинные пароли.

Требование изменять пароли на регулярной основе (либо через определенный промежуток времени, либо после определенного числа использований) также является очевидным и штатно предусмотрено в большинстве систем. При этом пароли привилегированных пользователей должны меняться чаще.

При смене пароля недопустимо выбирать пароли, которые уже использовались ранее. Разные системы имеют разную "глубину хранения" списка использованных паролей: от одного (последнего) до всех, использованных с момента установки системы.

Запрет использования автоматического входа в систему можно найти в любом учебнике по безопасности также как и требование не раскрывать и не давать другим пользователям личный пароль.

Все пользователи должны знать, что необходимо:

1. Хранить пароли строго конфиденциально.
2. Избегать записывать пароли на бумаге, если они не хранятся в безопасном месте.

3. При компрометации (разглашении или подозрении на разглашение пароля) немедленно менять пароли.

4. Выбирать качественные пароли, а именно:

- Длина пароля - не менее 8 символов.
- Пароль легко запоминается.
- Пароль не является легко идентифицируемой информацией (имя пользователя, дата рождения и т.п.).
- Пароль не является повторяющейся последовательностью каких-либо символов (например, "111111", "аааааа" и т.п.).

5. Изменять пароли на регулярной основе (либо через определенный промежуток времени, либо после определенного числа использований), при этом пароли привилегированных пользователей должны меняться чаще. При смене пароля недопустимо выбирать пароли, которые уже использовались ранее.

6. Изменять заданный администратором временный пароль при первом же входе в систему.

7. Не использовать автоматический вход в систему, не применять сохранение пароля под функциональными клавишами.

8. Не сообщать другим пользователям личный пароль, не регистрировать их в системе под своим паролем.

✓ **Оборудование пользователей, оставляемое без присмотра**

Пользователи должны:

1. Завершать активную сессию перед тем, как отлучиться от оборудования, за исключением случаев длительной автоматической обработки данных при обязательном условии блокировки экрана и клавиатуры.

2. Обязательно завершать соединение с сервером по окончании работы с ним, а не просто выключать терминал или компьютер.

3. Обеспечивать безопасность рабочих станция и терминалов путем блокирования клавиатуры в случае ухода с рабочего места.

Обратим внимание на тот факт, что эти очевидные требования далеко не всегда выполняются на практике и часто сотрудники компании относятся к их выполнению достаточно халатно. Поэтому в автоматизированной системе необходимо учесть

автоматическое выполнение данных функций (по тайм-ауту, например), чтобы свести влияние человеческого фактора к минимуму.

### 1.4.4 Контроль и управление удаленного (сетевого) доступа

- ✓ **Правила использования сетевых служб и сервисов**

Строгая предварительная регламентация использования сетевых служб и сервисов является чрезвычайно важным фактором для безопасности компании в целом. При планировании функционирования распределенных бизнес процессов в сети компании необходимо в соответствии с требованием стандарта (и в соответствии со здравым смыслом) продумать:

1. К каким объектам и сервисам требуется предоставлять удаленный доступ (с точки зрения функционирования бизнес процессов).
2. Кому разрешен удаленный доступ, к каким объектам и сервисам. Какова процедура авторизации удаленного доступа, то есть, кто разрешает (авторизует) доступ пользователя к определенным объектам и сервисам.
3. Применяемые методы и средства сетевой защиты.
4. Такое предварительное планирование функционирования всей сети именно с точки выполнения бизнес процессов может стать первым шагом к пониманию, какие сервисные функции эта сеть должна выполнять, какие задачи и какого уровня конфиденциальности она должны решать и какой уровень защиты требуется каждому ее ресурсу и службе всей сети в целом.

- ✓ **Ложная маршрутизация**

При предоставлении удаленного доступа в систему необходимо продумать методы идентификации точки доступа и контроля маршрута к ресурсам системы. Эти методы давно и активно применяются на практике (межсетевые экраны, потоковые шифраторы трафика, виртуальные частные сети (VPN) и т.д.) - к этому мы привыкли. Но стоит обратить внимание на тот факт, что стандарт рекомендует смотреть на эту проблему именно в комплексе (имея в виду не только межсетевые экраны), не забывая, например, о прикладных системах, где контроль соединений между программным обеспечением также может иметь соответствующее применение на прикладном уровне.

- ✓ **Контроль над сетевыми соединениями**

Очевидность контроля над сетевыми соединениями и роутингом не вызывает сомнения и это требование стандарта давно воплощено на практике. Для этого существуют межсетевые экраны, потоковые шифраторы, средства адаптивного управления безопасностью, средства контроля трафика - все эти средства решают задачу контроля над сетевыми соединениями в соответствии с существующей в компании политикой безопасности. Речь идет о таких аспектах контроля соединений, как установление временных рамок входа в систему, идентификация терминалов и сетевых адресов (т.е. точек доступа), ограничение числа одновременных соединений одного пользователя, запрет или ограничение числа соединений с одного адреса под разными идентификаторами и т.п.

### 1.4.5 Контроль доступа в операционную систему

Необходимо обеспечить:

1. Идентификацию и аутентификацию пользователя, а при необходимости и идентификацию оборудования (сетевой адрес, номер терминала и т.п.), с которого осуществляется доступ.
2. Запись успешных и неудачных попыток входа.
3. Использование качественных паролей, если применяется парольная система аутентификации.
4. При необходимости ограничить временные рамки доступа пользователя в систему и число одновременных подключений.

В теории требование проверки месторасположения каждого авторизованного пользователя выглядит совершенно логично для критичных систем. На практике это также достаточно легко реализуемая задача (контроль за IP адресом отправителя, например), находящая свое воплощение во многих реальных системах. Однако смысл этого требования стал теряться с развитием криптографии и средств сетевой криптографической защиты трафика, когда не важно, откуда территориально осуществляется доступ, важно, что трафик надежно защищен и пользователь надежно авторизован. Хотя, для особо критичных задач это требование может применяться как дополнительная к криптозащите трафика мера. Также это требование может применяться и без криптозащиты трафика (например, администрирование межсетевого экрана из приватной сети только из сегмента администратора).

Требование записи успешных и неудачных попыток входа часто на практике реализуется только на половину, когда протоколируются только успешные входы в систему, а запись

неудачных попыток входа не ведется. Это не совсем верно, так как затрудняет анализ журналов на предмет поиска злонамеренной активности.

- ✓ **Процедура входа в систему (log on)**

Стандарт регламентирует следующие требования к данной процедуре:

1. Анонимность системы до завершения процедуры авторизации. Для выполнения данного требования необходимо не высвечивать системные надписи, по которым можно понять, что это за система или приложение, пока процедура входа не будет успешна завершена. Как известно, по системным заставкам в процессе входа с ОС или приложение можно сразу понять, что именно за система здесь установлена. Это может помочь потенциальному злоумышленнику осуществить атаку на данную систему, зная ее конкретную версию. В том же случае, если системные надписи отсутствуют, то процесс определения типа ОС или приложения становится не тривиальным и сложно детерминируемым. Поэтому выполнение данного требования стандарта может сильно усложнить жизнь злоумышленнику. Развивая это требование, можно ввести злоумышленника в заблуждение, высветив в процессе входа в систему заведомо неверное сообщение о ее типе.
2. Соблюдение требования высвечивать предупреждение, что вход в компьютер возможен только для авторизованных пользователей важно с точки зрения соблюдения законодательства многих стран, где нарушение считается нарушением только, если нарушитель был предварительно предупрежден о том, что он совершает противоправные действия.
3. Требование не предоставлять сообщений подсказок в течение процедуры входа для избежания какой-либо возможной помощи неавторизованному пользователю является очевидным и обычно реализовано во всех системах.
4. Требование проверки всей введенной информации, запрашиваемой при входе в систему только целиком, когда вся информация будет введена пользователем, хорошо знакомо пользователям Интернет банкинга, когда ошибка возникает только в конце всей процедуры и не известно на каком шаге была введена неверная информация (неверное имя пользователя, постоянный пароль или пароль из заранее полученного персонального списка паролей).
5. Требование ограничения числа неудачных попыток входа может быть предусмотрено, но его применение требует определенной аккуратности и заранее продуманной политики. Проблема здесь может заключаться во введении функции блокирования учетной записи после нескольких неудачных попыток входа, что часто

применяется в Интернет банкинге. Например, три неверных ввода пароля при входе в систему приводит к блокировке учетной записи и необходимости пользователю позвонить операционисту. Это может позволить злоумышленнику организовать автоматизированную целенаправленную атаку на пользователей Интернет банкинга и заблокировать большое число учетных записей. Наличие такой функции в системе биржевых торгов может дать возможность заблокировать доступ конкурента к торговой сессии и нанести ему ощутимый ущерб. Поэтому выполнение данного требования требует определенной осторожности.

6. На требование высвечивания времени и даты предыдущего успешного входа в систему и подробностей любых неуспешных попыток входа со времени последнего успешного входа в систему стоит также обратить внимание. Его выполнение в реальной системе может помочь практически сразу же после входа в систему авторизованного пользователя обнаружить попытки несанкционированного входа под именем данного пользователя в том случае, если пользователь будет внимательно читать полученные от системы данные (это должно входить в его должностные обязанности).

- ✓ **Система управления паролями**

1. Обязательное применение индивидуальных паролей.
2. По возможности, позволять пользователям выбирать и менять свой пароль, а также предусмотреть процедуры контроля ошибок при вводе пароля.
3. Обязательное (путем применения соответствующей процедуры) применение качественных паролей.
4. В системах, где пользователь должен сам создать свой пароль, обязательно должна присутствовать процедура смены заданного администратором пароля при первом входе в систему.
5. Обеспечить запись старых паролей пользователей (например, за предыдущие 12 месяцев), чтобы предотвратить их повторное использование.
6. Пароль не должен отображаться при вводе.
7. Файл (база данных) паролей должен храниться отдельно от данных прикладных программ.
8. Файл (база данных) паролей должен храниться в защищенном при помощи криптографических методов виде, при этом должны применяться стойкие алгоритмы.
9. Пароли по умолчанию, устанавливаемые производителями оборудования и программного обеспечения, должны быть заменены в обязательном порядке.

Отметим требование стандарта семантической бессмысленности имени пользователя, так чтобы имя не показывало на возможный уровень доступа данного пользователя (имена

supervisor, manager желательно не использовать). Это требование очевидно, но про него иногда забывают.

Требования к системе управления паролями достаточно очевидны и не нуждаются в особых комментариях на сегодняшний день. Отметим лишь спорность требования обеспечения записи старых паролей пользователей (например, за предыдущие 12 месяцев) для предотвращения их повторного использования. Дело в том, что часто пользователи придумывают свои новые пароли так или иначе на основе старых и если такой файл попадет к злоумышленнику, то он может почерпнуть из него много полезной информации для подбора новых паролей. Поэтому, если в системе планируется выполнение данного требования, необходимо предпринять специальные меры защиты, против этой угрозы. Например, хранить не сами пароли, а значение вычисленной от них хеш-функции.

### 1.4.6 Контроль и управление доступом к приложениям

Прикладная система должна:

**1.** Управлять доступом пользователей к информации и системным вызовам приложений в соответствии с определенной политикой безопасности.

**2.** Обеспечивать защиту от несанкционированного доступа к системным утилитам.

**3.** Иметь возможность предоставлять доступ к информации только ее владельцу.

Требования по ограничению доступа к информации:

**1.** Система меню для управления доступом к функциям прикладных программ.

**2.** Информация о функциях информационных систем и приложений должна предоставляться пользователю, в зависимости от уровня его доступа (необходима соответствующая редакция пользовательской документации и системного меню).

**3.** Управление правами доступа пользователей (читать, писать, удалять, выполнять).

**4.** Обеспечение отправления выходных данных приложений с важной информацией только на авторизованные терминалы, включая периодическую проверку выходных данных, чтобы убедиться, что избыточная информация там отсутствует.

**5.** Изоляция особо важных систем.

Безопасность должна контролироваться и обеспечиваться не только на уровне операционной системы или сети. Безопасность также должна быть заложена и на уровень приложений, то есть прикладных систем.

Данные требования стандарта к безопасности прикладных систем должны быть учтены и обычно учитываются их разработчиками. Обратим здесь еще раз внимание на пункт

обеспечения защиты на уровне приложения от неавторизованного доступа к системным утилитам - особая важность системных утилит подчеркивается и здесь.

В требованиях ограничения доступа к информации прикладных систем имеет смысл обратить внимание на необходимость ограничения информации о функциях информационных систем и приложений, которая должна предоставляться пользователю, в зависимости от уровня его доступа (необходима соответствующая редакция пользовательской документации и системного меню). То есть имеет смысл не предоставлять обычным пользователям системную документацию, чтобы уменьшить вероятность несанкционированного использования или проникновения в систему. Однако данное требование на практике учитывается далеко не всегда, что недопустимо.

Также отметим требование обеспечения отправления выходных данных приложений с важной информацией только на авторизованные терминалы, включая периодическую проверку выходных данных, чтобы убедиться, что избыточная информация там отсутствует. Это требование может быть реализовано как на уровне операционной системы или сети, так и на уровне приложения, что позволит дублировать защиту на обоих уровнях и строить более гибкие, многоуровневые системы безопасности.

В любой компании обычно существуют прикладные системы, которые имеют особое значение для данной компании. Эти системы обычно относятся к так называемой операционной среде и непосредственно решают бизнес задачи или хранят и обрабатывают информацию повышенной важности. Подобные особо важные приложения в соответствии с требованием стандарта должны быть изолированы и для их использования должна быть разработана специальная политика безопасности, учитывающая все их особенности.

### 1.4.7 Мониторинг доступа и использования систем

- ✓ **Журнал событий**

Важность ведения и последующего (подчеркнем это) анализа журнала регистрации событий не подвергается сомнению. Стандарт рекомендует вести протоколирование вышеперечисленных событий, из которых стоит отметить запись не только успешных, но и неудачных попыток входа в систему и записи об успешных или неудачных попытках получения доступа к данным и иным ресурсам. То есть в особо важных системах рекомендуется вести журнал доступа на уровне ресурсов системы.

И еще раз повторим важность анализа журнала событий, поэтому он должен быть максимально информативен и для его анализа лучше всего применять специальные утилиты. При этом возникает ряд спорных моментов. Например, существуют аргументы "за" и

"против" записи в журнал введенного пароля при неудачной попытке доступа. С одной стороны, при анализе это может дать некоторую информацию, облегчающую идентификацию нарушителя. С другой стороны, в случае ошибки в одном символе при вводе пароля законным пользователем, его пароль, фактически, компрометируется.

✓ **Мониторинг использования системы**

Осуществляя мониторинг системы путем анализа журнала регистрации стандарт рекомендует обратить внимание на следующие детали:

1. В случае авторизованного доступа:

- идентификатор пользователя;
- дата и время важных (ключевых) событий;
- тип события;
- затребованные файлы;
- использованные программы и утилиты

Анализ этой информации позволит составить полную картину о поведении пользователя и выявить все возможные попытки отклонения от своих прямых должностных обязанностей.

2. В случае выполнения привилегированных операций:

- вход с правами суперпользователя (администратора);
- старт и остановка системы;
- присоединение устройств ввода-вывода;

Таким образом осуществляется контроль над действиями администраторов системы и все критичные действия не останутся без внимания.

Отметим требование стандарта о необходимости разделения ответственности между сотрудником, проводящим постоянный (динамический) анализ логов и тем, кто анализирует события в целом (события за неделю, например). Данную работу лучше получать разным людям, чтобы уменьшить вероятность ошибки и вероятность сговора.

Стандарт подчеркивает важность точности фиксации времени, когда произошло данное событие и когда оно было записано в журнал. Сбой в системной дате и времени серьезно затруднит последующий анализ произошедших событий.

### 1.4.8 Мобильные компьютеры и пользователи

✓ **Удаленная работа**

Мобильные пользователи являются неотъемлемой частью крупных компаний. Сотрудники, находящиеся в командировках, должны продолжать выполнять свои должностные обязанности. Но обычно в командировках персоналу требуется осуществлять удаленный доступ к внутренним ресурсам компании, что приводит к дополнительным сложностям при построении архитектуры безопасности сети компании, в которой имеются мобильные пользователи. Стандарт безопасности рекомендует обратить самое серьезное внимание на обеспечение безопасности мобильных пользователей, и это не лишено смысла. Примеры кражи или утери ноутбуков с конфиденциальной и даже секретной информацией сотрудниками спецслужб регулярно появляются в прессе. Что же говорить об обычных компаниях, где уровень защиты, как правило, существенно ниже.

Поэтому для мобильных пользователей необходима разработка отдельных требований и нормативных документов по физической защите, разграничению доступа, криптографической защите, резервному сохранению, антивирусной защите. Также, согласно стандарту, необходима политика, которая бы определяла правила доступа к корпоративной сети и отдельный документ, посвященный правилам осуществления доступа в корпоративную сеть из общественных мест и сетей. Без этих документов безопасная работа мобильных пользователей невозможна.

Требования безопасности:

- обеспечение физической защиты места удаленной работы, включая физическую безопасность здания или ближайшего окружения;
- обеспечение безопасности телекоммуникаций, учитывающее необходимость удаленного доступа к внутренним ресурсам компании; важность информации и систем, к которым будет осуществлен удаленный доступ; прохождение через каналы связи;
- учет возможной угрозы неавторизованного доступа к информации или ресурсам, от иных близких к удаленному пользователю людей, например, семья, друзья.

Обеспечение безопасности:

- обеспечение необходимым оборудованием для удаленного мобильного доступа;
- определение разрешенных видов работ, разрешенного времени доступа, классификация информации, которая может обрабатываться удаленно, определение систем и сервисов, к которым данному мобильному пользователю разрешен удаленный доступ;
- обеспечение необходимым коммуникационным оборудованием, включая средства обеспечения безопасности;
- физическая безопасность;
- правила доступа к оборудованию и информации для членов семьи и посетителей;
- обеспечение программным обеспечением и оборудованием;

- наличие процедур резервного копирования и обеспечения непрерывности ведения бизнеса;
- аудит и мониторинг безопасности;
- аннулирование разрешения, прав доступа и возврат оборудования при отмене (завершении) удаленного мобильного доступа.

### 1.5 Разработка и техническая поддержка вычислительных систем

#### 1.5.1 Безопасность приложений

✓ **Проверка входных данных**

Для разработчиков приложений стандарт предлагает свои специфические требования безопасности. Речь идет, прежде всего, о проверке правильности входных и выходных данных.

Проверка входных данных приложений является чрезвычайно важно задачей. Как известно практикам, самое большое число взломов сетевого программного обеспечения случается именно из-за ошибок, связанных с переполнением буфера, то есть неправильной интерпретации входных данных. В случае входных данных стандарт рекомендует проведение следующих проверок.

Проверка входных данных на следующие ошибки:

- превышение размерности значения;
- недопустимые символы во входном потоке;
- отсутствующие или неполные данные;
- объем входных данных выше или ниже нормы;
- запрещенные или неверные управляющие значения.

Стандарт рекомендует обращать в целом серьезное внимание на данные, поступающие на вход (на обработку) в информационные системы компании. Неверные входные данные (случайно или злонамеренно) могут привести к серьезным ошибкам на выходе системы. Поэтому стандарт рекомендует вышеуказанные проверки.

Необходимость процедур проверки достоверности входных данных (желательно автоматизированных) избавит от многих случайных ошибок (превышение размерности, например). Процедуры определения ответственности и процедуры контроля входных данных для всего персонала, вовлеченного в процесс обработки и ввода входных данных, вынудят

персонал относится соответствующе к этому процессу и сократят возможные ошибки и злоупотребления при вводе данных.

- ✓ **Проверка правильности выходных данных**

Проверка правильности выходных данных является логическим продолжением проверки правильности входных данных. Проверив вход, необходимо проверить, что получилось на выходе. Разработчикам ПО следует обратить внимание на предъявляемое стандартом требование проверки прохождения программой всех контрольных точек, чтобы убедиться, что все данные были обработаны. Разработчикам систем стоит продумать процедуры для проверки правильности выходной информации. Службе безопасности необходимо определить ответственность для всего персонала, вовлеченного в процесс обработки выходных данных.

- ✓ **Зоны риска**

Основной риск - риск сбоев процессов и нарушения целостности. Поэтому применяют:

- программы с функциями добавления или уничтожения данных;
- процедуры по предотвращению некорректного запуска программ после предыдущих сбоев;
- применение программ для восстановления после сбоев.

- ✓ **Проверки и средства управления**

1. Контроль сессий и автоматического выполнения заданий на предмет отклонений от обычного использования ресурсов.
2. Контроль изменений использования ресурсов по сравнению с предыдущими:
   - запусками программ;
   - изменениями файла;
   - передачами управления от программы к программе.
3. Проверка правильности сгенерированных системных данных.
4. Проверка целостности данных и программного обеспечения после их передачи с одного компьютера на другой.
5. Общая контрольная сумма (хеш) всех записей и файлов.
6. Проверка того, что программы запускаются в соответствующее время.

7. Проверка того, что программы запускаются в соответствующем режиме и останавливаются в случае неисправностей, а также что связанные процессы останавливаются до устранения всех проблем.

### 1.5.2 Средства криптографической защиты

- ✓ **Политика использования систем криптографической защиты (СКЗИ)**

Криптография давно прочно вошла в повседневную жизнь, как простых пользователей, так и компаний и государств. Сегодня криптография является по сути единственным надежным способом идентификации/аутентификации пользователя (правда, не стоит забывать о биометрических методах идентификации личности, которые пока применяются достаточно редко) и защиты хранимой и передаваемой по каналам связи информации.

У любой компании обычно существует конфиденциальная информация соответствующего уровня, требующая криптографической защиты при хранении и при передаче по каналам связи. Поэтому, на основе анализа рисков бизнес процессов и обрабатываемой в системе информации стандарт рекомендует разработать политику применения средств криптографической защиты. Такая политика должна определить какая бизнес информация подлежит защите с применением криптографических средств и определить требуемый уровень криптозащиты, учитывающий тип и качество криптоалгоритма, а также длину ключа. Кроме того, требуется принять единый стандарт криптозащиты для организации и определить, начиная с какого уровня, информация требует криптографической защиты при хранении и при передаче по каналам связи. Обратим особое внимание на необходимость разработки подхода к управлению ключами, включая методы для восстановления зашифрованной информации в случае утери, компрометации или уничтожения ключей и определения ответственных за обеспечение криптозащиты лиц.

Применяя криптографические алгоритмы важно обеспечить соответствующую защиту ключей как в случае обычного шифрования с симметричными ключами, так и в случае шифрования с открытыми ключами, так как секретные ключи являются слабым звеном любого алгоритма шифрования.

И так, при разработке политики необходимо учесть:

- управленческий подход к использованию СКЗИ внутри организации, включая основные принципы, какие именно классы информации должны быть защищены;

- политика управления ключами, включая методы для восстановления зашифрованной информации в случае утери, компрометации или уничтожения ключей;
- распределение обязанностей:
  - кто и за что несет ответственность;
  - внедрение политики;
  - управление ключами;
  - порядок определения адекватного уровня криптографической защиты;
  - стандарты, которые могут быть внедрены и адаптированы в организации (какие решения подходят для каких бизнес процессов).

✓ **Стандарты, процедуры, методы**

Данный пункт стандарта определяет типовые подходы к системе генерации, хранения и управления криптографическими ключами. Все вышеизложенные требования стандарта являются общеизвестными, но требуют детальной проработки, так как когда речь идет о применении криптографии, то обычно защищаются особо важные для компании данные, соответственно требуется повышенная ответственность и максимальная детализация и проработка всех рабочих процедур.

Основные процедуры:

- генерация ключей для разных криптосистем и разных приложений;
- генерация и получение открытых ключей;
- выдача ключей пользователям, включая процедуру активации ключа после его получения;
- хранение ключей, включая порядок получения авторизованными пользователями доступа к ключам;
- порядок смены ключей;
- действия в случае компрометации ключей;
- отзыв ключей, включая порядок их деактивации при компрометации или увольнении ответственного за них сотрудника, а также определение случаев, когда эти ключи должны быть сохранены;
- восстановление поврежденных или утерянных ключей (как часть управления непрерывностью бизнеса);
- архивирование и резервное копирование ключей;
- уничтожение ключей;

- протоколирование всех действий, связанных с управлением ключами;
- ограничение срока действия ключей.

### 1.5.3 Безопасность системных файлов

✓ **Контроль объектов операционной системы**

Основные требования:

1. Обновление библиотек должно выполняться только с разрешения руководства.
2. Если возможно, ОС должна содержать только исполняемые файлы.
3. Исполняемые файлы и изменения библиотек не должны внедряться в ОС до подтверждения их успешного тестирования, а также информирования и обучения пользователей (если в этом нет острой необходимости).
4. После всех изменений в библиотеках должна быть обеспечена проверка всех регистрационных журналов.
5. Предыдущие версии должны быть сохранены для непредвиденных случаев.

### 1.5.4 Защита рабочих данных, используемых при тестах систем

На этот пункт стандарта имеет смысл обратить особое внимание, так как подобные требования не столь очевидны и не так часто встречаются. Как известно перед вводом в строй новых версий систем, выполняющих непосредственные бизнес операции (ПО операционной среды) необходимо обеспечить их многоплановые проверки и тесты. Для этого часто требуется работа с настоящими рабочими данными из операционной среды. Поэтому в этом случае тестовая среда должна иметь уровень защиты, соответствующий уровню защиты реальной рабочей системы, что и рекомендует стандарт. Кроме того, в соответствии с требованием стандарта при копировании рабочей информации в тестовую систему требуется получение специального разрешения от руководства и это должно быть запротоколировано для обеспечения последующей возможности аудита. И последнее, что рекомендует данный пункт стандарта, это требование немедленного удаления рабочей информации из тестовой системы после завершения тестов.

### 1.5.5 Контроль доступа к исходным текстам программ и библиотек

Не менее важно в рабочей системе обеспечить контроль доступа к исходным текстам программ и библиотек. Во-первых, исходные тексты программ и библиотек не должны содержаться в ОС, чтобы уменьшить список лиц, которые имеют или потенциально могут получить к ним доступ. Также отметим требования запрета неограниченного доступа персонала из службы поддержки к исходным текстам программ и библиотек. Персонал должен получать доступ только к тем исходным текстам, которые необходимы ему для выполнения должностных обязанностей. Это требование по духу совпадает с требованием стандарта не предоставлять всему персоналу полной технической документации на ОС и приложения. Для каждого приложения должен быть назначен ответственный сотрудник, отвечающий за контроль исполняемых модулей. Изменения и дополнения в исходные тексты программ и библиотек, а также передача исходных текстов программистам должна осуществляться только вместе с библиотеками и по разрешению менеджера поддержки данного приложения. Листинги программ должны храниться в безопасном месте. Старые версии исходных текстов программ должны быть заархивированы, с отметкой времени и даты и вместе со всем сопутствующим программным обеспечением, процедурами, описаниями и т.д. Поддержка и копирование исходных текстов библиотек и программ должны быть предметом процедур контроля изменений.

Реализация требования записи всех попыток получения доступа к исходным текстам программ позволит осуществить при необходимости анализ и аудит данной активности в случае внесения какого-либо изменения в исходные тексты выявить его автора.

### 1.5.6 Процедуры контроля изменений

Внесение любых изменений является сложным и комплексным процессом. Изменения в одной системе могут повлечь за собой цепную реакцию необходимости изменений в соседних системах или вызвать общий сбой в работе всей системы. Это чрезвычайно сложный процесс и стандарт рекомендует подойти к его решению со всей серьезностью. Прежде всего, требуется идентифицировать ПО, информацию, базы данных, аппаратное обеспечение, которое требует изменений. Затем получить формальное разрешение, где детально описано, что именно будет меняться в системе. Не менее важным фактом является обеспечение того, что авторизованные пользователи принимают и понимают изменения до их внедрения - человеческий фактор требуется учесть и здесь.

Самым сложным требованием на практике является обеспечение безопасного внедрения изменения без последствий для бизнеса. Для его выполнения требуется иметь серьезную программу предварительных тестов вносимых изменений, а также обучения и подготовки персонала. Кроме того, необходимо продумать возможность снятия изменений и

возвращения системы в первоначальное состояние в установленный период времени (в том случае, если изменения приведут к незапланированному сбою системы). И последнее - это целый ряд требований, касающихся внесения соответствующих изменений в пользовательскую документацию, архивацию и контроль над предыдущими версиями документации.

### 1.5.7 Технический обзор изменений в операционной среде

После внесения изменений в операционную среду, стандарт предлагает осуществить анализ важных приложений и целостности процедур для того, чтобы убедиться в их работоспособности, так как несмотря на предварительные тесты, внесенные изменения могут не запланировано нарушить работоспособность и целостность среды.

Перед внесением изменений стандарт рекомендует убедиться, что годовой план поддержки систем и бюджет покроет расходы на анализ и тестирование систем после изменений ОС, в противном случае компания просто не может себе позволить вносить данные изменения.

И последнее на что стоит обратить внимание, это требование убедиться, что соответствующие изменения также внесены в планы обеспечения непрерывности бизнеса, которые основаны на текущей конфигурации рабочей системы.

### 1.5.8 Ограничения на изменения прикладного ПО

Основное требование, которое распространяется на изменение прикладного ПО (на все изменения в остальном ПО оно накладывается несколько меньше) - не вносить изменения без существенной необходимости!

Основная рекомендация стандарта здесь одна - получить согласие поставщика на внесение изменений, а лучше всего воспользоваться стандартными файлами с обновлениями, полученными напрямую от поставщика. Вносить же изменения на свой риск без согласия производителя стандарт не рекомендует, т.к. поставщик может отказать в дальнейшем сопровождении системы.

### 1.5.9 Безопасность процессов разработки и поддержки

- ✓ **Скрытые каналы и Троянский код**

Одна из основных задач службы безопасности не допустить внедрение в систему каналов утечки информации. Новое, непроверенное программное обеспечение всегда несет в себе скрытую угрозу наличия в нем неизвестных покупателю скрытых каналов, по которым в систему возможен несанкционированный доступ или по которым из системы возможна утечка информации.

Требуется:

- источники получения программ должны быть проверены и обладать соответствующей репутацией;
- покупая программы с исходным кодом, убедиться, что верификация кода возможна;
- применять качественные продукты;
- проверять весь исходный код;
- контролировать доступ и возможность модификации уже инсталлированного кода;
- использовать только проверенный персонал для работы на ключевых особо важных системах.

## 1.6 Управление непрерывностью бизнеса

### 1.6.1 Процесс управления непрерывным ведением бизнеса

Непрерывность ведения бизнеса является тем разделом, про который часто забывают, но он по праву считается одним из важнейших в общей политике безопасности компании. Да, непрерывность ведения бизнеса это один из разделов информационной безопасности, и это первое о чем говорит нам стандарт. У современного менеджмента сложилось двоякое мнение о данной теме. С одной стороны, многие менеджеры воспринимают непрерывность бизнеса как отдельную задачу, не имеющую отношения к безопасности компании в целом, и считают ее менее затратной темой, чем безопасность в целом, так как реализация комплекса мер по обеспечению непрерывности бизнеса позволит в критический момент минимизировать ущерб (но те же слова можно сказать и про безопасность, что часто упускается из вида). С другой стороны, менеджеры особенно в средних компаниях часто вообще упускают из вида эту важнейшую тему. Примером серьезного отношения к обеспечению непрерывного ведения бизнеса могут служить террористические акты в США 11 сентября 2001, когда часть компания, имевших подробные контраварийные планы смогли восстановить свой бизнес в установленный срок, несмотря на страшную трагедию. Компании, не имевшие

разработанной стратегии, понесли серьезные убытки и их бизнес был остановлен на продолжительный срок.

Стандарт безопасности рекомендует обратить самое серьезное внимание на данную тематику и начать, прежде всего, с осознания рисков, их вероятностей и возможных последствий, включая идентификацию и расстановку приоритетов для критичных бизнес процессов. Это означает проведение комплексного анализа всех бизнес процессов компании с выявлением наиболее критичных из них. На следующем шаге проводится анализ рисков (учитывая стихийные бедствия и т.д.) по бизнес процессам, расчет вероятностей их возникновения и оценку возможных последствий с оценкой ущерба.

Отметим рекомендацию стандарта о приобретении соответствующей страховки, которая может являться формой управления непрерывностью ведения бизнеса, но не стоит считать ее панацеей от всех бед - страховка снизит ущерб, но не восстановит технологический процесс ведения бизнеса.

Также не менее важно согласно стандарту заранее формализовать и задокументировать стратегию ведения непрерывного бизнеса, содержащую согласованные цели бизнеса и приоритеты, что является наиболее важным с точки зрения бизнеса, и какие бизнес объекты надо восстанавливать в первую очередь в случае происшествий.

Требование регулярного тестирования и обновления контраварийных планов и процессов является очевидным, но про него, к сожалению, часто забывают - аварии обычно происходят, к счастью, не так часто и топ менеджеры предпочитают проводить дорогостоящее тестирование планов как можно реже, что может пагубно отразиться на подготовке персонала и деталей плана в случае происшествия.

И последнее, на что необходимо обратить внимание, это на необходимость убедиться, что управление непрерывным ведением бизнеса внедрено в организационные процессы и структуру компании. Ответственность для координации управления непрерывным ведением бизнеса должна быть распространена по соответствующим уровням внутри всей организации и должен быть создан форум по информационной безопасности, на котором ответственные лица могли бы обсуждать соответствующие вопросы.

### 1.6.2 Создание и внедрение плана непрерывности бизнеса

Создание и внедрение плана непрерывного ведения бизнеса является важнейшей задачей. Стандарт рекомендует в очередной раз обратить внимание на распределение ответственности, определение всех контраварийных процедур и выработку четкого порядка действий в аварийных ситуациях. При внедрении контраварийных процедур для восстановления систем в отведенный период времени стоит обратить особое внимание на

оценку зависимости бизнеса от внешних связей, то есть насколько бизнес способен выживать сам по себе в случае отсутствия связей с внешним миром. Отметим также необходимость разработки документации о всех принятых контраварийных процессах и процедурах - это важно для обучения персонала действиям в критических случаях и требование регулярного тестирования и обновления планов.

### 1.6.3 Основы планирования непрерывности бизнеса

Данный пункт стандарта рекомендует учесть следующие требования, на которые стоит обратить внимание.

1. Условия вступления в действие планов (как оценить ситуацию, кто в нее вовлечен).
2. Контраварийные процедуры, описывающие действия в случае инцидентов, представляющих опасность для бизнес операций или/и человеческой жизни. Процедуры должны включать в себя мероприятия по связям с общественностью и органами власти.
3. Процедуры нейтрализации неисправностей, в которых описываются действия по выведению жизненно важных бизнес нужд или служб поддержки во временное альтернативное помещение и возвращение их в соответствующий период времени.
4. Процедуры восстановления, в которых описаны действия по возвращению к нормальному процессу бизнес операций.
5. Разработка программы, в которой описаны, как и когда план будет протестирован и процесс внедрения этого плана
6. Действия по информированию и обучению, которые разрабатываются для понимания персоналом процесса обеспечения непрерывности бизнеса и гарантии, что этот процесс продолжает быть эффективным.
7. Личная ответственность - кто именно отвечает за выполнение каждого компонента плана, с указанием дублирующих лиц.

### 1.6.4 Тестирование планов обеспечения непрерывности бизнеса

Тестирование контраварийных планов является отличительной чертой, показывающей серьезность отношения к принципам поддержки непрерывного ведения бизнеса.

Стандарт рекомендует применение различных технологий тестирования для гарантии того, что план будет работать в реальной жизни:

1. Обсуждение мероприятий (мозговой штурм) по восстановлению бизнеса в случае аварий - наиболее дешевый вид тестов. Однако практика показывает, что без проведения реальных тренировок сложно добиться приемлемого результата.

2. Тренировка поведения людей в случае кризисной ситуации и тестирование технических мероприятий по восстановлению для гарантии того, что информационная система будет эффективно восстановлена в отведенный промежуток времени.

3. Тестирование технических мероприятий по восстановлению в альтернативном месте - запуск бизнес процессов вместе с восстановительными мероприятиями вне основного места расположения - имеет смысл в случае серьезного происшествия на основном объекте.

4. Тестирование систем и сервисов поставщиков в случае аварий - позволит оценить работу внешних связей в случае возникновения неисправностей.

### 1.6.5 Обеспечение и переоценка планов

Примеры ситуаций, когда требуется изменение планов, в случае обновления ОС, покупки нового оборудования и изменений в:

- персонале;
- адресах или телефонных номерах;
- стратегии бизнеса;
- местоположении и информационных ресурсах;
- законодательстве;
- подрядчиках, поставщиках и ключевых заказчиках
- процессах, при добавлении новых или снятии старых
- рисков (операционных и финансовых)

Бизнес компании редко бывает статичен - постоянно возможны различные изменения. Автоматизированная система компании также подвергается соответствующим изменениям для адекватного соответствия выполняемым бизнес задачам. Поэтому стандарт рекомендует обратить внимание на необходимость внесения изменения в планы обеспечения непрерывности бизнеса в случае возникновения изменения в вышеизложенных параметрах, от которых зависит бизнес.

## 1.7. Соответствие системы основным требованиям

Соответствие информационной системы компании законам мирового сообщества и страны, в которой компания осуществляет бизнес, является неоспоримым фактом.

Требование соблюдения законов, связанных с авторским правом, является общемировой практикой и компания должна строго выполнять данное требование законодательства.

Отметим некоторые требования стандарта, посвященные соблюдению авторских прав на программное обеспечение.

Требование обеспечения осведомленности пользователей о авторских правах на программное обеспечение, правилах приобретения ПО и уведомление пользователей, что в случае нарушения будут предприняты дисциплинарные действия, является важным шагом на пути соблюдения данного закона, так как именно пользователи часто бывают инициаторами внесения в систему нелицензионного ПО или нарушения лицензионного законодательства.

Требования контроля над превышением максимального числа пользователей лицензии имеет смысл не только для соблюдения буквы закона, но и для обеспечения нормального функционирования информационной системы, которая в случае превышения числа пользователей, указанных в лицензии, может перестать корректно работать.

Требование выполнения регулярных проверок, что только разрешенные и лицензионные продукты инсталлированы, позволит снизить возможный ущерб от применения персоналом нелицензионного ПО.

Условия внесения в информационную систему компании ПО и информации, полученных из открытых сетей, является чрезвычайно важным фактором, систематизирующим работу компании и регулирующим и отсекающим поток нелицензионного ПО и вредоносного кода (вирусов, троянских коней), коими переполнены открытые сети.

В Европе принят закон, регламентирующий обработку и передачу персональных данных.

Выполнение данного закона требует соответствующей структуры управления и контроля. Часто лучше всего назначить специального менеджера по защите персональных данных.

Использование информационной системы компании в личных целях сотрудников, не совпадающих со своими прямыми должностными обязанностями, приносит компаниям колоссальные убытки, снижая производительность труда. Для предотвращения подобных злоупотреблений стандарт рекомендует устанавливать системы мониторинга активности сотрудников и предусмотреть в контракте дисциплинарные методы воздействия в случае нарушения данного пункта контракта. Кроме того, в контракт необходимо внести пункт, разрешающий компании использовать подобную систему мониторинга, легальность которого варьируется от страны к стране, поэтому прежде чем ее внедрить необходимо проконсультироваться у юриста.

Во многих странах есть законодательство против компьютерных злоупотреблений. Необходимо чтобы пользователи знали, что именно им разрешено делать в информационной

системе. Пользователь должен подписать соответствующий документ, регламентирующий порядок его работы в системе.

### 1.7.1 Соответствие требованиям законодательства

✓ **Регулирование применения криптографических методов**

Компании, осуществляющие бизнес в разных странах, могут столкнуться с тем, что там существует свои законы, связанные с применением криптографии. Примером могут стать США, где запрещен экспорт стойких криптоалгоритмов или Россия, где их легальное применение компаниями возможно лишь с разрешения спецслужб.

Необходимо предусмотреть контроль за следующим:

- импорт и/или экспорт программного или аппаратного криптографического обеспечения;
- импорт и/или экспорт программного или аппаратного обеспечения, куда можно встроить криптографические функции;
- мандатная или дискретная политика доступа, принятая в стране для доступа к информации, защищенной программным или аппаратным криптографическим обеспечением.

✓ **Сохранение улик (свидетельств, доказательств)**

Правила обращения с уликами.

1. Степень допустимости улики: когда и при каких условиях она может быть использована в суде в качестве доказательства.
2. Вес улики: качество и полнота улики.
3. Адекватность улики. Подсистема регистрации работает корректно и непрерывно; осуществляется запись всей информации; в любой момент можно получить необходимые сведения (улику) из регистрационных журналов.

Необходимо обеспечить соответствие информационной системы организации какому-либо опубликованному стандарту безопасности (для России - РД ГТК).

Для гарантии качества и полноты улики необходимо обеспечить подлинность улики:

- для бумажных документов: обеспечена безопасность хранения оригинала, ведется запись кто, где и когда нашел его и кто был свидетелем обнаружения. Расследование должно показать, что оригинал не был изменен.

- для информации в электронной форме: гарантия доступности должна быть обеспечена путем создания копий любых съемных носителей, информации на жестких дисках и в оперативной памяти. Все действия в процессе копирования должны быть запротоколированы и засвидетельствованы. Одна копия носителя и протокола должна храниться в безопасном месте.

### 1.7.2 Соответствие политике безопасности

Основное требование стандарта, основанное на факте постоянного изменения информационной системы любой компании, представляющей собой растущий и меняющейся организм, состоит в необходимости проводить регулярный анализ соответствия объектов системы существующей политике безопасности и стандартам:

- информационные системы;
- системы обеспечения;
- владельцы информации и информационных ресурсов;
- пользователи;
- менеджеры.

Особенно это необходимо после внесения серьезных изменений в информационную систему компании.

### 1.7.3 Соответствие техническим требованиям

Информационные системы должны проходить регулярную проверку на соответствие стандартам безопасности. Проверка технического соответствия включает проверку ОС на предмет корректного функционирования аппаратных и программных систем управления. Проверка должна производиться либо лично инженером, либо автоматизированным средством, отчет которого будет анализироваться затем инженером.

Проверка соответствия также включает тесты на проникновение, которые должны проводиться независимыми экспертами.

### 1.7.4 Методы и средства управления системным аудитом

Необходимость проведение регулярного аудита безопасности не подлежит сомнению и особо подчеркивается в стандарте. Отметим рекомендации стандарта, касающиеся проведения аудита.

1. Требования аудита должны быть согласованы с соответствующими руководителями.
2. Масштаб проверок должен быть согласован и подконтролен.
3. При осуществлении проверок режимом доступа к программному обеспечению и данным должен быть "только для чтения".
4. При необходимости предоставления режима доступа, отличного от "только для чтения", его необходимо предоставлять к изолированным копиям системных файлов, которые после выполнения аудита должны быть уничтожены.
5. Информационные ресурсы, которые должны пройти проверку, должны быть четко определены и доступны.
6. Требования для специальных или дополнительных процессов должны быть определены и согласованы.
7. Необходим мониторинг и протоколирование всех видов доступа в процессе аудита.
8. Все процедуры, требования и ответственность должны быть задокументированы.

**Часть 2**

**Типовая политика информационной безопасности**

***Пример типовой политики безопасности компании, имеющей выход в Интернет и обладающей ресурсами, к которым необходим доступ из Интернет***

**2.1 Сетевая безопасность**

1. Головной файрвол. Обязателен антивирусный контроль трафика на файрволе (АВП с еженедельным обновлением через Интернет). Файрвол администрируется локально или удаленно (с обязаельным использованием средств шифрования трафика и только из внутренней сети с виртуального фиксированного НАТ адреса администратора).

Из операционной системы на файрволе удаляются все не нужные сервисы и протоколы, ставятся и регулярно обновляются необходимые патчи, создается максимально безопасная конфигурация ОС. Пользователь имеется только один - администратор.

ДОСТУП из Интернет в корпоративную сеть:

- во внутреннюю приватную сеть доступ извне запрещен;
- к файрволу извне доступ запрещен;
- В ДМЗ (демилитаризованная зона) доступ разрешен ТОЛЬКО к следующим портам на объектах (в остальных случаях доступ запрещен):

➢ *Веб-сервер*

- анонимный доступ всем разрешен только к 80 порту;
- разрешен авторизованный FTP-доступ на 21 порт и 20 порт (возможно с предварительной идентификацией / аутенитификацией на файрволе) администратору веб-сервера только из сегмента административного управления (с приватного ИП-адреса администратора);
- из приватной сети, только из сегмента административного управления (с ИП-адреса администратора) возможен удаленный терминальный доступ по протоколу rsh на веб-сервер.

➢ *Мейл-сервер (SMTP and POP3*)

- разрешен доступ только из приватной корпоративной сети к сервису POP3 - 110 порт, исключая учебную подсеть;
- разрешен доступ к SMTP сервису - 25 порт только из приватной сети, исключая учебную подсеть.

Доступ из корпоративной сети в Интернет разрешен без ограничений.

2. Свитч:

- Доступ из учебной сети во всю рабочую сеть (три сегмента) запрещен (но доступ из учебного сегмента в Интернет разрешен);
- Доступ из сети персонала в сети менеджеров и административного управления запрещен.

Свитч выбирается такой, чтобы можно было задавать политику безопасности и запрещать доступ из одного сегмента в другой. Также свитч должен быть по возможности устойчив к ARP-атаке, чтобы такая атака, переполнив ARP-таблицу свитча, не перевела его в режим хаба.

3.Электронная почта. Необходимо обеспечить возможность безопасной отправки - приема почты через корпоративный сервер через Интернет.

Универсальное решение - это ssl- редиректор. Клиент посылает запрос на 110 или 25 порт сервера; попытка установления соединения обнаруживается клиентским редиректором, пропускается через (например) socks с ssl и отправляется на сервер (какой-нибудь другой порт). Там это получает аналогичный редиректор, расшифровывает и перебрасывает на 110 порт.

*Плюсы решения:* стандартные клиент и сервер, не надо писать свои.

*Минусы решения:* клиенту все же надо иметь с собой спец. софт, но это терпимо, если он компактный и не требует настройки.

4. Система обнаружения атак (IDS-Intrusion Detection System).

Можно использовать ISS Real Secure или любую иную программу данного типа (в том случае, если применяется файрвол Check Point, имеющий возможность сопряжения с ISS Real Secure (RS), которая обладает возможностью автоматической реконфигурации данного файрвола в случае обнаружения атаки) или бесплатная юникс программа snort. Располагается на выделенных компьютерах, контролируя входной трафик из Интернет на файрвол и трафик внутри сегментов корпоративной сети.

Консоль управления RS находится в сегменте административного управления (или RS администрируется локально).

5. Контроль содержания трафика.

Для контроля содержимого трафика устанавливается система анализа и контроля трафика типа MIMEsweeper (Baltimore)

6. Протоколирование и регулярный мониторинг доступа.

На межсетевом экране заводится лог-файл, куда записываются все обращения (попытки создания соединений) в корпоративную сеть и из корпоративной сети. Лог файл должен храниться локально и удаленно.

Система обнаружения атак сохраняет информацию об атаках и подозрительной активности в лог-файл. Лог файл должен храниться локально и удаленно.

Веб-сервер сохраняет информацию о его посещении в лог-файл. Лог файл должен храниться локально и удаленно.

Сервер анализа контента сохраняет информацию о нарушениях в лог-файл. Лог файл должен храниться локально и удаленно.

### 2.2 Локальная безопасность (безопасность рабочих станций и серверов)

1. Антивирусный контроль.

Обязательный антивирусный контроль на рабочих станциях. Обязателен автоматический запуск антивирусного монитора и обязательно его автоматическое обновление через Интернет каждую неделю.

2. Защита от НСД.

Необходимо поставить аппаратную систему защиты от НСД, которая должна контролировать и разграничивать доступ к каждой рабочей станции и серверу на аппаратном уровне (при загрузке). Система должна быть:

- ОС-независима и выполнена в виде платы к ЭВМ;
- при загрузке идентификация пользователя должна производиться при помощи смарт карты или электронной «таблетки» и при помощи пароля;
- блокировать доступ в сетап всех рабочих станций и серверов всем пользователям кроме администратора;
- блокировать компьютер, если пользователь покинул свое место (либо по нажатию клавиш, либо по таймауту).

3. Криптографическая защита данных.

Сотрудники компании должны сохранять информацию начиная с уровня «Строго Конфиденциально» (см. положение о уровнях секретности информации) на PGP крипто диске (или на крипто диске иной разработки), разрешенном менеджментом компании.

4. Защита персональным файрволом.

Все рабочие станции и мобильные компьютеры должны быть защищены персональным файрволом.

5. Резервирование данных.

Обязательным является резервирование пользователями важных данных на персональных компьютерах на внутреннем сервере данных компании.

Обязательно наличие бэкап-диска для сервера данных. Бэкап делается либо каждую неделю, либо после серьезных изменений в системе. Необходимо сохранять три цикла генерации бэкапа.

6. Протоколирование доступа

- При локальном доступе пользователя к рабочей станции ведется лог-файл его посещений (протоколируются все удачные и неудачные попытки входа в систему).
- При локальном доступе администратора к серверам ведется лог-файл его посещений (протоколируются все удачные и неудачные попытки входа в систему).

### 2.3 Физическая безопасность

1. Файрвол, веб-сервер, сервера IDS и контроля за трафиком и все сервера данных должны находится в отдельном помещении, доступ в которое разрешен только администраторам, у которых есть ключ или магнитная карта к этой комнате (комната обычно закрыта). Необходимо введение отдельной должности администратора безопасности, и все изменения в системах они будут делать только вдвоем: одна часть пароля администратора имеется у ИТ - администратора, вторая - у администратора безопасности.

2. Помещение должно быть оборудовано принудительной вентиляцией и пожарной защитой (полуавтоматической или автоматической) и, возможно, видео наблюдением за действиями администраторов.

3. Вход в офис компании должен осуществляться только по магнитным картам.

### 2.4 Типовые документы, основанные на стандарте безопасности ISO 17799

#### 2.4.1 Основные требования по обеспечению внутренней ИТ- безопасности компании. Общие положения

- ✓ **Положение о категорировании ресурсов АС**

В компании вводятся следующие уровни категорий секретности информации:

- Общедоступно.
- Конфиденциально.
- Строго Конфиденциально.
- Секретно.

Сотрудникам компании строго запрещается разглашать кому-либо информацию, начиная с уровня «конфиденциально».

Общедоступной информацией является информация, уже опубликованная в средствах массовой информации (в т.ч. на веб-сайте).

Решение о придании статуса «Общедоступно»принимает генеральный или технический директор.

Конфиденциальной информацией в компании является любая внутренняя информация компании.

Строго конфиденциальной информацией в компании является:

- коммерческая информация: тексты договоров и соглашений с партнерами и клиентами, разглашение которых было бы не желательно для компании;
- техническая информация (тексты отчетов, ТЗ, значимые документы, продукты, ключи лицензирования и т.д.).

Решение о придание статуса «Строго Конфиденциально» коммерческой информации принимает генеральный директор.

Решение о придание статуса «Строго Конфиденциально» технической информации принимает технический директор.

Секретной информацией в компании является:

- финансовая информация о деятельности компании;
- особо важная техническая информация.

Решение о придание статуса «Секретно» финансовой информации принимает генеральный директор.

Решение о придание статуса «Секретно» технической информации принимает технический директор.

- ***Положение о категорировании пользователей АС***

В АС вводятся следующие категории пользователей:

- Администраторы. В нее входят администраторы ИТ и безопасности. Администраторы имеют полный доступ к ресурсам АС для ее администрирования.

- Топ-менеджеры. В группу входят президент компании, ген. директор, тех. Директор.
- Сотрудники. В группу входят все сотрудники компании.
- Студенты. В группу входят студенты семинаров.

Член соответствующей группы может получить доступ к информации более высокого уровня секретности только с письменного разрешения уполномоченного лица группы Топ-менеджеры.

### ✓ Порядок обращения с информацией, подлежащей защите

Должны быть четко описаны и классифицированы следующие действия с информацией:

1. копирование;
2. хранение;
3. передача почтой, факсом, е-мейлом;
4. передача голосом, включая мобильные телефоны, голосовую почту;
5. уничтожение.

Информация уровня «общедоступно». Доступ, копирование и любая передача информации данного уровня не ограничены. Уничтожение информации возможно только ее владельцем.

Информация уровня «конфиденциально». Подлежит защите от НСД средствами разграничения доступа.

Доступ к данной информации может осуществляться сотрудниками компании локально и удаленно. Удаленный доступ из корпоративной сети осуществляется без применения средств шифрования трафика. Удаленный доступ из Интернет осуществляется с применением средств шифрования трафика.

Доступ к информации уровня «конфиденциально» осуществляется категориями пользователей: Администраторы, Топ-менеджеры, Сотрудники.

Копирование и любая передача информации данного уровня ограничены периметром компании. Уничтожение информации возможно только ее владельцем.

Информация уровня «строго конфиденциально». Подлежит защите от НСД средствами разграничения доступа и криптографической защите.

Удаленный доступ из корпоративной сети осуществляется с применением средств шифрования трафика. Удаленный доступ сотрудников из Интернет осуществляется с применением средств шифрования трафика.

Копирование и любая передача информации данного уровня возможно только в пределах компании и только авторизованным персонам. Уничтожение информации возможно только ее владельцем.

Право на удаление информации уровня «строго конфиденциально» имеет только администратор безопасности вместе с ИТ-администратором администратором (root пароль разделен на две части между ними) с разрешения тех. директора.

Доступ к информации уровня «строго конфиденциально» осуществляется категориями пользователей: Топ-менеджеры, Сотрудники (с разрешения тех. директора)

Информация уровня «секретно». Подлежит защите от НСД, криптографической защите и обязательному протоколированию доступа.

Удаленный доступ из корпоративной сети осуществляется с применением средств шифрования трафика. Удаленный доступ из Интернет запрещен.

Копирование и любая передача информации данного уровня возможно только в пределах компании и только авторизованным персонам.

Уничтожение информации возможно только ее владельцем.

Право на удаление информации уровня «секретно» имеет только администратор безопасности вместе с ИТ-администратором администратором (root пароль разделен на две части между ними) с разрешения тех. директора.

Доступ к информации уровня «строго конфиденциально» осуществляется категориями пользователей: Топ-менеджеры.

### 2.4.2 Основные правила, инструкции и требования по обеспечению внутренней ИТ-безопасности компании

#### ✓ Правила парольной защиты

1. Длина паролей должна быть не менее 8 символов.
2. Пароль обязательно должен содержать любую комбинацию минимум из двух следующих групп: маленьких букв, больших букв, цифр и специальных символов.
3. СТРОГО запрещается:

- использовать в качестве пароля свои имя, фамилию, дату рождения, имена родственников, кличку собаки и т.п., равно как и обычные слова;
- использовать в качестве пароля русское слово, введенное, когда клавиатура находится в латинском регистре;
- где-либо записывать пароль;

- разглашать свои персональные пароли доступа.

4. Пароли обязаны меняться каждый год.

5. 16-байтовый административный пароль уровня ROOT разделен на две части (по 8 байт каждая). Каждая часть находится соответственно у администратора безопасности и ИТ-администратора.

6. Обязательно применение индивидуальных паролей (если необходимо, то возможно применение групповых паролей, но это обычно не рекомендуется).

7. Необходимо позволять пользователям выбирать и менять свой пароль и предусмотреть процедуры контроля ошибок пи вводе пароля.

8. В случае, если пользователь сам создает пароль, то необходимо предусмотреть его автоматическое изменение после первого же входа в систему.

9. Записывать при смене все старые паролей пользователей (например, за предыдущие 12 месяцев), чтобы предотвратить их повторное использование.

10. Не выдавать на дисплей пароль при вводе.

11. Хранить файл с паролями отдельно от системных приложений.

12. Хранить файл с паролями в зашифрованном виде, используя стойкие алгоритмы шифрования.

### ✓ Правила защиты от вирусов и злонамеренного программного обеспечения

1. Обязательное применение лицензионного ПО и запрет на использование несанкционированно установленного ПО.

2. Обязательно централизованное еженедельное обновление антивирусных баз данных на рабочих станциях и сервере. Обеспечение регулярного сканирования и постоянного мониторинга.

3. Обязательная проверка всех приходящих в систему файлов на вирусы.

4. Регулярный анализ ПО и данных в системах, занимающихся обработкой критичных данных. Наличие несоответствующих файлов должно быть расследовано.

5. СТРОГО запрещается (за исключением крайних случаев зависания компьютера) выключать антивирусные мониторы на рабочих станциях и серверах.

6. В случае необходимости временного отключения антивирусного монитора пользователю необходимо получить разрешение у администратора безопасности и сообщить об этом ИТ-администратору. ИТ-администратор должен принять немедленные меры по запуску антивирусного монитора.

7. При выключенном антивирусном мониторе, СТРОГО запрещается запуск, открытие, пересылка вновь внесенных в систему документов (в формате ворд, эксель и др.) и исполняемых файлов.

8. Наличие плана по восстановлению непрерывности бизнеса после вирусных атак, включая бек-апы софта и данных.

✓ ***Требования по контролю за физическим доступом***

1. Посетители безопасного периметра должны контролироваться и их время и дата посещения и выхода должны быть запротоколированы. Посетители должны получать доступ только в соответствии с необходимостью и должны быть ознакомлены с инструкциями по безопасности и по действиям в аварийных ситуациях.

2. Доступ к секретной информации и средствам ее обработки должен контролироваться и быть только авторизованным. Должны применяться средства аутентификации (например, смарт-карты). Вся информация о доступе в систему должна протоколироваться.

3. Персонал должен носить хорошо видимые идентификаторы и должен оповещать службу безопасности обо всех обнаруженных незнакомцах без идентификаторов.

4. Права доступа должны подвергаться регулярному анализу и обновлению.

✓ ***Требования по физической защите оборудования***

1. Оборудование должно располагаться с учетом требования минимизации доступа в рабочее помещение лиц, не связанных с обслуживанием этого оборудования.

2. Системы обработки и хранения информации, содержащие важные данные, должны быть расположены так, чтобы минимизировать возможность случайного или преднамеренного доступа к ним неуполномоченных лиц в процессе их обработки.

3. Объекты, требующие специальной защиты, должны быть изолированы.

4. Меры защиты должны быть приняты для минимизации следующих потенциальных угроз:

- кража;
- гонь;
- взрыв;
- дым;
- вода;
- пыль;

- химические вещества;
- побочные электромагнитные излучения и наводки.

5. Политика компании должна запрещать прием пищи, напитков и курение вблизи оборудования.

6. Оборудование должно подвергаться регулярным осмотрам и дистанционному контролю с целью обнаружения признаков, которые могут повлечь за собой отказ системы.

7. Использование специальных средств защиты, таких как накладка на клавиатуру, необходимых в случае расположения оборудования в промышленных зонах.

8. Должны быть учтены воздействия от происшествий на соседних объектах (пожар у соседей, наводнение или затопление верхнего этажа, взрыв на улице и т.д.)

✓ Инструкция по безопасному уничтожению информации или оборудования

1. Устройства хранения информации, содержащие ценную информацию, при списывании должны быть физически уничтожены или должна быть осуществлена безопасная (многократная или на физическом уровне) перезапись информации.

2. 2. Все оборудование, включая медианосители (жесткие диски, например), должно быть проверено на предмет того, что важная информация или лицензионное ПО уничтожены перед списанием.

3. Поврежденные устройства хранения, содержащие важную информацию, должны подвергнуться анализу на предмет того, уничтожить ли данное устройство, восстановить или отказаться от него.

✓ **Инструкция по безопасности рабочего места (документов на рабочем столе и на экране монитора)**

1. Документы на всех видах носителей и вычислительная техника, в случае если ими не пользуются, а также в нерабочее время, должны храниться в запираемом помещении.

2. Ценная информация, когда она не используется, должна храниться в защищенном месте (огнеупорный сейф, выделенное помещение).

3. Персональные компьютеры, терминалы и принтеры не должны оставаться без присмотра во время обработки информации и должны защищаться блокираторами клавиатуры, паролями или иными методами на время отсутствия пользователя.

4. Должны быть приняты надежные меры, исключающие несанкционированное использование копировальной техники в нерабочее время.

5. Распечатки, содержащие ценную (конфиденциальную) информацию должны изыматься из печатающего устройства немедленно.

✓ ***Правила осуществления удаленного доступа***

1. Пользователи и администраторы имеют право неограниченного доступа из корпоративной сети в Интернет только согласно своим служебным обязанностям.
2. Пользователи и администраторы имеют право доступа из корпоративной сети к ресурсам корпоративной сети только согласно своим служебным обязанностям.
3. Персоналу СТРОГО запрещается:

- сканирование и попытки атак внутренних ресурсов корпоративной сети и ресурсов в сети Интернет ;
- сообщать кому-либо свои идентификаторы и пароли доступа к корпоративным ресурсам.

ВСЕМУ ПЕРСОНАЛУ, ВКЛЮЧАЯ ТОП-МЕНЕДЖЕРОВ, СТРОГО ЗАПРЕЩЕНО:

1. Устанавливать модемы на рабочих местах без получения разрешения у администратора безопасности и одобрения технического директора.
2. Осуществлять удаленный доступ к корпоративной сети из Интернет без использования шифрования трафика или в обход разработанной в данном документе схем и правил.

✓ Правила осуществления локального доступа

1. Все пользователи осуществляют доступ к выделенным им при поступлении на работу персональным компьютерам.
2. Пользователи и администраторы должны, уходя со своего рабочего места, блокировать доступ к своему рабочему компьютеру.
3. Обязательно соответствующее завершение сессии на серверах по ее окончании (а не просто выключать компьютеры или терминалы).
4. Пользователям и администраторам СТРОГО запрещается:

- выключать антивирусные мониторы и персональные файрволы без разрешения администратора безопасности;
- сообщать кому-либо свои идентификаторы и передавать электронные ключи доступа к персональным компьютерам;
- осуществлять доступ к персоналкам других пользователей или к серверам;

- пытаться осуществлять несанкционированный доступ к любым объектам корпоративной сети.

✓ ***Требования резервного сохранения информации***

1. Резервные копии вместе с инструкциями по восстановлению должны храниться в месте, территориально отдаленном от основной копии информации. Для особо важной информации необходимо сохранять три последних копии.

2. К резервным копиям должен быть применен адекватный ряд физических и организационных мер защиты, соответствующий стандартам, принятым для используемых носителей.

3. Носители, на которые осуществляется резервное копирование, должны регулярно проверяться на отсутствие сбоев.

4. Регулярная проверка процедур восстановления и практический тренинг персонала с целью поддержания возможности восстановления данных в установленном порядке и за гарантированный промежуток времени.

✓ Требования мониторинга и ведения диагностических лог файлов

1. Запись действий операторов:

- время старта и остановки системы;
- системные ошибки и действия по их исправлению;
- подтверждение корректного обращения с входными и выходными данными;
- идентификатор оператора, совершившего действие, которое повлекло запись в журнал регистрации.

2. Ведение лога системных сбоев:

- анализ журнала системных сбоев на предмет корректности и завершенности процесса устранения последствий сбоев;
- анализ произведенных действий на предмет соответствия установленным процедурам

✓ ***Требование мониторинга доступа и использования систем и ведения лог файлов***

1. Лог событий должен включать:

- идентификатор пользователя;

- дата и время входа и выхода;
- идентификатор терминала или сетевого адреса, если это возможно;
- запись об успешных или неудачных попытках входа в систему;
- запись об успешных или неудачных попытках получения доступа к данным и иным ресурсам.

2. Обязателен периодический анализ лога.
3. Места повышенного риска:

➢ фиксация в журнале данных о доступе, включая:

- идентификатор пользователя;
- дата и время важных (ключевых) событий;
- тип события;
- затребованные файлы;
- использованные программы и утилиты.

➢ фиксация в журнале всех привилегированных операций, таких как:

- вход с правами суперпользователя (администратора);
- старт и остановка системы;
- присоединение устройств ввода-вывода.

➢ фиксация в журнале всех попыток неавторизованного доступа, таких как:

- неудачные попытки;
- нарушения правил политик доступа и уведомления на межсетевой экран;
- тревоги от систем обнаружения вторжений.

➢ фиксация в журнале всех системных предупреждений и неисправностей таких как:

- консольные уведомления или тревожные сообщения;
- сбои при ведении системного журнала;
- тревожные сообщения при сбоях в сетевом управлении.

✓ ***Требования при обращении с носителями данных***

1. Носители должны контролироваться и быть защищены.
2. Управление съемными носителями:

- все носители, срок эксплуатации которых истек, должны быть уничтожены в установленном порядке;
- для выноса носителей за пределы организации, должно быть получено специальное разрешение; факт выноса должен быть зафиксирован в специальном журнале (базе данных);

- все носители должны храниться в безопасном месте в соответствии с требованиями компании-производителя.

3. Хранение и обращение с носителями:

➢ Хранение в безопасном месте.

➢ Следующие носители и информация требуют повышенной безопасности при хранении:

- бумажные документы;
- записи на кассетах;
- копировальная бумага;
- отчеты;
- картриджи;
- магнитные ленты;
- съемные диски или кассеты;
- оптические носители;
- листинги программ;
- тестовые данные;
- системная документация.

✓ ***Требования по неэлектронному информационному обмену***

Необходима разработанная политика безопасности, связанная с передачей информации голосом, факсом и видео.

Всему персоналу необходимо:

1. Соблюдать меры предосторожности при телефонных звонках:

- близость иных людей при звонках по мобильным телефонам;
- перехват звонков при физическом доступе к линии;
- люди, находящиеся рядом с абонентом, принимающим звонок.

2 Не проводить конфиденциальные переговоры в общественных местах или открытых офисах или офисах с тонкими стенами.

3. Не оставлять приватных сообщений на автоответчиках.

4. Учитывать следующие проблемы с факсами:

- неавторизованный доступ к месту получения сообщений;
- запланированное или случайное программирование факса для посылки сообщений по определенным номерам;
- посылка сообщений по неверным номерам.

✓ ***Требования при регистрации пользователей***

1. Использовать уникальный идентификатор пользователя, по которому его можно однозначно идентифицировать. Применение групповых идентификаторов может быть разрешено только там, где это требуется для выполнения работы.
2. Проверка, что пользователь авторизован ответственным за систему для работы с ней. Возможно получение отдельного разрешения для наделения правами пользователя у руководства.
3. Проверка, что уровень доступа соответствует бизнес задачам политике безопасности организации и не противоречит распределению обязанностей (ответственности).
4. Документальная фиксация назначенных пользователю прав доступа.
5. Ознакомление пользователя под роспись с предоставленными правами доступа и порядком его осуществления.
6. Все сервисы должны разрешать доступ только аутентифицированным пользователям.
7. Обеспечение формального списка всех пользователей, зарегистрированных для работы в системе.
8. Немедленное исправление (удаление) прав доступа при изменении должностных обязанностей (увольнении).
9. Периодический контроль и удаление не используемых учетных записей.
10. Обеспечение недоступности запасных идентификаторов другим пользователям.

✓ Требования по проверке прав пользователей

Необходима периодическая проверка прав пользователей.

1. Проверка прав пользователей должна проводиться регулярно (каждые 6 месяцев) или после каждого изменения в системе.
2. Проверка прав пользователей, имеющих особые привилегии для доступа в систему должна проводиться чаще - каждые 3 месяца.
3. Необходимо регулярно проверять адекватность назначенных привилегий, во избежание получения кем-либо из пользователей излишних прав.

✓ Требования по контролю доступа в операционную систему

Необходимо обеспечить:

1. Идентификацию и аутентификацию пользователя, а при необходимости и идентификацию оборудования (сетевой адрес, номер терминала и т.п.), с которого осуществляется доступ.

2. Запись успешных и неудачных попыток входа.

3. Использование качественных паролей, если применяется парольная система аутентификации.

4. При необходимости ограничить временные рамки доступа пользователя в систему и число одновременных подключений.

- ✓ **Требование к процедуре входа в систему (log on)**

Процедура должна:

1. Не выдавать информации о типе и версии системы или приложения ("системных баннеров") до успешного завершения процедур идентификации и аутентификации.

2. Выдавать предупреждение, что вход в систему разрешен только авторизованным пользователям.

3. Не выдавать подсказок и справочной информации, чтобы усложнить проникновение в систему неавторизованному пользователю.

4. Проверка введенной информации осуществлять только после полного ее ввода. В случае обнаружения ошибки система не должна уточнять, какие именно данные введены неправильно.

5. Ограничивать число неудачных попыток входа. При этом каждая итерация должна включать:

- Запись неудачной попытки входа.
- Временную задержку перед следующей попыткой входа в систему или блокирование всех дальнейших попыток входа без дополнительной авторизации (как с введением ПИН кода в мобильном телефоне).
- Отсоединение.

6. Контролировать ограничения по времени, заданные для пользователя, и отказывать в доступе при их нарушении.

7. После успешного входа пользователя в систему информировать его:

- О дате и времени предыдущего входа в систему.
- О любых неуспешных попытках входа, произошедших с момента последней успешной регистрации.

✓ **Правила использования системных утилит**

1. Применять процесс аутентификации при использовании системных утилит.
2. Раздельно хранить системные утилиты и приложения.
3. Ограничить использование системных утилит минимально возможному числу доверенных авторизованных пользователей.
4. Специальная авторизация при использовании системных утилит.
5. Ограничение доступности системных утилит.
6. Протоколирование использования системных утилит.
7. Определение и документирование способа авторизации для запуска системных утилит.
8. Удаление всех системных утилит, использовании которых в данной системе не является необходимым.

✓ Правила удаленной работы мобильных пользователей

Для этой категории пользователей необходимы отдельные требования и нормативные документы по физической защите, разграничению доступа, криптографической защите, бэк-апу, антивирусной защите. Также необходима политика, которая бы определяла бы правила доступа к корпоративной сети и отдельная документ, по правилам осуществления доступа в корпоративную сеть из общественных мест и сетей.

Компания может разрешить удаленную работу пользователей только, если будут обеспечены соответствующие требования:

1. Обеспечение физической защиты места удаленной работы, включая физическую безопасность здания или ближайшего окружения.

2. Обеспечение безопасности телекоммуникаций, учитывающее необходимость удаленного доступа к внутренним ресурсам компании; важность информации и систем, к которым будет осуществлен удаленный доступ; прохождение через каналы связи.

3. Учет возможной угрозы неавторизованного доступа к информации или ресурсам, от иных близких к удаленному пользователю людей, например, семья, друзья.

Следующие требования должны быть предусмотрены:

1. Обеспечение необходимым оборудованием для удаленного мобильного доступа.
2. Определение разрешенных видов работ, разрешенного времени доступа, классификация информации, которая может обрабатываться удаленно, определение систем и сервисов, к которым данному мобильному пользователю разрешен удаленный доступ.

3. Обеспечение необходимым коммуникационным оборудованием, включая средства обеспечения безопасности

4. Физическая безопасность.

5. Правила доступа к оборудованию и информации для членов семьи и посетителей.

6. Обеспечение программным обеспечением и оборудованием.

7. Наличие процедур резервного копирования и обеспечения непрерывности ведения бизнеса.

8. Аудит и мониторинг безопасности.

9. Аннулирование разрешения, прав доступа и возврат оборудования при отмене (завершении) удаленного мобильного доступа.

✓ Требование распределения ответственности при обеспечении безопасности

Необходимо назначение менеджера, который отвечает за обеспечение безопасности в целом, и менеджеров, которые отвечают за безопасность каждой конкретной системы.

Возможна передача ответственности владельцами ресурса отдельным менеджерам или сервис провайдерам, но, тем не менее, полная ответственность лежит на владельцах системы.

Зона ответственности каждого менеджера должна быть четко определена:

1. Определение ресурсов, имеющих отношение к информационной безопасности, по каждой системе.

2. Для каждого ресурса (или процесса) должен быть назначен ответственный сотрудник из числа руководителей. Разграничение ответственности должно быть закреплено документально.

3. Для каждого ресурса должен быть определен и закреплен документально список прав доступа (матрица доступа).

✓ **Правила безопасности при выборе персонала**

1. Необходимо включить задачу обеспечения безопасность в служебные обязанности сотрудников.

2. Проверка персонала при приеме на работу:

- проверка рекомендаций;
- проверка CV;
- подтверждение ученых степеней и образования;
- идентификация личности.

3. Заключение соглашений о конфиденциальности с персоналом.
4. Условия работы персонала.
5. Пример типового соглашения банка с персоналом:

Вся информация, находящаяся на электронных носителях рабочих станций и в вычислительных сетях банка, является собственностью банка.

Подразделения и лица, уполномоченные на то Правлением, Председателем Правления, имеют право в установленном порядке, без уведомления пользователей, производить проверки соблюдения требований настоящей Инструкции, а также осуществлять контроль за данными, находящимися на электронных носителях. В целях осуществления указанных действий они могут получить доступ к любым данным пользователей, находящихся на электронных носителях рабочих станций и в Сети, а пользователь обязан предоставить требуемую ими информацию.

Банк имеет право без согласия пользователя передавать информацию, хранящуюся на электронных носителях, третьим лицам, включая правоохранительные органы и иные организации, уполномоченные на это действующим законодательством.

Любые компоненты Сети могут использоваться пользователями только для выполнения своих служебных обязанностей.

Использование компонентов Сети не по назначению, использование, нарушающее требования настоящей Инструкции, приказов и распоряжений руководства банка (Председателя Правления, заместителей Председателя Правления, руководителей подразделений), а также такое использование, которое наносит вред банку, может повлечь за собой дисциплинарные взыскания, включая увольнение.

- ✓ ***Требования контроля оперативных изменений***

1. Идентификация и запись важных изменений.
2. Оценка потенциального последствий таких изменений.
3. Формальное утверждение процедуры внесения изменений.
4. Взаимодействие со всеми заинтересованными лицами при внесении изменений
5. Процедуры определения ответственности и возврата в исходное состояние при неудачных попытках изменений.

- ✓ **Требования проверки входных данных**

Необходимы следующие поверки:

1. Проверка входных данных на следующие ошибки:

- превышение размерности значения;
- недопустимые символы во входном потоке;
- отсутствующие или неполные данные;
- объем входных данных выше или ниже нормы;
- запрещенные или неверные управляющие значения.

2. Периодическая проверка целостности и правильности содержимого ключевых полей или файлов данных.

3. Проверка твердых копий входных документов на любые запрещенные (несанкционированные) изменения.

4. Процедуры реагирования на подтвержденные ошибки.

5. Процедуры проверки достоверности входных данных.

6. Определение ответственности для всего персонала, вовлеченного в процесс обработки и ввода исходных данных.

✓ Требования к применению криптографических средств управления

**1. Необходима разработанная политика использования криптографических средств.**

При разработке политики необходимо учесть:

1. Управленческий подход к использованию СКЗИ внутри организации, включая основные принципы, какие именно классы информации должны быть защищены.

2. Политика управления ключами, включая методы для восстановления зашифрованной информации в случае утери, компрометации или уничтожения ключей.

3. Распределение обязанностей: кто и за что несет ответственность.

4. Внедрение политики.

5. Управление ключами.

6. Порядок определения адекватного уровня криптографической защиты.

7. Стандарты, которые могут быть внедрены и адаптированы в организации (какие решения подходят для каких бизнес процессов).

2. Стандарты, процедуры, методы.

1. Генерация ключей для разных криптосистем и разных приложений.

2. Генерация и получение открытых ключей.

3. Выдача ключей пользователям, включая процедуру активации ключа после его получения.

4. Хранение ключей, включая порядок получения авторизованными пользователями доступа к ключам .

5. Порядок смены ключей.

6. Действия в случае компрометации ключей.

7. Отзыв ключей, включая порядок их деактивации при компрометации или увольнении ответственного за них сотрудника, а также определение случаев, когда эти ключи должны быть сохранены.

8. Восстановление поврежденных или утерянных ключей (как часть управления непрерывностью бизнеса).

9. Архивирование и резервное копирование ключей.

10. Уничтожение ключей.

11. Протоколирование всех действий, связанных с управлением ключами.

12. Ограничение срока действия ключей.

✓ ***Требования по контролю программ операционной системы***

1. Обновление библиотек должно выполняться только с разрешения руководства.

2. Если возможно, ОС должна содержать только исполняемые файлы.

3. Исполняемые файлы и изменения библиотек не должны внедряться в ОС до подтверждения их успешного тестирования, а также информирования и обучения пользователей (если в этом нет острой необходимости).

4. После всех изменений в библиотеках должна быть обеспечена проверка всех регистрационных журналов.

5. Предыдущие версии должны быть сохранены для непредвиденных случаев.

✓ Требования по контролю доступа к исходным текстам программ и библиотек

1. Где возможно, исходные тексты программ не должны содержаться в ОС.

2. Для каждого приложения должен быть назначен ответственный сотрудник, отвечающий за контроль исполняемых модулей.

3. Персонал из службы поддержки не должен иметь неограниченный доступ к исходным текстам программ и библиотек.

4. Изменения и дополнения в исходные тексты программ и библиотек, а также передача исходных текстов программистам должна осуществляться только вместе с библиотеками и по разрешению менеджера поддержки данного приложения.

5. Листинги программ должны храниться в безопасном месте

6. Все попытки осуществления доступа к исходным текстам должны протоколироваться.

7. Старые версии исходных текстов программ должны быть заархивированы, с отметкой времени и даты и вместе со всем сопутствующим программным обеспечением, процедурами, описаниями и т.д.

8. Поддержка и копирование исходных текстов библиотек и программ должны быть предметом процедур контроля изменений.

- ✓ **Требования контроля вносимых изменений**

1. Документальное закрепление типовых уровней доступа.

2. Обеспечение, того, что изменения сделаны авторизованными пользователями.

3. Идентификация всего программного обеспечения, информации, баз данных, аппаратного обеспечения, которое требует изменений.

4. Получение формального разрешения для детализации предложений до начала работ.

5. Обеспечение того, что авторизованные пользователи принимают (проверяют) изменения до их внедрения.

6. Обеспечение безопасного внедрения изменений без последствий для бизнеса.

7. Обеспечение изменений системной документации после каждой модификации, а также архивация старой документации или ее отклонение.

8. Обеспечение контроля версий для всех обновлений программного обеспечения.

9. Обеспечение протоколирования всех запросов на изменение.

10. Обеспечение соответствующих изменений оперативной и пользовательской документации.

11. Обеспечение того, что внедрение изменений имело место в соответствующее время и не затронуло вовлеченные в процесс бизнес процессы.

**После внесения изменений в ОС необходимо осуществить:**

1. Анализ важных приложений и целостности процедур (необходимо убедиться в их работоспособности).

2. Убедиться, что годовой план поддержки систем и бюджет покроет расходы на анализ и тестирование систем после изменений ОС.

3. Убедиться, что уведомление об изменениях в ОС пришло вовремя, что позволило сделать необходимый анализ перед внедрением изменений.

4. Убедиться, что соответствующие изменения внесены в планы обеспечения непрерывности бизнеса.

Ограничения на изменения прикладного ПО

1. Не проводить без существенной необходимости.

2. В случае если необходимо, требуется учесть:

- риск возможной компрометации встроенных процессов управления и целостности процессов;
- получить согласие поставщика;
- возможность получить от поставщика стандартные файлы с обновлениями;
- последствия самостоятельного внесения изменений в программное обеспечения (отказ производителя от сопровождения).

*Скрытые каналы и Троянский код*

Необходимо:

1. Источники получения программ должны быть проверены и обладать соответствующей репутацией.

2. Покупая программы с исходным кодом, убедиться, что верификация кода возможна.

3. Применять качественные продукты.

4. Проверять весь исходный код.

5. Контролировать доступ и возможность модификации уже инсталлированного кода.

6. Использовать только проверенный персонал для работы на ключевых особо важных системах.

✓ ***Требование обеспечения непрерывности бизнеса:***

Аспекты управления непрерывного ведения бизнеса

1. Последствия неисправностей, секьюрити инцидентов, отказов сервисов должны быть расследованы.

2. План на случай непредвиденных обстоятельств должен быть разработан и внедрен, чтобы бизнес процессы были вновь запущены в установленное время.

**Процесс управления непрерывного ведения бизнеса**

1. Осознание рисков, их вероятностей, возможных последствий, включая идентификацию и расстановку приоритетов для критичных бизнес процессов.

2. Осознание ущерба в случае прерывания бизнеса и создание бизнес целей для информационно-обрабатывающей системы компании.

3. Выбор подходящей схемы страхования, которая может являться одной из форм поддержки непрерывности ведения бизнеса.

4. Формализация и документирование стратегии ведения непрерывного бизнеса, содержащей согласованные цели бизнеса и приоритеты.

5. Регулярное тестирование и обновление планов и процессов.

6. Необходимо убедиться, что управление непрерывным ведением бизнеса внедрено в организационные процессы и структуру компании. Ответственность для координации управления непрерывным ведением бизнеса должна быть распространена по соответствующим уровням внутри организации, так называемый форум по информационной безопасности.

Непрерывность бизнеса и анализ воздействий

Требуется выяснить, что может послужить причиной прерывания бизнес процессов (сбой оборудования, пожар, наводнение).

Основываясь на анализе необходимо разработать соответствующий стратегический план и подходы для обеспечения непрерывности бизнеса.

***Создание и внедрение плана непрерывности бизнеса***

1. Распределение ответственности и определение всех контр аварийных процедур (порядок действий в аварийной ситуации).

2. Внедрение контр аварийных процедур для восстановления систем в отведенный период времени. Особое внимание уделяется оценке зависимости бизнеса от внешних связей.

3. Документирование всех процессов и процедур.

4. Соответствующее обучение персонала порядку действий в аварийных ситуациях включая управление в кризисных процессах.

5. Тестирование и обновление планов.

Основы планирования непрерывности бизнеса

1. Условия вступления в действие планов (как оценить ситуацию, кто в нее вовлечен).

2. Контр аварийные процедуры, описывающие действия в случае инцидентов, представляющих опасность для бизнес операций или/и человеческой жизни. Процедуры должны включать в себя мероприятия по связям с общественностью и органами власти.

3. Процедуры нейтрализации неисправностей, в которых описываются действия по выведению жизненно важных бизнес нужд или служб поддержки во временное альтернативное помещение и возвращение их в соответствующий период времени.

4. Процедуры восстановления, в которых описаны действия по возвращению к нормальному процессу бизнес операций.

5. Разработка программы, в которой описаны, как и когда план будет протестирован и процесс внедрения этого плана.

6. Действия по информированию и обучению, которые разрабатываются для понимания персоналом процесса обеспечения непрерывности бизнеса и гарантии, что этот процесс продолжает быть эффективным.

7. Личная ответственность - кто именно отвечает за выполнение каждого компонента плана, с указанием дублирующих лиц.

**Тестирование, обеспечение и переоценка плана обеспечения непрерывности бизнеса**

Тестирование:

1. Базовые тесты различных сценариев (обсуждение мероприятий по восстановлению бизнеса в случае различных ситуаций).

2. Моделирование (практический тренинг персонала по действиям в критичной ситуации).

3. Тестирование технических мероприятий по восстановлению (для гарантии того, что информационная система будет эффективно восстановлена).

4. Тестирование технических мероприятий по восстановлению в альтернативном месте (запуск бизнес процессов вместе с восстановительными мероприятиями вне основного места расположения).

5. Тесты систем и поставщиков услуг (гарантия, что внешние предоставляемые сервисы и продукты будут соответствовать контрактным обязательствам).

6. Комплексные учения (тестирование того, что компания, персонал, оборудование, информационная система могут справиться с нештатной ситуацией).

- ✓ Обеспечение и переоценка планов

Примеры ситуаций, когда требуется изменение планов, в случае обновления ОС, покупки нового оборудования и изменений в:

- персонале;
- адресах или телефонных номерах;
- стратегии бизнеса;

- местоположении и информационных ресурсах;
- законодательстве;
- подрядчиках, поставщиках и ключевых заказчиках;
- процессах при добавлении новых или снятии старых;
- рисков (операционных и финансовых).

✓ ***Требования соблюдения авторского права на программное обеспечение***

1. Разработка и внедрение политики соблюдения авторского права на программное обеспечение, где определяется легальное использование ПО и информационных продуктов.
2. Выпуск стандартов для процедур приобретения программного обеспечения.
3. Обеспечение осведомленности пользователей об авторских правах на программное обеспечение, правилах приобретения программного обеспечения и уведомление пользователей, что в случае нарушения будут предприняты дисциплинарные действия.
4. Обеспечение возможности доказательства, что данное программное обеспечение лицензионно (лицензии и т.д.).
5. Контроль того, что максимальное число пользователей в лицензии не превышено.
6. Выполнение проверок, что только разрешенные и лицензионные продукты инсталлированы.
7. Разработка политики для обеспечения соответствующих условий лицензионного соглашения.
8. Разработка политики для размещения или передачи программного обеспечения сторонним лицам или компаниям.
9. Применение соответствующих средств аудита.
10. Соблюдение условий для программного обеспечения и информации, полученных из открытых сетей.

✓ **Требования обеспечения сохранности улик (свидетельств, доказательств)**

**Правила обращения с уликами**

1. Степень допустимости улики: когда и при каких условиях она может быть использована в суде в качестве доказательства.
2. Вес улики: качество и полнота улики.
3. Адекватность улики. Подсистема регистрации работает корректно и непрерывно; осуществляется запись всей информации; в любой момент можно получить необходимые сведения (улику) из регистрационных журналов.

**Степень допустимости улики**

Для этого необходимо гарантировать, что ИТ система организации соответствует любому опубликованному стандарту безопасности.

**Качество и полнота улики**

Для гарантии качества и полноты улики необходимо обеспечить подлинность улики:

1. Для бумажных документов: обеспечена безопасность хранения оригинала, ведется запись кто, где и когда нашел его и кто был свидетелем обнаружения. Расследование должно показать, что оригинал не был изменен.

2. Для информации в электронной форме: гарантия доступности должна быть обеспечена путем создания копий любых съемных носителей, информации на жестких дисках и в оперативной памяти. Все действия в процессе копирования должны быть запротоколированы и засвидетельствованы. Одна копия носителя и протокола должна храниться в безопасном месте.

✓ **Требования по управлению системным аудитом**

1. Требования аудита должны быть согласованы с соответствующими руководителями.
2. Масштаб проверок должен быть согласован и подконтролен.
3. При осуществлении проверок режимом доступа к программному обеспечению а данным должен быть "только для чтения".
4. При необходимости предоставления режима доступа, отличного от "только для чтения", его необходимо предоставлять к изолированным копиям системных файлов, которые после выполнения аудита должны быть уничтожены.
5. Информационные ресурсы, которые должны пройти проверку, должны быть четко определены и доступны.
6. Требования для специальных или дополнительных процессов должны быть определены и согласованы.
7. Необходим мониторинг и протоколирование всех видов доступа в процессе аудита.
8. Все процедуры, требования и ответственность должны быть задокументированы.

✓ **Инструкции:**

**1. По приему на работу и допуску новых сотрудников к работе в АС и наделения их необходимыми полномочиями по доступу к ресурсам системы**

При приеме на работу нового сотрудника администратор безопасности обязан ознакомить пользователя с политикой безопасности компании и необходимыми нормативными документами и инструкциями. После чего проводится инструктаж сотрудника и проверка его знаний.

Сотруднику администратором безопасности присваивается соответствующий идентификатор для доступа в систему. Пароль сотрудник придумывает самостоятельно (в соответствии с правилами парольной защиты) и вводит его в систему. Пароль сотрудника известен только ему лично и не сообщается никому. Уровень доступа к информации сотруднику назначается топ-менеджерами (генеральным директором или техническим директором).

В соответствии с распоряжением топ-менеджеров сотруднику может быть предоставлен доступ на чтение к части информации уровня выше чем конфиденциально.

Администратор безопасности подчиняется шефу службы безопасности, который подчиняется техническому директору. В случае отсутствия шефа службы безопасности, администратор безопасности подчиняется напрямую генеральному или техническому директору.

Администратор ИТ подчиняется ИТ-менеджеру, который подчиняется техническому директору. В случае отсутствия ИТ-менеджера, ИТ-администратор подчиняется техническому директору.

**2. По увольнению работников и лишения их прав доступа в систему**

В случае увольнения сотрудника, в последний день его работы (до получения им выходного пособия) производятся следующие действия:

1. Идентификатор и пароль сотрудника удаляются из системы.
2. Электронные ключи доступа сдаются сотрудником администратору безопасности. Возможность доступ по старым ключам блокируется.
3. Администратор безопасности вместе с ИТ-администратором анализирует рабочее место на наличие закладок, вирусов и т.д., после чего затем все данные на винчестере сотрудника уничтожаются и ОС на рабочем месте переинсталлируются.
4. Администратор безопасности анализирует все данные, к которым имел доступ сотрудник на предмет их зараженности вирусами.
5. Администратор безопасности вместе с непосредственным руководителем сотрудника анализирует целостность данных, к которым имел доступ сотрудник.
6. В случае обнаружения неправомерных действий сотрудника (удалении информации, внесения в систему закладок и вирусов) информация докладывается шефу службы безопасности или техническому директору и согласно контракту сотрудник

увольняется без выходного пособия и решается вопрос о возбуждении против сотрудника уголовного дела по факту нанесения ущерба компании.

В случае увольнения администратора (безопасности или ИТ) в последний день его работы (до получения им выходного пособия) производятся следующие действия:

1. Назначается новый администратор. Ему присваивается имя, пароль и меняется головной пароль суперпользователя.
2. Идентификатор, пароль и часть пароля суперпользователя увольняемого администратора удаляются из системы.
3. Электронные ключи доступа сдаются новому администратору безопасности. Возможность доступ по старым ключам блокируется.
4. Новый администратор безопасности анализирует рабочее место на наличие закладок, вирусов и т.д., после чего все данные на винчестере сотрудника уничтожаются и ОС на рабочем месте переинсталлируются.
5. Новый администратор безопасности анализирует все данные, к которым имел доступ сотрудник на предмет их зараженности вирусами.
6. Новый администратор безопасности вместе с непосредственным руководителем сотрудника анализирует целостность данных, к которым имел доступ сотрудник.
7. В случае обнаружения неправомерных действий сотрудника (удалении информации, внесения в систему закладок и вирусов) информация докладывается шефу службы безопасности или техническому директору и согласно контракту администратор увольняется без выходного пособия и решается вопрос о возбуждении против сотрудника уголовного дела по факту нанесения ущерба компании.

**3. По действиям различных категорий персонала, включая сотрудников отдела безопасности информации, по ликвидации последствий кризисных (аварийных или нештатных) ситуаций, в случае их возникновения**

Возможны следующие кризисные ситуации:

1. Уничтожение данных вследствие стихийного бедствия, пожара или наводнения.
2. Уничтожение, кража, раскрытие или модификация данных вследствие физического взлома и проникновения в помещение.
3. Уничтожение, модификация, раскрытие данных или нарушение работоспособности системы вследствие успешно проведенной атаки.

**4. Действия персонала по ликвидации последствий кризисных (аварийных или нештатных) ситуаций в случае их возникновения:**

- ***Уничтожение данных вследствие стихийного бедствия, пожара или наводнения***

При возникновении ситуации любому сотруднику, обнаружившему факт возникновения кризисной ситуации, необходимо:

- немедленно оповестить других сотрудников и принять все меры для самостоятельной оперативной защиты помещения ;
- немедленно позвонить в соответствующие службы помощи (пожарная и т.д.);
- немедленно доложить президенту компании, генеральному и техническому директору, шефу службы безопасности или администратору безопасности.

После оперативной ликвидации причин, вызвавших кризис, назначается комиссия во главе с ген. директором по устранению последствий кризиса. Комиссия определяет ущерб (какая информация и оборудование уничтожены), причины, по которым произошло происшествие и выявляет виновных.

- **Уничтожение, кража, раскрытие или модификация данных вследствие физического взлома и проникновения в помещение**

При возникновении ситуации любому сотруднику, обнаружившему факт взлома помещения или пропажи важного оборудования необходимо:

- немедленно доложить президенту компании, генеральному и техническому директору, шефу службы безопасности;
- сохранять помещение в первоначальном виде и воспрепятствовать проходу остальных сотрудников и возможному уничтожению улик в помещении.

Президент компании или генеральный директор, ознакомившись на месте происшествия, принимает решение о необходимости вызова милиции.

После оперативной ликвидации причин, вызвавших кризис, назначается комиссия во главе с ген. директором по устранению последствий кризиса. Комиссия определяет ущерб (какая информация и оборудование уничтожены или украдены), причины, по которым произошло происшествие и выявляет виновных.

- **Уничтожение, модификация, раскрытие данных или нарушение работоспособности системы вследствие успешно проведенной атаки**

При возникновении ситуации любому сотруднику, обнаружившему факт возникновения кризисной ситуации, необходимо немедленно оповестить администратора безопасности. Администратор безопасности обязан немедленно доложить шефу службы безопасности, генеральному и техническому директору об инциденте.

Немедленно после обнаружения факта инцидента или при подозрении на инцидент создается комиссия, куда входят администратор безопасности, секьюрити эксперт, шеф службы безопасности и технический директор. Комиссия определяет ущерб (какая информация подверглась атаке), причины, по которым произошло происшествие и выявляет виновных.

Возможные варианты действий при различных атаках:

1. Внешнее проникновение.

В случае подозрения на удаленную атаку и проникновение злоумышленника в корпоративную сеть извне немедленно отключатся все внешние связи, сеть компании изолируется от внешней сети и начинается расследование, по каким причинам злоумышленник смог проникнуть в сеть и к каким данным он смог получить доступ и чем это чревато для компании. После обнаружения, из-за чего стала возможна атака, причина успеха атаки ликвидируется, и система вводится в строй.

По результатам работы комиссии осуществляется попытка поиска атаковавшего и вырабатываются адекватные меры по снижению ущерба и не допущению такого типа атак в будущем.

2. Внутреннее проникновение.

В случае подозрения на атаку и проникновение злоумышленника в корпоративную сеть изнутри (атака осуществлена собственным персоналом) негласно создается комиссия, которая осуществляет внутренне расследование причин этой атаки и нанесенного ей ущерба. В результате работы комиссии находится виновный и вырабатываются адекватные меры по снижению ущерба и не допущению таких атак в будущем.

Характерными внешними чертами внешнего или внутреннего проникновения являются признаки утраты компанией конфиденциальной информации (обнаружение ее у конкурентов, выявления специфичной информации, которую конкурент не мог бы получить без проникновения в сеть и т.д.).

## 5. Действия администратора безопасности при обнаружении попыток сканирования, проникновения или атак на отказ в обслуживании

Администратор безопасности обязан осуществлять ежедневный анализ лог-файлов серверов удаленного доступа и систем обнаружения атак с целью обнаружения

подозрительной активности, попыток сканирования и несанкционированного проникновения в сеть. В случае обнаружения подобной активности Администратор обязан:

- запротоколировать данный случай и сообщить о нем в своем еженедельном отчете;
- в случае подозрения на целенаправленную постоянно осуществляющуюся атаку взломщика (не автоматизированных средств или червей, а именно человека) необходимо немедленно сообщить шефу службы безопасности и техническому директору;
- убедиться, что атака успешна отражена и не повлекла за собой последствий;
- предпринять ответные меры, включающие в себя:
  - выявление источника атаки (диапазоны IP-адресов, с которых осуществлена атака);
  - анализ по базе RIPE принадлежности IP-адресов, с которых была осуществлена атака;
  - выявление по базе ответственных за данный диапазон лиц и принадлежности этого диапазона к определенной организации;
  - отправка сообщений о атаках по официальным адресам;
  - если ответа нет (официальные адреса устарели), то самостоятельное сканирование диапазона адресов, с которых осуществлена атака, выявления принадлежности их какой-либо организации, поиск по открытой информации актуальных адресов системных администраторов и отправка им сообщений о произведенной с их диапазона атаки.

✓ ***Процедуры контроля в случае инцидентов***

1. Процедуры должны быть разработаны для покрытия всех возможных типов секьюрити инцидентов, включая:

- сбои в информационных системах;
- отказ в обслуживании;
- ошибки из-за незавершенных или неправильных бизнес данных;
- недостатки конфиденциальности.

2. В дополнении к обычному плану восстановления (разработанному для восстановления систем или служб как можно более оперативно) процедуры должны также рассматривать:

- анализ и идентификация причин инцидента;
- планирование и внедрение мер для предотвращения повторения (если необходимо);
- анализ и сохранение доказательств, следов инцидента, улики и свидетельств;
- взаимодействие между теми, кто пострадал или был вовлечен в восстановительный процесс;

- сообщение о действиях соответствующему начальству.

3. Следы инцидента, улики и свидетельства должны быть собраны и им необходимо обеспечить соответствующую безопасность для:

  - анализа внутренних проблем;
  - использования улик в отношении потенциальных нарушителей контрактов, нарушителей корпоративных требований или законов страны о компьютерных преступлениях;
  - переговоры о компенсациях с поставщиками железа и софта.

4. Действия по восстановлению после обнаружения дырок в системе безопасности и исправлению системных ошибок и неисправностей должны быть внимательно и формально запротоколированы. Процедура должна гарантировать что:

- только четко идентифицированный и авторизованный персонал может получать доступ к «ожившим» системам и данным;
- все аварийные действия задокументированы в деталях;
- обо всех аварийных действиях было доложено менеджменту в соответствующем порядке;
- целостность бизнес системы и ее управляемость подтверждена с минимальными задержками.

**Часть 3**

**Современные методы и средства сетевой защиты**

Рассмотрим самые распространенные и зарекомендовавших себя средства сетевой защиты. Ниже будут рассмотрены:

- Межсетевые экраны.
- Системы контроля.
- Системы построения VPN.
- Системы обнаружения атак.
- Системы анализа защищенности (сканеры безопасности).
- Обманные системы.

Пожалуй, именно эти средства вызывают наибольший интерес у пользователей и именно на них возлагаются основные надежды при обеспечении защиты от сетевых атак. И все же за пределами рассмотрения остаются не менее интересные технологии, такие как, криптографическая защита информации, инфраструктура PKI, системы аутентификации и т.д. Однако названные технологии хотя и являются важной составляющей комплексной и эффективной системы обеспечения информационной безопасности, но предназначены для решения несколько иных задач.

Необходимо лишний раз добавить, что в данном разделе рассматриваются лишь некоторые аспекты, связанные с названными выше средствами и технологиями.

### 3.1 Межсетевые экраны

Когда речь заходит о защите от атак, то первое, что приходит на ум большинству пользователей, - это межсетевые экраны (firewall). И это закономерно. Данная технология является одной из самых первых и поэтому самой известной. Итак, что же такое межсетевой экран? Говоря общими словами, - это средство, которое разграничивает доступ между двумя сетями (или, в частном случае, узлами) с различными требованиями по обеспечению безопасности. В самом распространенном случае межсетевой экран устанавливается между корпоративной сетью и Internet.

Межсетевой экран, защищающий сразу множество (не менее двух) узлов, призван решить две задачи, каждая из которых по-своему важна и в зависимости от организации, использующей межсетевой экран, имеет более высокий приоритет по сравнению с другой:

1. Ограничение доступа внешних (по отношению к защищаемой сети) пользователей к внутренним ресурсам корпоративной сети. К таким пользователям могут быть отнесены партнеры, удаленные пользователи, хакеры и даже сотрудники самой

компании, пытающие получить доступ к серверам баз данных, защищаемых межсетевым экраном.

2. Разграничение доступа пользователей защищаемой сети к внешним ресурсам. Решение этой задачи позволяет, например, регулировать доступ к серверам, не требуемым для выполнения служебных обязанностей.

Все межсетевые экраны используют в своей работе один из двух взаимоисключающих принципов:

1. Разрешено все, что не запрещено в явном виде". С одной стороны данный принцип облегчает администрирование межсетевого экрана, т.к. от администратора не требуется никакой предварительной настройки - межсетевой экран начинает работать сразу после включения в сеть электропитания. Любой сетевой пакет, пришедший на МСЭ, пропускается через него, если это не запрещено правилами. С другой стороны, в случае неправильной настройки данное правило делает межсетевой экран дырявым решетом, который не защищает от большинства несанкционированных действий, описанных в предыдущих главах. Поэтому в настоящий момент производители межсетевых экранов практически отказались от использования данного принципа.

2. "Запрещено все, что не разрешено в явном виде". Этот принцип делает межсетевой экран практически неприступной стеной (если на время забыть на возможность подкопа этой стены, ее обхода и проникновения через незащищенные бойницы). Однако, как это обычно и бывает, повышая защищенность, мы тем самым нагружаем администратора безопасности дополнительными задачами по предварительной настройке базы правил межсетевого экрана. После включения такого МСЭ в сеть, она становится недоступной для любого вида трафика. Администратор должен на каждый тип разрешенного взаимодействия задавать одно и более правил.

### ✓ Классификация

До сих пор не существует единой и общепризнанной классификации межсетевых экранов. Каждый производитель выбирает удобную для себя классификацию и приводит ее в соответствие с разработанным этим производителем межсетевым экраном. Однако, основываясь на приведенном выше неформальном определении МСЭ, можно выделить следующие их классы, учитывающие уровни OSI или стека TCP/IP:

- коммутаторы, функционирующие на канальном уровне;
- сетевые или пакетные фильтры, которые, как видно из названия, функционируют на сетевом уровне;
- шлюзы сеансового уровня (circuit-level proxy);

- посредники прикладного уровня (application proxy или application gateway);
- инспекторы состояния (stateful inspection).

### 3.1.1 Коммутаторы

Данные устройства, функционирующие на канальном уровне, не принято причислять к классу межсетевых экранов, т.к. они разграничивают доступ в рамках локальной сети и не могут быть применены для ограничения трафика из Internet. Однако, основываясь на том факте, что межсетевой экран разделяет доступ между двумя сетями или узлами, такое причисление вполне закономерно.

Многие производители коммутаторов, например, Cisco, Nortel, 3Com, позволяют осуществлять фильтрацию трафика на основе MAC-адресов, содержащихся во фреймах, пытающихся получить доступ к определенному порту коммутатора. Наиболее эффективно данная возможность реализована в решениях компании Cisco, в частности в семействе коммутаторов Catalyst, которые обладают механизмом Port Security. Однако надо заметить, что практически все современные сетевые карты позволяют программно изменять их MAC-адреса, что приводит к неэффективности такого метода фильтрации. Поэтому существуют и другие параметры, которые могут использоваться в качестве признака фильтрации. Например, VLAN, которые разграничивают трафик между ними - трафик одной VLAN никогда не пересекается с трафиком другой VLAN. Более "продвинутые" коммутаторы могут функционировать не только на втором, но и на третьем, четвертом (например, Catalyst) и даже седьмом уровнях модели OSI (например, TopLayer AppSwitch) . Необходимо сразу сделать небольшое замечание. Существует некоторая путаница в терминологии. Одни производители упоминают про коммутацию на пятом уровне, другие - на седьмом. И те и другие правы, но в маркетинговых целях эффектнее выглядит заявление о коммутации на 7-ми, а не 5-ти уровнях. Хотя на самом деле в обоих случаях подразумевается одно и то же. Ведь в модели TCP/IP всего пять уровней и последний, прикладной, уровень включает в себя заключительные три уровня, существующие в модели OSI/ISO.

| **Достоинства** | **Недостатки** |
|---|---|
| Высокая скорость работы. | Отсутствует возможность анализа прикладного уровня. |
| Данная возможность встроена в большинство коммутаторов, что не требует дополнительных финансовых затрат. | Отсутствует возможность анализа заголовков сетевого и сеансового уровней (исключая некоторые коммутаторы). |
| | Нет защиты от подмены адреса. |

### 3.1.2 Пакетные фильтры

Пакетные фильтры (packet filter) - это одни из первых и самые распространенные межсетевые экраны, которые функционируют на третьем, сетевом уровне и принимают решение о разрешении прохождения трафика в сеть на основании информации, находящейся в заголовке пакета. Многие фильтры также могут оперировать заголовками пакетов и более высоких уровней (например, TCP или UDP). Распространенность этих межсетевых экранов связана с тем, что именно эта технология используется в абсолютном большинстве маршрутизаторов (экранирующий маршрутизатор, screening router) и даже коммутаторах (например, в решениях компании Cisco). В качестве параметров, используемых при анализе заголовков сетевых пакетов, могут использоваться:

- адреса отправителей и получателей;
- тип протокола (TCP, UDP, ICMP и т.д.);
- номера портов отправителей и получателей (для TCP и UDP трафика);
- другие параметры заголовка пакета (например, флаги TCP-заголовка).

С помощью данных параметров, описанных в специальном наборе правил, можно задавать достаточно гибкую схему разграничения доступа. При поступлении пакета на любой из интерфейсов маршрутизатора, он сначала определяет, может ли он доставить пакет по назначению (т.е. может ли осуществить процесс маршрутизации). И только потом маршрутизатор сверяется с набором правил (т.н. список контроля доступа, access control list), проверяя, должен ли он маршрутизировать этот пакет. При создании правил для пакетных фильтров можно использовать два источника информации: внутренний и внешний. Первый источник включает в себя уже названные поля заголовка сетевого пакета. Второй, реже используемый источник оперирует информацией внешней по отношению к сетевым пакетам. Например, дата и время прохождения сетевого пакета.

Сетевые фильтры, обладая рядом достоинств, не лишены и ряда серьезных недостатков. Во-первых, исходя из того, что они анализируют только заголовок (такие фильтры получили название stateless packet filtering), за пределами рассмотрения остается поле данных, которое может содержать информацию, противоречащую политике безопасности. Например, в данном поле может содержаться команда на доступ к файлу паролей по протоколу FTP или HTTP, что является признаком враждебной деятельности. Другой пример. Пакетный фильтр может пропустить в защищаемую сеть TCP-пакет от узла, с которым в настоящий момент не открыто никаких активных сессий. Т.к. межсетевой экран, функционирующий на сетевом уровне, не анализирует информацию, присущую транспортному и более высокому уровню, то он пропустит такой пакет в сеть. В целом, недостаток пакетных фильтров заключается в

том, что они не умеют анализировать трафик на прикладном уровне, на котором совершается множество атак - проникновение вирусов, Internet-червей, отказ в обслуживании и т.д. Некоторые производители, например, Cisco, предлагают пакетные фильтры с учетом состояния (stateful packet filtering), которые сохраняют в памяти сведения о состоянии текущих сеансов, что позволяет предотвратить некоторые атаки (в частности, описанные в последнем примере).

Другой недостаток пакетных фильтров - сложность настройки и администрирования. Приходится создавать как минимум два правила для каждого типа разрешенного взаимодействия (для входящего и исходящего трафика). Мало того, некоторые правила, например, реализованные в решениях компании Cisco, различаются для каждого интерфейса маршрутизатора, что только усложняет создание таблицы правил (списка контроля доступа). Неконтролируемое увеличение числа правил может приводить к появлению брешей в первой линии обороны, создаваемой пакетными фильтрами. Известны случаи, когда таблицы правил маршрутизаторов содержали тысячи правил. Только представьте, с какой головной болью столкнулись бы администраторы, пожелавшие локализовать какую-либо проблему с пропуском трафика. И не стоит забывать, что при настройке фильтра может случиться ситуация, когда одно правило противоречит другому. Увеличение числа правил несет с собой и еще одну проблему - снижение производительности межсетевого экрана. Ведь пришедший пакет проверяется на соответствие таблицы правил, начиная с ее верха, что в свою очередь требует внимательного отношения к порядку следования правил. Такая проверка осуществляется до тех пор, пока не будет найдено соответствующее правило или не будет достигнут конец таблицы. Во многих реализациях, каждое новое правило, пусть не намного, но все же уменьшает общую производительность фильтра. Одним из немногих исключений является уже неоднократно упоминавшаяся продукция компании Cisco, в которой реализованы высокоэффективные механизмы обработки сетевого трафика.

Еще один недостаток пакетных фильтров - слабая аутентификация трафика, которая осуществляется только на основе адреса отправителя. Текущая версия протокола IP (v4) позволяет без труда подменять такой адрес, подставляя вместо него любой из адресов, принадлежащий адресному пространству IP-протокола, реализуя тем самым атаку "подмена адреса" (IP Spoofing). И даже, если адрес компьютера-отправителя не изменялся, то что мешает злоумышленнику сесть за этот компьютер. Ведь сетевой фильтр не запрашивает у пакета идентификатор и пароль пользователя, т.к. эта информация принадлежит прикладному уровню.

Данные МСЭ могут быть реализованы как аппаратно, например, в фильтрующих маршрутизаторах компании Cisco, так и программно, например, в ОС Windows 2000, Unix и т.д. Причем пакетный фильтр может быть установлен не только на устройстве,

расположенном на границе между двумя сетями (например, на маршрутизаторе), но и на рабочей станции пользователя, повышая тем самым ее защищенность.

Однако простота реализации пакетных фильтров, их высокая производительность и малая цена (зачастую такие фильтры являются свободно распространяемыми) перевешивает указанные недостатки и обуславливает их повсеместное распространение и использование как обязательного (а зачастую единственного) элемента системы сетевой безопасности. Кроме того, они являются составной частью практически всех межсетевых экранов, использующих контроль состояния и описываемых далее.

| **Достоинства** | **Недостатки** |
|---|---|
| Высокая скорость работы. | Отсутствует возможность анализа прикладного уровня. |
| Простота реализации. | Нет защиты от подмены адреса. |
| Данная возможность встроена во все маршрутизаторы и многие ОС, что не требует дополнительных финансовых затрат. | Сложность настройки и администрирования. |
| Низкая стоимость или свободное распространение (в случае приобретения). | При увеличении числа правил возможно снижение производительности. |
| | Требуется детальное знание сетевых услуг и протоколов. |
| | Нет контроля состояния соединения. |
| | Трудность функционирования в сетях с динамическим распределением адресов. |

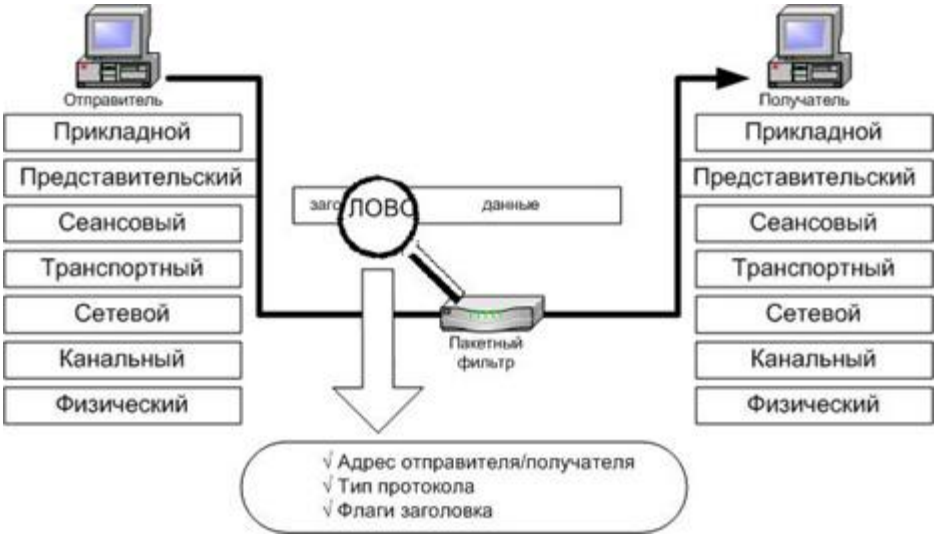



Рисунок 1.1 «Пакетный фильтр»

### 3.1.3 Шлюзы сеансового уровня

Шлюз сеансового уровня - это другая технология, используемая в межсетевых экранах, но на сегодняшний день ее очень трудно встретить в виде единственной технологии, реализованной в межсетевом экране. Как правило, они поставляются в рамках прикладных шлюзов или инспекторов состояний. Кроме того, обеспечиваемый им уровень защиты немногим выше, чем у пакетных фильтров, при более низкой производительности.

Смысл технологии фильтрации на сеансовом уровне заключается в том, что шлюз исключает прямое взаимодействие двух узлов, выступая в качестве т.н. посредника (proxy), который перехватывает все запросы одного узла на доступ к другому и, после проверки допустимости таких запросов, устанавливает соединение. После этого шлюз сеансового уровня просто копирует пакеты, передаваемые в рамках одной сессии, между двумя узлами, не осуществляя дополнительной фильтрации. Как только авторизованное соединение установлено, шлюз помещает в специальную таблицу соединений соответствующую информацию (адреса отправителя и получателя, состояние соединения, информация о номере последовательности и т.д.). Как только сеанс связи завершается, запись о нем удаляется из этой таблицы. Все последующие пакеты, которые могут быть сформированы злоумышленником и "как бы относятся" к уже завершенному соединению, отбрасываются.

Достоинство данной технологии, ярким представителем которой является SOCKS в том, что она исключает прямой контакт между двумя узлами. Адрес шлюза сеансового уровня является единственным элементом, который связывает внешнюю сеть, кишащую хакерами, с внутренними, защищаемыми ресурсами. Кроме того, поскольку соединение между узлами устанавливается только после проверки его допустимости, то тем самым шлюз предотвращает возможность реализации подмены адреса, присущую пакетным фильтрам.

Несмотря на кажущуюся эффективность этой технологии, у нее есть один очень серьезный недостаток - невозможность проверки содержания поля данных. Т.е. тем самым злоумышленнику представляется возможность передачи в защищаемую сеть троянских коней и других Internet-напастей. Мало того, описанная в предыдущих главах возможность перехвата TCP-сессии (TCP hijacking), позволяет злоумышленнику даже в рамках разрешенной сессии реализовывать свои атаки.

| **Достоинства** | **Недостатки** |
|---|---|
| Высокая скорость работы. | Отсутствует возможность анализа прикладного уровня. |
| Простота реализации. | |
| Исключение прямого взаимодействия между двумя узлами. | |
| Контроль состояния соединения. | |
| | |

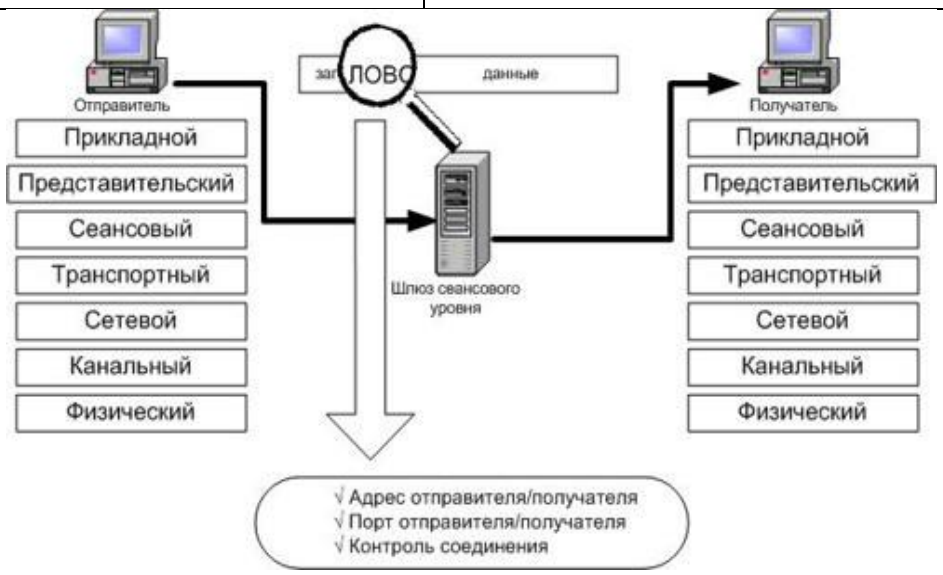



Рисунок 1.2 «Шлюз сеансового уровня»

### 3.1.4 Посредники прикладного уровня

Посредники прикладного уровня практически ничем не отличаются от шлюзов сеансового уровня, за одним исключением. Они также осуществляют посредническую функцию между двумя узлами, исключая их непосредственное взаимодействие, но позволяют проникать в контекст передаваемого трафика, т.к. функционируют на прикладном уровне. Межсетевые экраны, построенные по этой технологии, содержат т.н. посредников

приложений (application proxy), которые, "зная" как функционирует то или иное приложение, могут обрабатывать сгенерированный ими трафик. Таким образом, эти посредники могут, например, разрешать в исходящем трафике команду GET (получение файла) протокола FTP и запрещать команду PUT (отправка файла) и наоборот. Еще одно отличие от шлюзов сеансового уровня - возможность фильтрации каждого пакета.

Однако, как видно из приведенного описания, если для какого-либо из приложений отсутствует свой посредник приложений, то межсетевой экран не сможет обрабатывать трафик такого приложения, и он будет отбрасываться. Именно поэтому так важно, чтобы производитель межсетевого экрана своевременно разрабатывал посредники для новых приложений, например, для мультимедиа-приложений.

| **Достоинства** | **Недостатки** |
|---|---|
| Анализ на прикладном уровне и возможность реализации дополнительных механизмов защиты (например, анализ содержимого). | Невозможность анализа трафика от "неизвестного" приложения. |
| Исключение прямого взаимодействия между двумя узлами. | Невысокая производительность. |
| Высокий уровень защищенности. | Уязвимость к атакам на уровне ОС и приложений. |
| Контроль состояния соединения. | Требование изменения модификации клиентского ПО. |
| | Не всегда есть посредник для приложений на базе протоколов UDP и RPC. |
| | Двойной анализ - на уровне приложения и уровне посредника. |

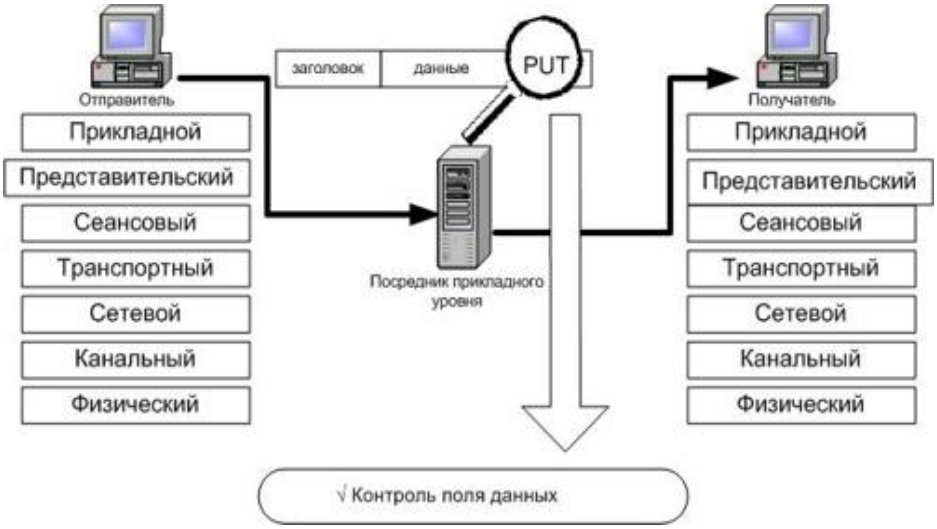



Рисунок 1.3 «Посредник прикладного уровня»

### 3.1.5 Инспекторы состояния

Каждый из названных классов межсетевых экранов обладает рядом достоинств и может применяться для защиты корпоративных сетей. Однако куда более эффективным было бы объединить все названные классы МСЭ в одном устройстве. Что и было сделано в инспекторах состояний, которые совмещают в себе все достоинства названных выше типов экранов, начиная анализ трафика с сетевого и заканчивая прикладным уровнями, что позволяет совместить в одном устройстве казалось бы несовместимые вещи - большую производительность и высокую защищенность. Эти межсетевые экраны позволяют контролировать:

- каждый передаваемый пакет - на основе имеющейся таблицы правил;
- каждую сессию - на основе таблицы состояний;
- каждое приложение - на основе разработанных посредников.

Действуя по принципу "продвинутого" шлюза сеансового уровня, инспектор состояния, тем не менее, не препятствует установлению соединения между двумя узлами, за счет производительность такого межсетевого экрана существенно выше, чем у шлюза сеансового и прикладного уровня, приближаясь к значениям, встречающимся только у пакетных фильтров. Еще одно достоинство межсетевых экранов с контролем состояния - прозрачность для конечного пользователя, не требующая дополнительной настройки или изменения конфигурации клиентского программного обеспечения.

Завершая описание классов межсетевых экранов, хотим заметить, что термин "stateful inspection", введенный компанией Check Point Software, так полюбился производителям, что сейчас очень трудно найти межсетевой экран, который бы не относили к этой категории (даже если он и не реализует эту технологию). Таким образом, сейчас на рынке существует всего два класса межсетевых экранов - инспекторы состояний и пакетные фильтры.

- ✓ **Выбор межсетевого экрана**

Существует замечательная русская поговорка: "Не стоит класть все яйца в одну корзину". Именно по такому принципу и надо выбирать межсетевой экран. Нельзя сделать однозначный выбор в пользу какого-либо из названных экранов. Лучше если вы сможете использовать два межсетевых экрана, строя таким образом эшелонированную оборону своей сети. Если один из экранов будет выведен из строя, то до тех пор его работоспособность не будет восстановлена, весь удар примет на себя второй экран. Обычно используется комбинация "пакетный фильтр - инспектор состояния (или посредник прикладного уровня)". И эта комбинация хороша еще и тем, что вам не придется тратиться на приобретение пакетного фильтра, уже встроенного в маршрутизатор, установленный на границе вашей сети.

- ✓ **Возможности**

Помимо фильтрации трафика межсетевые экраны позволяют выполнять и другие, не менее важные функции, без которых обеспечение защиты периметра было бы неполным. Разумеется, приводимый ниже список не является исчерпывающим, но и данный материал не является руководством по выбору межсетевого экрана. Здесь всего лишь указаны некоторые средства защиты от атак, описанных ранее.

- ✓ **Трансляция сетевых адресов**

Как показано ранее, для реализации многих атак злоумышленнику необходимо знать адрес своей жертвы. Чтобы скрыть эти адреса, а также топологию всей сети, межсетевые экраны выполняют очень важную функцию - трансляцию сетевых адресов (network address translation). Трансляция может осуществлять двумя способами - динамически и статически. В первом случае адрес выделяется узлу в момент обращения к межсетевому экрану. После завершения соединения адрес освобождается и может быть использован любым другим узлом корпоративной сети. Во втором случае адрес узла всегда привязывается к одному адресу МСЭ.

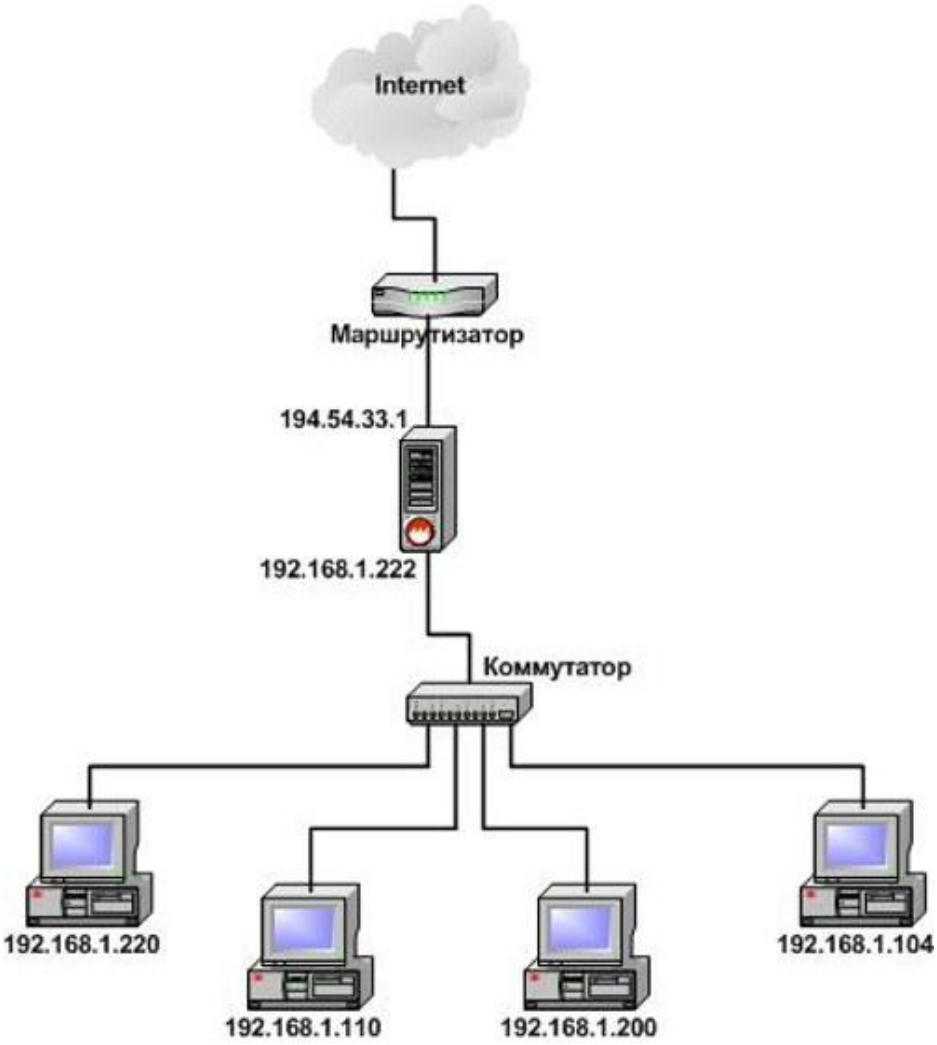



Рисунок 1.4 «Трансляция сетевых адресов»

✓ Аутентификация пользователей

Межсетевые экраны помимо разрешения или запрещения допуска различных приложений в сеть, также могут выполнять аналогичные действия и для пользователей, которые желают получить доступ к внешним или внутренним ресурсам, разделяемым межсетевым экраном. При этом проверка подлинности (аутентификация) пользователя может осуществляться как при предъявлении обычного идентификатора (имени) и пароля, так и с помощью более надежных методов, например, с помощью SecureID или цифровых сертификатов.

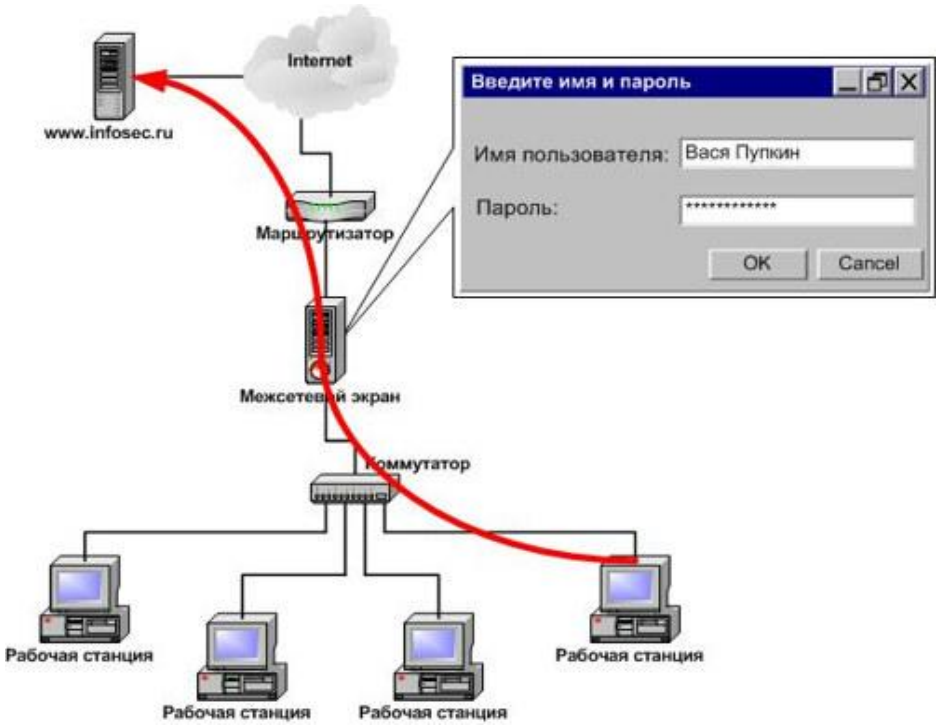



Рисунок 1.5 «Аутентификация»

✓ Регистрация событий

Являясь критическим элементом системы защиты корпоративной сети, межсетевой экран имеет возможность регистрации всех действий, им фиксируемых. К таким действиям относятся не только пропуск или блокирование сетевых пакетов, но и изменение правил разграничения доступа администратором безопасности и другие действия. Такая регистрация позволяет обращаться к создаваемым журналам по мере необходимости - в случае возникновения инцидента безопасности или сбора доказательств для предоставления их в судебные инстанции или для внутреннего расследования.

✓ **Реализация**

Существует два варианта реализации межсетевых экранов - программный и программно-аппаратный. Второй вариант также может быть реализован двояко - в виде специализированного устройства и в виде модуля в маршрутизаторе или коммутаторе. Интерес к программно-аппаратным решениям за последние два года во всем мире возрос. Такие решения постепенно вытесняют "чисто" программные системы и начинают играть первую скрипку на данном рынке.

Первое решение - наиболее часто используемое в настоящее время и на первый взгляд более привлекательное. Это связано с тем, что, по мнению многих, для его применения достаточно только приобрести программное обеспечение межсетевого экрана и установить на любой компьютер, имеющийся в организации. Однако на практике далеко не всегда в организации находится свободный компьютер, да еще и удовлетворяющий достаточно

высоким требованиям по системным ресурсам. Поэтому одновременно с приобретением программного обеспечения приобретается и компьютер для его установки. Потом следует процесс установки на компьютер операционной системы и ее настройка, что также требует времени и оплаты работы установщиков. И только после этого устанавливается и настраивается программное обеспечение системы обнаружения атак. Как видно, использование обычной персоналки далеко не так просто, как кажется на первый взгляд. Именно поэтому в последние годы стали получать распространения специализированные программно-аппаратные решения, называемые security appliance. Они поставляются, как специальные программно-аппаратные комплексы, использующие специализированные или обычные операционные системы (как правило, на базе FreeBSD или Linux), "урезанные" для выполнения только заданных функций. К достоинству таких решений можно отнести:

1. Простота внедрения в технологию обработки информации. Поскольку такие устройства поставляются уже с предустановленной и настроенной операционной системой и защитными механизмами, необходимо только подключить его к сети, что выполняется в течение нескольких минут. И хотя некоторая настройка все же требуется, время, затрачиваемое на нее, существенно меньше, чем в случае установки и настройки межсетевого экрана "с нуля".
2. Простота управления. Данные устройства могут управляться с любой рабочей станции Windows 9x, NT, 2000 или Unix. Взаимодействие консоли управления с устройством осуществляется либо по стандартным протоколам, например, Telnet или SNMP, либо при помощи специализированных или защищенных протоколов, например, Ssh или SSL.
3. Производительность. За счет того, что из операционной системы исключаются все "ненужные" сервисы и подсистемы, устройство работает более эффективно с точки зрения производительности и надежности.
4. Отказоустойчивость и высокая доступность. Реализация межсетевого экрана в специальном устройстве позволяет реализовать механизмы обеспечения не только программной, но и аппаратной отказоустойчивости и высокой доступности. Такие устройства относительно легко объединяются в кластеры.
5. Сосредоточение на защите. Решение только задач обеспечения сетевой безопасности не приводит к трате ресурсов на выполнение других функций, например, маршрутизации и т.п. Обычно, попытка создать универсальное устройство, решающее сразу много задач, ни к чему хорошему не приводит.

В отчете, опубликованном независимой консалтинговой компанией Gartner Group в июне 1997 года, было написано, что к 2002 году 80% компаний с доходами от 20 до 200 миллионов долларов выберут именно аппаратные решения, а не программные. Основная причина такого выбора - обеспечение такого же высокого уровня защиты, как и в программных решениях, но

за меньшие деньги. И вторая причина - простота и легкость интеграции таких решений в корпоративную систему.

На первый взгляд такие аппаратные реализации существенно дороже, но это только на первый взгляд. Стоимость программно-аппаратного решения составляет порядка $5000-12000. Стоимость решения, основанного на применении только программного обеспечения, выполняющего аналогичные функции, может быть существенно выше. И это несмотря на то, что само ПО стоит меньше. Такой эффект достигается за счет того, что стоимость программного решения включает в себя:

1. Стоимость компьютера.
2. Стоимость лицензионного дистрибутива операционной системы.
3. Стоимость сопутствующего программного обеспечения (например, броузера Internet Explorer или СУБД Oracle).
4. Стоимость затрат на установку и настройку всего комплекса в целом. Обычно эти затраты составляют 20-30% от стоимости составляющих всего комплекса.
5. Стоимость поддержки всех составляющих комплекса (компьютера и его аппаратных составляющих, операционной системы, дополнительного ПО и т.д.).

Для программно-аппаратного комплекса этих "дополнительных" затрат не существует, т.к. они уже включены в стоимость "железа".

| | **Универсальный компьютер** | **Специализированный компьютер** |
|---|---|---|
| *Достоинства* | 1. Неограниченная функциональная расширяемость | 1. Высокая производительность<br>2. Простота внедрения<br>3. Простота управления<br>4. Отказоустойчивость |
| **Недостатки** | 1. Средняя производительность<br>2. Уязвимости ОС<br>3. Низкая отказоустойчивость | 1. Минимальная функциональная расширяемость |

Однако сразу необходимо заметить, что специализированный компьютер - это не то же самое, что маршрутизатор с функциями обнаружения атак (например, маршрутизаторы с Cisco Secure Integrated Software). У производителя маршрутизаторов приоритетной задачей

всегда является улучшение процесса и повышение скорости маршрутизации. И только затем он пытается реализовать функции защиты. Поэтому, делая выбор между маршрутизацией и защитой, они всегда делают его в пользу маршрутизации. Как показывает практика, использование защитных механизмов на маршрутизаторах существенно снижает их производительность. Либо же защитные функции ограничены.

- ✓ **Недостатки**

Выше уже были перечислены некоторые недостатки, присущие межсетевым экранам, а также способы их обхода. Ниже мы укажем еще некоторые из них.

- ✓ **Ограничение функциональности сетевых сервисов**

Некоторые корпоративные сети используют топологии, которые трудно "уживаются" с межсетевым экраном (например, широковещательная рассылка трафика), или используют некоторые сервисы (например, NFS) таким образом, что применение МСЭ требует существенной перестройки всей сетевой инфраструктуры. В такой ситуации относительные затраты на приобретение и настройку межсетевого экрана могут быть сравнимы с ущербом, связанным с отсутствием МСЭ.

Решить данную проблему можно только путем правильного проектирования топологии сети на начальном этапе создания корпоративной информационной системы. Это позволит не только снизить последующие материальные затраты на приобретение средств защиты информации, но и эффективно встроить межсетевые экраны в существующую технологию обработки информации. Если сеть уже спроектирована и функционирует, то, возможно, стоит подумать о применении вместо межсетевого экрана какого-либо другого решения, например, системы обнаружения атак.

- ✓ **Потенциально опасные возможности**

Новые возможности, которые появились недавно, и которые облегчают жизнь пользователям Internet, разрабатывались практически без учета требований безопасности. Например, JavaScript, Java, ActiveX и другие сервисы, ориентированные на работу с данными. Специфика мобильного кода такова, что он может быть использован и как средство для проведения атак, и как объект атаки. В первом варианте опасность заключается в том, что мобильный код загружается на компьютер пользователя и выполняется на нем как обычная программа, получая доступ к системным ресурсам. Второй вариант, как правило, используется для модификации мобильного кода - как предварительный этап перед проведением атак на локальный компьютер пользователя. Атаки на мобильный код, как на средство выполнения каких-либо функций, пока не получили широкого распространения.

Связано это с тем, что мобильный код пока не применяется для выполнения каких-либо серьезных операций, например, проведения финансовых транзакций. Хотя уже известны примеры банковских систем, в том числе и российских, использующих технологию Java для работы с клиентом.

Как средство для проведения атак мобильный код может быть реализован в виде:

- вируса, который вторгается в информационную систему и уничтожает данные на локальных дисках, постоянно модифицируя свой код, затрудняя тем самым свое обнаружение и удаление;
- агента, перехватывающего пароли, номера кредитных карт и т.п.;
- программы, копирующей конфиденциальные файлы, содержащие деловую и финансовую информацию;
- прочее.

Маскироваться такие программы могут под анимационные баннеры, интерактивные игры, звуковые файлы и т.п. Российские пользователи не так часто используют компьютер для совершения финансовых сделок и других действий, которые могли бы нарушить конфиденциальность данных. Поэтому рассмотрим примеры враждебного мобильного кода, который нарушает функционирование узла, на котором он запускается. Это наиболее простая в реализации и, как следствие, часто применяемая угроза, которой может подвергнуться любой пользователь сети Internet. Такая угроза может осуществляться путем:

- создания высокоприоритетных процессов, выполняющих несанкционированные действия;
- генерации большого числа окон;
- "захвата" большого объема памяти и важных системных классов;
- загрузки процессора бесконечным циклом;
- и т.п.

Обычный подход, используемые при обнаружении мобильного кода, заключается в том, чтобы сканировать весь входящий трафик на 80-м или 443-м портах, используемых протоколами HHTP и HTTPS, с целью выявить такие элементы, как соответствующие теги. Но этого недостаточно, чтобы остановить мобильный код, потому что можно получить управляющие элементы ActiveX и апплеты Java и другими способами. Для примера представим, что Java-апплет (обычно имеющий расширение .class) выдает себя за изображение (то есть имеет расширение gif или jpg). Если межсетевой экран считает, что это изображение, то оно пропускается в сеть и загружается в кэш броузера, после чего броузер выходит из строя, так как загруженный файл не является изображением. Однако это неважно - мобильный код уже находится на компьютере. И если позже его можно будет

активизировать, то могут возникнуть серьезные проблемы с защищенностью системы. Другой способ проникновения - использование нестандартного порта для работы Web-сервера.

Одним из вариантов защиты, например для Java-апплетов, можно считать сканирование всего трафика, проходящего в защищаемом сегменте, чтобы выявить наличие конкретных участков кода. Такое выявление осуществляется путем поиска числа идентифицирующего байт-код, которое в шестнадцатеричной форме выглядит как "CA FE BA BE". Однако данный подход производителями средств защиты практически не применяется, так как трафик обычно слишком интенсивен, чтобы фильтровать его поток через каждый порт для выявления конкретных текстовых фрагментов.

- ✓ **Вирусы и атаки**

Практически ни один межсетевой экран не имеет встроенных механизмов защиты от вирусов и, в общем случае, от атак. Как правило, эта возможность реализуется путем присоединения к МСЭ дополнительных модулей или программ третьих разработчиков (например, система антивирусной защиты Trend Micro для МСЭ Check Point Firewall-1 или система обнаружения атак RealSecure для него же). Использование нестандартных архиваторов или форматов передаваемых данных, а также шифрование трафика, сводит всю антивирусную защиту "на нет". Как можно защититься от вирусов или атак, если они проходят через межсетевой экран в зашифрованном виде и расшифровываются только на оконечных устройствах клиентов?

В таком случае лучше перестраховаться и запретить прохождение через межсетевой экран данных в неизвестном формате. Для контроля содержимого зашифрованных данных в настоящий момент ничего предложить нельзя. В этом случае остается надеяться, что защита от вирусов и атак осуществляется на оконечных устройствах. Например, при помощи системных агентов системы RealSecure.

- ✓ **Снижение производительности**

Очень часто межсетевые экраны являются самым узким местом сети, снижая ее пропускную способность. В тех случаях, когда приходится анализировать не только заголовок (как это делают пакетные фильтры), но и содержание каждого пакета ("proxy"), существенно снижается производительность межсетевого экрана. Для сетей с напряженным трафиком использование обычных межсетевых экранов становится нецелесообразным. В таких случаях на первое место надо ставить обнаружение атак и реагирование на них, а

блокировать трафик необходимо только в случае возникновения непосредственной угрозы. Тем более что некоторые средства обнаружения атак (например, BlackICE Gigabit Sentry) могут функционировать и на гигабитных скоростях.

Компромисс между типами межсетевых экранов - более высокая гибкость в пакетных фильтрах против большей степени защищенности и отличной управляемости в шлюзах прикладного уровня или инспекторах состояния. Хотя на первый взгляд кажется, что пакетные фильтры должны быть быстрее, потому что они проще и обрабатывают только заголовки пакетов, не затрагивая их содержимое, это не всегда является истиной. Многие межсетевые экраны, построенные на основе прикладного шлюза, показывают более высокие скоростные характеристики, чем маршрутизаторы, и представляют собой лучший выбор для управления доступом. Это связано с тем, что как уже говорилось, маршрутизаторы являются не специализированными устройствами и функции фильтрации для них не являются приоритетными.

- ✓ **Персональные межсетевые экраны**

За последние несколько лет в структуре корпоративных сетей произошли серьезные изменения. Если раньше границы таких сетей можно было четко очертить, то сейчас это практически невозможно. Еще недавно такая граница проходила через все маршрутизаторы или иные устройства (например, модемы), через которые осуществлялся выход во внешние сети. В удаленных офисах организации ситуация была схожа. Однако сейчас полноправным пользователем защищаемой межсетевым экраном сети является сотрудник, находящийся за пределами защищаемого периметра. К таким сотрудникам относятся пользователи, работающие на дому или находящиеся в командировке. Требуется ли им защита? Несомненно. Но все традиционные межсетевые экраны построены так, что защищаемые пользователи и ресурсы должны находиться под сенью их защиты, т.е. с внутренней стороны, что является невозможным для мобильных пользователей. Чтобы устранить эту проблему было предложено два подхода - виртуальные частные сети (virtual private network, VPN), которые будут описаны далее, и распределенные межсетевые экраны (distributed firewall). Примером первого решения можно назвать VPN-1 компании Check Point Software. Такая схема, похожая на осьминога, раскинувшего свои щупальца, обладала только одним недостатком - сам удаленный узел был подвержен атакам, хотя доступ в корпоративную сеть был защищен от несанкционированных воздействий. Установленный на удаленное рабочее место троянский конь мог дать возможность проникнуть злоумышленнику через межсетевой экран и по защищенному каналу. Ведь VPN шифрует и обычный, и несанкционированный

трафик, не делая между ними различий. Тогда-то и родилась идея распределенного межсетевого экрана (distributed firewall), который являлся бы мини-экраном, защищающим не всю сеть, а только отдельный компьютер. Примерами такого решения является BlackICE Agent компании Internet Security Systems или RealSecure Server Sensor того же производителя. Это решение понравилось и домашним пользователям, которые наконец-то получили возможность защиты своих компьютеров от рыскающих по сети злоумышленников. Но, т.к. многие функции распределенного МСЭ (например, централизованное управление или рассылка политики безопасности) для домашних пользователей были лишними, то технология распределенного МСЭ была модифицирована и новый подход получил название "персонального межсетевого экрана" (personal firewall), яркими представителями которых являются ZoneAlarm, и BlackICE Defender компаний ZoneLabs и ISS соответственно. Компания Check Point Software оказалась впереди и здесь, предложив решение VPN-1 SecureClient и VPN-1 SecureServer, которые не только защищают от внешних атак компьютеры, на которых они установлены, но и обеспечивают защиту трафика, передаваемого за пределы данного узла (т.е. организуя client\server VPN). Именно такое решение сделало подвластными межсетевым экранам сети с нечетко очерченными границами.

В чем отличие персонального межсетевого экрана от распределенного? Главное отличие одно - наличие функции централизованного управления. Если персональные межсетевые экраны управляются только с того компьютера, на котором они установлены, и идеально подходят для домашнего применения, то распределенные межсетевые экраны могут управляться централизованно, с единой консоли управления, установленной в главном офисе организации. Такие отличия позволили некоторым производителям выпускать свои решения в двух версиях - персональной (для домашних пользователей) и распределенной (для корпоративных пользователей). Так, например, поступила компания Internet Security Systems, которая предлагает персональный межсетевой экран BlackICE Defender и распределенный межсетевой экран BlackICE Agent.

Какими функциями должен обладать эффективный персональный МСЭ? Во-первых, этот экран не должен быть пассивной программой, которая только и делает, что блокирует входящий на компьютер трафик по заданным критериям, к которым обычно относятся адрес и порт источника. Злоумышленники давно научились обходить такие простые защитные механизмы и в сети Internet можно найти большое число программ, которые могут проникнуть через многие традиционные защитные барьеры. Примером такой программы является троянский конь SubSeven 2.2, позволяющий выполнять большое число функций на скомпрометированном компьютере без ведома его владельца. Чтобы защититься, необходим инструмент, который позволит проводить более глубокий анализ каждого сетевого пакета,

направленного на защищаемый узел. Таким инструментом является система обнаружения атак, которая в трафике, пропущенном через межсетевой экран, обнаруживает следы хакерской деятельности. Она не доверяет слепо таким разрешительным признакам, как адрес и порт источника. Как известно протокол IP, на основе которого построен современный Internet, не имеет серьезных механизмов защиты, что позволяет без труда подменить свой настоящий адрес, тем самым, делая невозможным отслеживание злоумышленника. Мало того, хакер может «подставить» кого-нибудь другого, заменив свой адрес на адрес подставного лица. И, наконец, для некоторых атак (например, «отказ в обслуживании») адрес источника вообще не нужен и по статистике в 95% случаев этот адрес хакером изменяется. Можно привести хорошую аналогию. Персональный межсетевой экран - это охранник в здании, который выписывает пропуска всем посетителям. В такой ситуации злоумышленник может без труда пронести в здание оружие или бомбу. Однако если на входе поставить металлодетектор, то ситуация в корне меняется и злоумышленнику уже не так легко пронести в защищаемую зону запрещенные предметы.

К сожалению, приходится отметить, что немногие межсетевые экраны обладают встроенной системой обнаружения атак. Одним из таких решений является системы BlackICE Defender и BlackICE Agent компании Internet Security Systems. Любой из компонентов семейства BlackICE содержит два основных модуля, осуществляющих обнаружение и блокирование несанкционированной деятельности - BlackICE Firewall и BlackICE IDS. BlackICE Firewall отвечает за блокирование сетевого трафика с определенных IP-адресов и TCP/UDP-портов. Предварительное блокирование трафика по определенным критериям позволяет увеличить производительность системы за счет снижения числа "лишних" операций на обработку неразрешенного трафика. Настройка данного компонента может осуществлять как вручную, так и в автоматическом режиме. В последнем случае, реконфигурация происходит после обнаружения несанкционированной деятельности модулем BlackICE IDS. При этом блокирование трафика может осуществляться на любой промежуток времени. BlackICE Firewall работает напрямую с сетевой картой, минуя встроенный в операционную систему стек протоколов, что позволяет устранить опасность от использования многих известных уязвимостей, связанных с некорректной реализацией стека в ОС. BlackICE IDS отвечает за обнаружение атак и других следов несанкционированной деятельности в трафике, поступающем от модуля BlackICE Firewall, и использует запатентованный алгоритм семиуровневого анализа протокола.

Следующим механизмом, которым должен обладать эффективный персональный межсетевой экран, является защита от опасного содержимого, которое можно получить из Internet. К такому содержимому можно отнести апплеты Java и управляющие элементы ActiveX, код ShockWave и сценарии JavaScript, Jscript и VBScript. С помощью этих, с одной

стороны незаменимых и удобных технологий, можно выполнить большое число несанкционированных действий на компьютере. Начиная от внедрения вирусов и установки троянских коней и заканчивая кражей или удалением всей информации. Также персональные межсетевые экраны должны защищать от cookies, которые могут раскрыть конфиденциальную информацию о владельце компьютера.

В некоторые персональные МСЭ (например, в Norton Internet Security компании Symantec) встроены антивирусные системы, которые помимо обнаружения троянцев могут обнаруживать и большое число вирусов, включая макрос-вирусы и Internet-червей. Зачастую производители встраивают в свою продукцию модули VPN (например, PGP Desktop Security или VPN-1 SecureClient), которые отвечают за обеспечение защищенного взаимодействия с центральным офисом.

Т.к. распределенные экраны управляются централизованно, то они должны обладать эффективным механизмом настройки, администрирования и контроля, позволяющим администратору безопасности без дополнительных усилий получить подробную информацию о зафиксированных попытках проникновения на защищаемые узлы. Мало того, в некоторых случаях необходимо инициировать процедуру расследования компьютерного преступления или собрать доказательства для обращения в правоохранительные органы. И здесь будет незаменимым механизм отслеживания злоумышленника (back tracing), реализованный в некоторых межсетевых экранах. Например, уже упоминаемые BlackICE Agent и Defender, позволяют отследить злоумышленника, осуществляющего атаку на защищаемый компьютер, и собрать о хакере следующую информацию:

- IP-, DNS-, WINS-, NetBIOS- и MAC-адреса компьютера, с которого осуществляется атака;
- имя, под которым злоумышленник вошел в сеть.

Немаловажной является возможность удаленного обновления программного обеспечения персонального межсетевого экрана (например, в VPN-1 SecureClient). В противном случае администратору приходилось бы самостоятельно посещать каждого из владельцев компьютера и обновлять его защитное ПО. Представьте, какую бурю возмущений это вызвало бы у владельцев компьютеров, которых отрывали бы от своей работы. Удаленное же и, главное, незаметное для владельца компьютера, обновление (включая и обновление сигнатур атак и вирусов) снимает эту проблему и облегчает нелегкий труд администратора безопасности. Осуществляя удаленное управление, не стоит забывать и о защите трафика, передаваемого между центральной консолью и удаленными агентами. Злоумышленник может перехватить или подменить эти команды, что нарушит защищенность удаленных узлов.

В заключение данного раздела нужно сказать, что правильный выбор персонального или распределенного межсетевого экрана позволит повысить защищенность компьютеров, которые при обычных условиях остаются незащищенными и могут служить точкой проникновения в корпоративную сеть.

### 3.2 Системы контроля содержания

Межсетевые экраны позволяют контролировать доступ сотрудников компании к внешним ресурсам по их IP-адресам. Однако представьте, что на одном сервере находится запрещенная и разрешенная информация. В таком случае межсетевому экрану придется либо разрешить полный доступ к этому сайту, либо полностью его запретить, что не всегда возможно. Другая проблема, которую не могут предотвратить межсетевые экраны - передача конфиденциальной информации за пределы компании. Согласно некоторым исследованиям за последний год до 90% организаций, имеющих доступ в Internet, сталкивались с такими случаями. Причем такая передача может осуществлять, как в сообщениях электронной почты, так и просто обращаясь к какому-либо внешнему Web-серверу (с помощью скрытого сценария или Java-апплета) или передавая ее через почтовый ящик на Web-сервере (например, на www.hotmail.com или mail.yahoo.com). И не забывайте про вирусы, троянские кони, загрузку порнографии и т.д. Если вы скажете, что эти напасти вам не грозят, то давайте обратимся к статистике:

1. Согласно данным ФБР и Института компьютерной безопасности США 97% организаций столкнулись с злоупотреблениями сотрудников в области использования Internet. По данным eMarketer.com 32.6% пользователей, «блуждающих» по Internet, не имеют никакой конкретной цели и «ходят по Сети просто так».
2. Потери, вследствие непроизводительного использования Internet (в США), составляют до 96000 долларов в год (на одного сотрудника). Вы можете и сами рассчитать эти потери. Просто умножьте часовую (среднее ежедневное время, которое проводят сотрудники в Internet в своих личных целях) зарплату сотрудника на количество рабочих дней в году. Вы убедитесь, что цифры получаются немалые.
3. 80% компаний сталкиваются с тем, что их сотрудники передают личные данные, использую корпоративную электронную почту.
4. 28% пользователей осуществляют покупки в Internet в рабочее время.
5. Основной объем порнотрафика (70%) передается именно в рабочие часы (с 9 утра до 5 вечера).

Все это приводит к снижению прибыли компании и, даже, потере имиджа из-за случайно отправленных не по адресу писем с нецензурной лексикой или содержащих вирусы и троянские кони.

Для защиты от такого рода напастей недостаточно применять обычные антивирусные системы и межсетевые экраны. Нужны другие средства, к которым можно отнести и системы контроля содержимого (content filtering). Как говорится в отчете консалтинговой компании IDC: «Это больше, чем антивирус. Это больше, чем блокировка URL». Эти технологии в той или иной мере используются во многих средствах сетевой безопасности. В частности, в

системе обнаружения атак RealSecure компании Internet Security Systems или в межсетевом экране Check Point Next Generation компании Check Point Software. Но реализованные в этих средствах механизмы отрывочны и не охватывают весь спектр возможных угроз. И это понятно. Они не предназначены для решения этой задачи и контроль содержимого для них дополнительный механизм, расширяющий спектр их применения. Нужны специальные средства, ориентированные на решение только этой задачи, что позволяет полностью сконцентрироваться на ней.

В последнее время системы контроля содержания стали очень активно применяться в корпоративных сетях. И это немудрено. При своей достаточно невысокой стоимости они позволяют обнаружить действия, которые могут привести к несоизмеримо большему ущербу.

- ✓ **Возможности средств контроля содержимого**

Существует большое число средств контроля содержимого, но все они используют схожие возможности, которые можно разделить на две основных категории:

1. Контроль почтового трафика.
2. Контроль Web-трафика.

В свою очередь в каждой из этих категорий реализуются свои возможности, которые мы бы и хотели перечислить:

1. Обнаружение спама. Данная возможность позволяет путем анализа в сообщениях типовых слов и фраз обнаруживать попытки рассылки спама. Анализ проводится не только в тексте сообщения, но и в заголовке и даже во вложениях, передаваемых в рамках сообщения. Некоторые системы (например, MAILsweeper for SMTP) позволяю создавать списки спамеров и даже блокировать сообщения, получаемые от них.
2. Анализ содержания сообщения. Это наиболее распространенная и типичная возможность, присущая системам контроля содержания, с помощью которой можно, путем поиска ключевых слов и фраз, обнаруживать утечку конфиденциальной информации, оскорбления и другие нарушения политики безопасности.
3. Обнаружение подмены адреса. Т.к. зачастую злоумышленники, в т.ч. и спамеры, пытаются подменить исходный адрес своих сообщениях, то некоторые системы контроля содержимого пытаются обнаруживать такие попытки.
4. Анализ размера сообщений и вложений. Если центральный или удаленные офисы компании подключается к сети Internet по низкопроизводительным каналам, то часто бывает необходимо ограничить объемы передаваемого трафика, что и реализуется с помощью указанной возможности. При этом пересылка сообщений, размер которых

превышает указанные в политике безопасности значения, могут отбрасываться, а могут блокироваться до тех пор, пока напряженность передаваемого трафика спадет.

5. Обнаружение вирусов и троянских коней. Эта возможность также является одной из самых распространенных. При этом обнаружение вирусов и других враждебных элементов (троянцев, Java и т.д.) осуществляется с помощью как собственных антивирусных подсистем, так и с помощью продуктов третьих фирм.

6. Анализ передаваемых файлов. В сообщениях электронной почты могут передаваться различные файлы, начиная от договоров и списков цен и заканчивая порнографическими картинками и музыкальными записями. Для того чтобы разрешать прохождение одних и запрещать прохождение других файлов, используется механизм анализа передаваемых файлов. При этом анализ может происходить как на основе расширения и имени файла, так и на основе самой структуры файла. Такая возможность присутствует во многих системах контроля содержания, но число распознаваемых форматов разнится от производителя к производителю. Например, семейство MIMEsweeper поддерживает следующие форматы:

- Архивы ARJ, ZIP, GZIP, TAR, RAR, LZH, CMP, BinHex, CAB, MIME, UUE, TNEF и т.д.
- Документы Word, Excel, PowerPoint, Acrobat, HTML, RTF, CDA, FAX, OLE, TXT и т.д.
- Исполняемые файлы DOS, Windows, байт-код Java.
- Графические изображения JPG, GIF, BMP, TIF, PIC, PNG, PSP, DWG, PCX, FLI, DXF
- Аудио-файлы MIDI, AIF, VOC, AU, WAV, MP3.
- Видео-файлы RM, MPEG, QTM, AVI.
- Шифрованные сообщения S/MIME, PGP.

7. Анализ вложений. Данная возможность позволяет не ограничиваться анализом текста сообщения электронной почты или HTML-страницы, но и анализировать содержание передаваемых файлов. Например, с помощью этой возможности можно обнаружить передачу документов, содержащих строку "СТРОГО КОНФИДЕНЦИАЛЬНО" или распознать в графическом изображении порнографию, как это, например, делает PORNsweeper.

8. Анализ скрытых HTML. Сейчас стало распространенным рассылать сообщения электронной почты не путем обычного текста, а виде HTML-страниц, что делает сообщения красочными и удобочитаемыми. Однако такая красота скрывает и ряд опасностей. Например, с помощью скрытого сценария в HTML-странице можно украсть

пароли или реализовать атаку типа "отказ в обслуживании". Некоторые системы контроля содержимого позволяют обнаруживать такие страницы и, в зависимости от требований политики безопасности, блокировать или разрешать их.

9. Блокировка доступа к определенным URL. Хотя возможность блокирования доступа к сайтам, содержащим материалы, противоречащие политике безопасности, может быть реализована и с помощью межсетевого экрана, но, как было показано в начале главы, в них этот механизм ограничен. Кроме того, очень неудобно указывать в правилах доступа IP-адреса запрещенных сайтов, число которых может насчитывать тысячи.

10. Анализ содержания HTML-страницы. Не всегда есть возможность задания конкретных адресов запрещенных сайтов или страниц. Поэтому некоторые системы контроля содержимого позволяют обнаруживать в страницах, к которым идет обращение, ключевые слова и фразы и, в случае превышения заданного порога вхождений, блокировать доступ к этой странице (в т.ч. и к динамически созданной).

✓ **Недостатки**

Разумеется, говоря о возможностях систем контроля содержания, нельзя не упомянуть и их недостатках. В первую очередь, это невозможность контроля зашифрованных сообщений. Поэтому во многих компаниях запрещается неконтролируемая передача таких сообщений. Вторая проблема - трудности с заданием адресов запрещенных страниц. Во-первых, необходимо держать такой список в актуальном состоянии, а во-вторых, существует способ нестандартного задания адресов, который позволяет обойти защитный механизм системы контроля содержания. Допустим, что мы хотим ограничить доступ к сайту www.playboy.com, что и указываете в настройках системы контроля содержания. Однако пользователь может использовать не доменное имя, что делается в абсолютном большинстве случаев, а IP-адрес (209.247.228.201) этого сервера. В случае отсутствия межсетевого экрана блокировать такой доступ будет сложно. Но на этом проблемы не заканчиваются. Пользователь может использовать десятичное значение этого адреса - 3522684105, что также позволит без проблем обращаться к интересующим его страницам.

### 3.3 Системы контроля целостности

Если, несмотря на использование "классических" систем обнаружения атак и другие предпринятые защитные меры злоумышленник все-таки проник в защищаемую систему, то, как правило, он попытается установить программы типа "троянский конь", изменить системные файлы или отключить систему защиты. В абсолютном большинстве случаев, все

эти действия реализуются путем изменения каких-либо файлов (исполняемых, конфигурационных, динамических библиотек, драйверов и т.п.).

Целевой анализ (target-based) (также известный как контроль целостности файлов) использует пассивные, не оказывающие заметного влияния на работу контролируемой системы методы для проверки целостности системы и файлов данных, а также объектов системы и их атрибутов (например, потоки данных, базы данных и ключи системного реестра). Системы контроля целостности используют криптографические проверки контрольных сумм для того, чтобы получить доказательства подделки для наиболее важных системных объектов и файлов. Алгоритмы этих проверок основаны на хэш-функциях, которые обладают тем свойством, что даже незначительные изменения во входных данных функции создают большие различия в результате. Это означает, что незначительное изменение в потоке входных данных приведет к тому, что алгоритм контроля целостности создает значительное изменение в контрольной сумме, генерируемой алгоритмом. Эти алгоритмы являются криптографически стойкими; то есть, при заданном конкретном входном значении (величине), практически невозможно сравняться с другим входным значением для алгоритма, которое будет создавать идентичное выходное значение. Это предотвращает наиболее распространенную атаку против сравнительно простых алгоритмов генерации контрольных сумм (CRC), при которых хакеры маскируют изменения в содержании файла, так что одинаковая контрольная сумма создается как для оригинального, так и для подделанного файла.

Системы контроля целостности работают по замкнутому циклу, обрабатывая файлы, системные объекты и атрибуты системных объектов с целью получения контрольных сумм; затем они сравнивают их с контрольными суммами, полученными на предыдущем цикле, отыскивая изменения. Когда изменение обнаружено, продукт посылает сообщение администратору безопасности, при этом фиксируя время, соответствующее времени вероятного изменения.

Контроль целостности позволяет реализовать стратегию эффективного мониторинга, сфокусированную на системах, в которых целостность данных и целостность процессов играет наиболее важную роль (например, системы управления базами данных). Этот подход позволяет контролировать конкретные файлы, системные объекты и атрибуты системных объектов на происходящие изменения, обращая особое внимание скорее на конечный результат атаки, а не на подробности развития атаки.

| **Достоинства** | **Недостатки** |
|---|---|
| Любая успешная атака, при которой | Поскольку современные реализации |

| | |
|---|---|
| были изменены файлы, даже если использовались rootkits или перехватчики сетевых пакетов, будет определяться независимо от того, использовался ли для определения атаки анализ сигнатур или статистический анализ. | этого подхода стремятся работать в пакетном (batch)-режиме, они приводят к реагированию на атаки не в реальном масштабе времени. |
| Поскольку нет зависимости от старых записей режимов работы, контроль целостности может обнаруживать атаки, которые другие методологии определить не могут. | В зависимости от количества файлов, системных объектов и атрибутов объектов, для которых вычисляются контрольные суммы, этот подход может все же оказать заметное влияние на производительные системы. |
| Этот подход допускает надежное обнаружение, как местоположения, так и наличия атак, которые видоизменяют систему (например, "троянских коней"). | Этот подход не очень хорошо подходит для осуществления обнаружения в реальном масштабе времени, поскольку он контролирует результаты атак, а не сами атаки, когда они находятся в развитии. |
| Из-за того, что собственные воздействия и влияния данного механизма являются незначительными, этот подход может быть полезным для мониторинга систем с умеренной полосой пропускания для обработки данных. | |
| Этот подход является эффективным для определения того, какие файлы необходимо заменить для того, чтобы восстановить систему, а не переинсталлировать все с оригинального источника или с резервной копии, как это часто делается. | |

### 3.4 Системы построения VPN

Из пункта А в пункт Б необходимо передать информацию таким образом, чтобы к ней никто не смог получить доступ. Вполне реальная и часто возникающая на практике ситуация, особенно в последнее время. В качестве пунктов А и Б могут выступать отдельные узлы или целые сегменты сетей. В случае с передачей информации между сетями в качестве защитной меры может выступать выделенный канал связи, принадлежащей компании, информация которой требует защиты. Однако поддержание таких каналов связи - это очень дорогое удовольствие. Проще, если информация будет передаваться по обычным каналам связи (например, через Internet), но каким-либо способом будет отделена или скрыта от трафика других компаний, циркулирующего в Internet. Но не стоит думать, что задача конфиденциальной передачи информации возникает в глобальных сетях. Такая потребность может возникнуть и в локальных сетях, в которых требуется отделать один тип трафика, от другого (например, трафик платежной системы от трафика информационно-аналитической системы). Итак, как сделать так, чтобы информация могла передаваться по тем же проводам, что и обычная информация, но при этом была недоступна для других? Помочь в этом может технология виртуальных частных сетей (virtual private network, VPN).

✓ **Классификация**

Однако мы понимаем эту технологию несколько шире, чем ее толкуют другие. Ведь по сути неважно, каким образом вы скрываете одни данные от других. Поэтому можно выделить два основных способа реализации VPN:

1. Разделение трафика в канале передачи.
2. Шифрование трафика в канале передачи.

✓ Разделение трафика в канале передачи

Первая технология достаточно недавно получила широкое распространение. Она может применяться как в глобальных, так и в локальных сетях. Причем второй случай распространен чаще - это всем известная технология виртуальных локальных сетей (VLAN), используемая для структуризации современных локальных сетей, построенных на базе коммутаторов. Однако помимо структуризации VLAN могут применяться и для отделения одного типа трафика от другого. Т.к. VLAN реализуются на канальном уровне, то их область применения не выходит за рамки локальной сети, но и тут они неплохо справляются со своими задачами. В частности, независимо от адреса канального уровня (уникального, группового или широковещательного) смешение данных из разных VLAN невозможно. В то же время внутри одной VLAN кадры передаются как обычно, только на тот порт, на который указывает адрес назначения кадра.

Узлы, входящие в VLAN могут группироваться на основе различных признаков:

1. Группировка по портам. Классический и самый простой способ формирования VLAN, согласно которому каждому порту коммутатора соответствует номер VLAN.

2. Группировка по MAC-адресам. Принадлежность к VLAN определяется по MAC-адресам сетевых пакетов.

3. Группировка по номерам подсетей сетевого уровня. В данном случае VLAN является аналогом обычной подсетью, которая известна по протоколам IP или IPX.

4. Группировка по меткам. Самый эффективный и надежный способ группирования узлов в VLAN, согласно которому номер виртуальной сети добавляется к кадру, передаваемому между коммутаторами.

Существуют и другие способы формирования VLAN, но все они менее распространены, чем вышеназванные. Технология VLAN реализована сейчас в большинстве коммутаторов ведущих сетевых производителей.


Рисунок 3.1 Разделение трафика в канале передачи

В глобальных сетях распространение получил аналог VLAN - технология MPLS (MultiProtocol Label Switching), которая также использует метки для разделения трафика и образования виртуальных каналов в IP-, ATM- и других сетях. Однако у технологии MPLS есть один недостаток (с точки зрения безопасности) - он может применяться только для связи "сеть - сеть" и не применим для соединения с отдельными узлами. Есть и второй недостаток - данные разных пользователей хоть и не смешиваются, но все-таки к ним можно получить данные, прослушивая сетевой трафик. Кроме того, провайдер, предлагающий услуги MPLS будет иметь доступ ко всей передаваемой информации. Однако данные технологии все же имеют право на существование, т.к. обеспечивают некоторый уровень защищенности информации и достаточно дешевы. Основным поставщиком MPLS является компания Cisco Systems.

- ✓ **Шифрование трафика в канале передачи**

Большую известность получила технология шифрования трафика, которая скрывает от глаз содержание данных, передаваемых по открытым сетям. Именно эта технология применяется многими разработчиками средств сетевой безопасности.


Рисунок 3.2 Шифрование трафика в канале передачи

- ✓ **Варианты построения**

Можно выделить четыре основных варианта построения сети VPN, которые используются во всем мире. Данная классификация предлагается компанией Check Point Software Technologies, которая считается законодателем моды в области VPN.

1. Вариант «Intranet VPN», который позволяет объединить в единую защищенную сеть несколько распределенных филиалов одной организации, взаимодействующих по открытым каналам связи. Именно этот вариант получил широкое распространение во всем мире, и именно его в первую очередь реализуют компании-разработчики.
2. Вариант "Remote Access VPN", который позволяет реализовать защищенное взаимодействие между сегментом корпоративной сети (центральным офисом или филиалом) и одиночным пользователем, который подключается к корпоративным ресурсам из дома (домашний пользователь) или через notebook (мобильный пользователь). Данный вариант отличается от первого тем, что удаленный пользователь, как правило, не имеет статического адреса, и он подключается к защищаемому ресурсу не через выделенное устройство VPN, а прямиком со своего собственного компьютера, на котором и устанавливается программное обеспечение, реализующее функции VPN.Компонент VPN для удаленного пользователя может быть выполнен как в программном, так и в программно-аппаратном виде. В первом случае программное обеспечение может быть как встроенным в операционную систему (например, в Windows 2000), так и разработанным специально. Во втором случае для реализации VPN используются небольшие устройства класса SOHO (Small Office\Home Office), которые не требуют серьезной настройки и могут быть использованы даже

неквалифицированным персоналом. Такие устройства получают сейчас широкое распространение за рубежом.

3. Вариант «Client/Server VPN», который обеспечивает защиту передаваемых данных между двумя узлами (не сетями) корпоративной сети. Особенность данного варианта в том, что VPN строится между узлами, находящимися, как правило, в одном сегменте сети, например, между рабочей станцией и сервером. Такая необходимость очень часто возникает в тех случаях, когда в одной физической сети необходимо создать несколько логических сетей. Например, когда надо разделить трафик между финансовым департаментом и отделом кадров, обращающихся к серверам, находящимся в одном физическом сегменте. Этот вариант похож на технологию VLAN, описанную выше. Но вместо разделения трафика, используется его шифрование.

4. Последний вариант «Extranet VPN» предназначен для тех сетей, к которым подключаются так называемые пользователи "со стороны" (партнеры, заказчики, клиенты и т.д.), уровень доверия к которым намного ниже, чем к своим сотрудникам. Хотя по статистике чаще всего именно сотрудники являются причиной компьютерных преступлений и злоупотреблений.

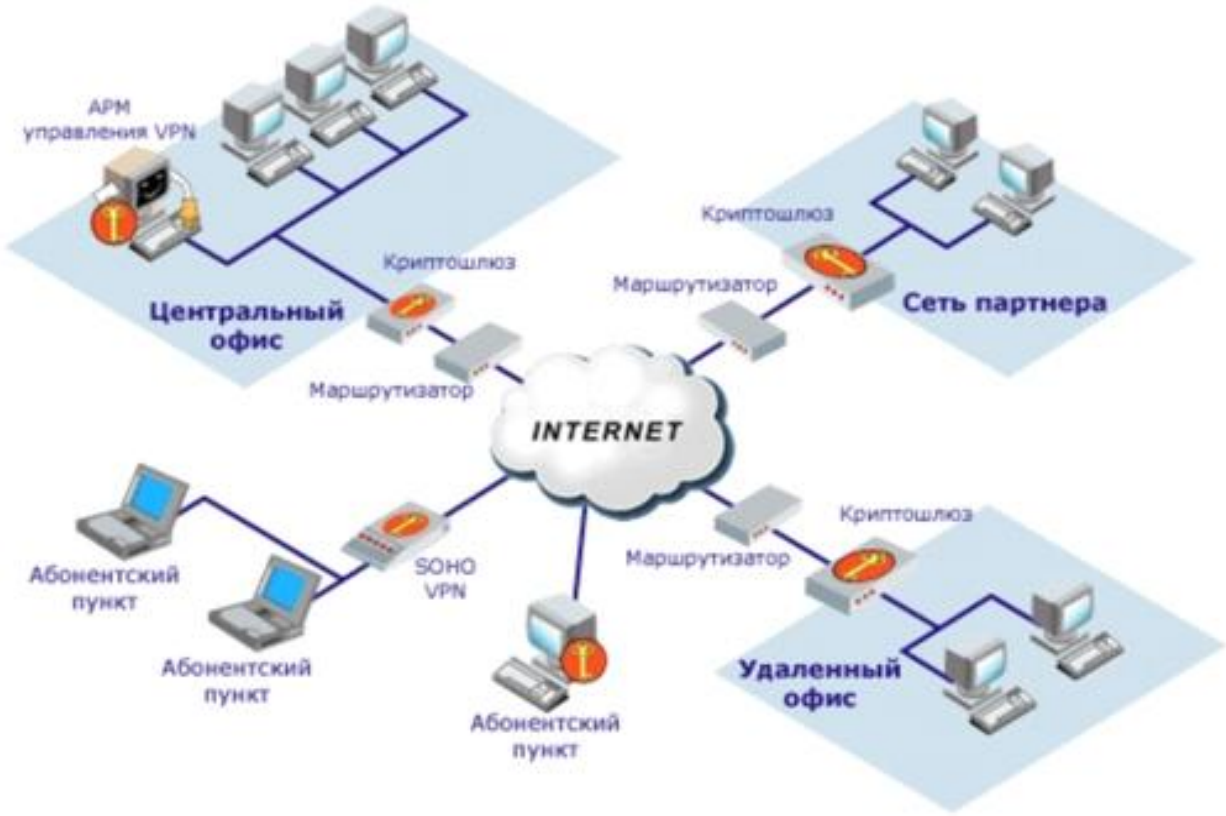



Рисунок 3.3. Вариант «Intranet VPN»

✓ Варианты реализации

Средства построения VPN могут быть реализованы по-разному:

1. В виде специализированного программно-аппаратного обеспечения, предназначенного именно для решения задач VPN. Основное преимущество таких устройств - их высокая производительность и, более высокая по сравнению с другими решениями, защищенность. Такие устройства могут применяться в тех случаях, когда необходимо обеспечить защищенный доступ большого числа абонентов. Недостаток таких решений состоит в том, что управляются они отдельно от других решений по безопасности, что усложняет задачу администрирования инфраструктуры безопасности, особенно при условии нехватки сотрудников отдела защиты информации. На первое место эта проблема выходит при построении крупной и территориально-распределенной сети, насчитывающей десятки устройств построения VPN. И это не считая такого же числа межсетевых экранов, систем обнаружения атак и т.д. Примером такого решения является Cisco 1720 или Cisco 3000.

2. В виде программного решения, устанавливаемого на обычный компьютер, функционирующий, как правило, под управлением операционной системы Unix. Российские разработчики «полюбили» ОС FreeBSD. Именно на ее изученной «вдоль и поперек» базе построены отечественные решения «Континент-К» и «Шип». Для ускорения обработки трафика могут быть использованы специальные аппаратные ускорители, заменяющие функции программного шифрования. Также в виде программного решения реализуется абонентские пункты, предназначенные для подключения к защищаемой сети удаленных и мобильных пользователей.

3. Интегрированные решения, в которых функции построения VPN реализуются наряду с функцией фильтрации сетевого трафика, обеспечения качества обслуживания или распределения полосы пропускания. Основное преимущество такого решения - централизованное управление всеми компонентами с единой консоли. Второе преимущество - более низкая стоимость в расчете на каждый компонент по сравнению с ситуацией, когда такие компоненты приобретаются отдельно. Пожалуй, самым известным примером такого интегрированного решения является VPN-1 от компании Check Point Software, включающий в себя помимо VPN-модуля, модуль, реализующий функции межсетевого экрана, модуль, отвечающий за балансировку нагрузки, распределение полосы пропускания и т.д. Кроме того, это решение имеет сертификат Гостехкомиссии России.

- ✓ **Зачем нужна VPN?**

Помимо обеспечения защиты от посторонних передаваемых данных, VPN несет с собой и ряд других преимуществ. В том числе и экономических. Например, исследовательская компания Forrester Research опубликовала следующие данные, характеризующие

преимущество применения VPN поверх Internet (из расчета 1000 пользователей) по сравнению с созданием центра удаленного доступа (Remote Access Service).

| **Статья затрат** | **Удаленный доступ (в млн. долл.)** | **VPN (в млн. долл.)** |
|---|---|---|
| Оплата услуг провайдера связи | 1,08 | 0,54 |
| Расходы на эксплуатацию | 0,3 | 0,3 |
| Капиталовложения | 0,1 | 0,02 |
| Прочие расходы | 0,02 | 0,03 |
| Всего | 1,5 | 0,89 |

Из таблицы можно видеть, что использование VPN позволяет снизить многие статьи затрат, включая закупку коммуникационного оборудования, оплату услуг Internet-провайдера и т.д. Эти, а также другие исследования, позволили Международной Ассоциации Компьютерной Безопасности (International Computer Security Association, ICSA) причислить технологию VPN к десятке самых известных технологий, которые будут в первую очередь применяться многими компаниями. Это подтверждает и компания Gartner Group, которая в одном из своих отчетов предсказала, что средства построения VPN будут применяться в 2002 г. в 90% компаний. Именно с этим связан прогноз рынка средств VPN, который исчисляется 11,94 миллиардами долларов в 2002 году и 18,77 миллиардами в 2004 году (по данным Frost & Sullivan).

### 3.5 Системы обнаружения атак

Обнаруживать, блокировать и предотвращать атаки можно несколькими путями. Этот способ применяется в "классических" системах обнаружения атак (например, RealSecure Network Sensor или Cisco Secure IDS), межсетевых экранах (например, Check Point Firewall-1), системах защиты информации от НСД (например, SecretNet) и т.п. Однако, "недостаток" средств данного класса в том, что атаки могут быть реализованы повторно. Они также повторно обнаруживаются и блокируются. И так далее, до бесконечности, что само собой разумеется, неэффективно, так как приводит к непозволительной трате временных, человеческих и материальных ресурсов. Было бы эффективнее предотвращать атаки еще до их реализации. Это и есть второй путь. Осуществляется он путем поиска уязвимостей (то есть, обнаружение потенциальных атак), которые могут быть использованы для реализации

атаки. И, наконец, третий путь, - обнаружение уже совершенных атак и предотвращение их повторного осуществления. Таким образом, системы обнаружения нарушений политики безопасности могут быть классифицированы по этапам осуществления атаки (Рисунок 1):

1. Системы, функционирующие на первом этапе осуществления атак и позволяющие обнаружить уязвимости информационной системы, используемые нарушителем для реализации атаки. Иначе средства этой категории называются системами анализа защищенности (security assessment systems) или сканерами безопасности (security scanners). Примером такой системы является Internet Scanner или SATAN. Некоторые авторы считают неправильным отнесение систем анализа защищенности к классу средств обнаружения атак, однако, если следовать описанным выше принципам классификации, то такое отнесение вполне логично.

2. Системы, функционирующие на втором этапе осуществления атаки и позволяющие обнаружить атаки в процессе их реализации, то есть в режиме реального (или близкого к реальному) времени. Именно эти средства и принято считать системами обнаружения атак в классическом понимании. Примером такой системы является RealSecure или Cisco Secure IDS. Помимо этого в последнее время выделяется новый класс средств обнаружения атак - обманные системы (deception systems), которые более подробно будут описаны ниже. Примером такой системы является RealSecure OS Sensor или DTK.

3. Системы, функционирующие на третьем этапе осуществления атаки и позволяющие обнаружить уже совершенные атаки. Эти системы делятся на два класса - системы контроля целостности (integrity checkers), обнаруживающие изменения контролируемых ресурсов, и системы анализа журналов регистрации (log checkers). В качестве примеров таких систем могут быть названы Tripwire или RealSecure Server Sensor.


Рисунок 3.4 Классификация систем обнаружения атак по этапам осуществления атаки

Помимо этого, существует еще одна распространенная классификация систем обнаружения нарушения политики безопасности - по принципу реализации: host-based, т.е. обнаруживающие атаки, направленные на конкретный узел сети, и network-based, направленные на всю сеть или сегмент сети. Обычно на этом дальнейшая классификация останавливается. Однако системы класса host-based можно разделить еще на три подуровня:

1. Системы обнаружения атак на уровне прикладного ПО (application-based), обнаруживающие атаки на конкретные приложения (например, на Web-сервер). Примером такой системы является RealSecure OS Sensor или WebStalker Pro.
2. Системы обнаружения атак на уровне ОС (OS-based), обнаруживающие атаки на уровне операционной системы. Примером такой системы является RealSecure Server Sensor или Intruder Alert.
3. Системы обнаружения атак на уровне системы управления базами данных (DBMS-based), обнаруживающие атаки на конкретные СУБД.

Выделение обнаружения атак на системы управления базами данных (СУБД) в отдельную категорию связано с тем, что современные СУБД уже вышли из разряда обычных прикладных приложений и по многим своим характеристикам, в том числе и по сложности, приближаются к операционным системам. При этом системы обнаружения атак (точнее системы анализа защищенности) на уровне СУБД могут функционировать как на самом узле, так и через сеть (например, Database Scanner). В свою очередь система обнаружения атак на уровне сети может функционировать и на конкретном узле, обнаруживая атаки, направленные не на все узлы сегмента, а только на тот узел, на котором она установлена. Пример такой системы - RealSecure Server Sensor.


Рисунок 3.5 Классификация систем обнаружения атак по принципу реализации

### 3.6 Системы анализа защищенности

Системы анализа защищенности, также известные как сканеры безопасности или системы поиска уязвимостей, проводят всесторонние исследования систем с целью обнаружения уязвимостей, которые могут привести к нарушениям политики безопасности. Результаты, полученные от средств анализа защищенности, представляют "мгновенный снимок" состояния защиты системы в данный момент времени. Несмотря на то, что эти системы не могут обнаруживать атаку в процессе ее развития, они могут определить потенциальную возможность реализации атак.

Функционировать системы анализа защищенности могут на всех уровнях информационной инфраструктуры, т.е. на уровне сети, операционной системы, СУБД и прикладного программного обеспечения. Наибольшее распространение получили средства анализа защищенности сетевых сервисов и протоколов. Связано это, в первую очередь, с универсальностью используемых протоколов. Изученность и повсеместное использование таких стеков протоколов, как TCP/IP, SMB/NetBIOS и т.п. позволяют с высокой степенью эффективности проверять защищенность информационной системы, работающей в данном сетевом окружении, независимо от того, какое программное обеспечение функционирует на более высоких уровнях. Вторыми по распространенности являются средства анализа защищенности операционных систем. Связано это также с универсальностью и распространенностью некоторых операционных систем (например, UNIX и Windows NT). Однако, из-за того, что каждый производитель вносит в операционную систему свои изменения (ярким примером является множество разновидностей ОС UNIX), средства анализа защищенности ОС анализируют в первую очередь параметры, характерные для всего семейства одной ОС. И лишь для некоторых систем анализируются специфичные для нее параметры. Средств анализа защищенности СУБД и приложений на сегодняшний день не так много, как этого хотелось бы. Такие средства пока существуют только для широко распространенных прикладных систем, типа Web-броузеров Netscape Navigator и Microsoft Internet Explorer, СУБД Microsoft SQL Server и Oracle, Microsoft Office и BackOffice и т.п.

При проведении анализа защищенности эти системы реализуют две стратегии. Первая - пассивная, - реализуемая на уровне операционной системы, СУБД и приложений, при которой осуществляется анализ конфигурационных файлов и системного реестра на наличие неправильных параметров; файлов паролей на наличие легко угадываемых паролей, а также других системных объектов на предмет нарушения политики безопасности. Вторая стратегия, - активная, - осуществляемая в большинстве случаев на сетевом уровне, позволяющая воспроизводить наиболее распространенные сценарии атак, и анализировать реакции системы на эти сценарии.

✓ **Классификация:**

**1. По уровням информационной системы**

Аналогично системам анализа защищенности, системы обнаружения атак также можно классифицировать по уровню информационной инфраструктуры, на котором обнаруживаются нарушения политики безопасности.

**2. На уровне приложений и СУБД**

Системы обнаружения атак данного уровня собирают и анализируют информацию от конкретных приложений, например, от систем управления базами данных, Web-серверов или межсетевых экранов, например, WebStalker Pro или RealSecure Server Sensor.

| **Достоинства** | **Недостатки** |
|---|---|
| Этот подход позволяет нацелиться на конкретные действия в системе, необнаруживаемые другими методами (например, мошенничество конкретного пользователя в платежной системе). | Уязвимости прикладного уровня могут подорвать доверие к обнаружению атак на данном уровне. |
| Обнаружение атак, пропускаемых средствами, функционирующими на других уровнях. | Атаки, реализуемые на нижних уровнях (сети и ОС) остаются за пределами рассмотрения данных средств. |
| Эти средства позволяют снизить требования к ресурсам за счет контроля не всех приложений, а только одного из них. | |

**3. На уровне ОС**

Системы обнаружения атак уровня операционной системы собирают и анализируют информацию, отражающую деятельность, которая происходит в операционной системе на отдельном компьютере (например, RealSecure Server Sensor или Intruder Alert). Эта информация представляется, как правило, в форме журналов регистрации операционной системы. В последнее время стали получать распространение системы, функционирующие на уровне ядра ОС, тем самым, предоставляя более эффективный способ обнаружения нарушений политики безопасности. К такого рода системам можно отнести LIDS.

| **Достоинства** | **Недостатки** |
|---|---|
| Системы данного класса могут | Уязвимости ОС могут подорвать |

| | |
|---|---|
| контролировать доступ к информации в виде "кто получил доступ и к чему". | доверие к обнаружению атак на данном уровне. |
| Системы данного класса могут отображать аномальную деятельность конкретного пользователя для любого приложения. | Атаки, реализуемые на нижних или более высоких уровнях (сети и приложений) остаются за пределами рассмотрения данных средств. |
| Системы данного класса могут отслеживать изменения режимов работы, связанные со злоупотреблениями. | Запуск механизмов аудита для фиксирования всех действий в журналах регистрации может потребовать использования дополнительных ресурсов. |
| Системы данного класса могут работать в сетевом окружении, в котором используется шифрование. | Когда журналы регистрации используются в качестве источников данных, они могут потребовать довольно большого дискового пространства для хранения. |
| Системы данного класса могут эффективно работать в коммутируемых сетях. | Эти методы зависят от типа конкретной платформы. |
| Позволяют контролировать конкретный узел и "не распыляться" на другие, менее важные, узлы. | Расходы на стоимость эксплуатации и управление, связанные со средствами обнаружения атак уровня операционной системы, как правило, значительно выше, чем в других подходах. |
| 100%-е подтверждение "успешности" или "неудачности" атаки. | Средства данного класса практически неприменимы для обнаружения атак на маршрутизаторы и иное сетевое оборудование. |
| Обнаружение атак, пропускаемых средствами, функционирующими на других уровнях. | При неполноте данных эти системы могут "пропускать" какие-либо атаки. |
| Возможность проведения автономного анализа. | |

**4. На уровне сети**

Системы обнаружения атак уровня сети собирают информацию из самой сети, то есть из сетевого трафика. Выполняться эти системы могут на обычных компьютерах (например, RealSecure Network Sensor или NetProwler), на специализированных компьютерах (например, RealSecure for Nokia или Cisco Secure IDS) или интегрированы в маршрутизаторы или коммутаторы (например, CiscoSecure IOS Integrated Software или Cisco Catalyst 6000 IDS Module). В первых двух случаях анализируемая информация собирается посредством захвата и анализа пакетов, используя сетевые интерфейсы в беспорядочном (promiscuous) режиме.

| **Достоинства** | **Недостатки** |
|---|---|
| Данные поступают без каких-либо специальных требований для механизмов аудита. | Атаки, реализуемые на более высоких уровнях (ОС и приложений) остаются за пределами рассмотрения данных средств. |
| Использование систем данного класса не оказывает влияния на существующие источники данных. | Системы данного класса не применимы в сетях, использующих канальное и, тем более, прикладное шифрование данных. |
| Системы данного класса могут контролировать и обнаруживать сетевые атаки типа "отказ в обслуживании" (например, атаки типа SYN flood или packet storm), направленные на выведение узлов сети из строя. | Системы данного класса неэффективно работают в коммутируемых сетях. |
| Системы данного класса могут контролировать одновременно большое число узлов сети (в случае с разделяемыми средами передачи данных). | Системы данного класса существенно зависят от конкретных сетевых протоколов. |
| Системы данного класса могут эффективно работать в коммутируемых сетях. | Эти методы зависят от типа конкретной платформы. |
| Низкая стоимость эксплуатации. | Современные подходы к мониторингу на сетевом уровне не могут работать на высоких скоростях (например, Gigabit Ethernet). |
| Трудность "заметания следов" для злоумышленника. | |
| Обнаружение и реагирование на атаки в | |

| | |
|---|---|
| реальном масштабе времени. | |
| Обнаружение подозрительных событий (например, "чужих" IP-адресов). | |
| Обнаружение атак, пропускаемых средствами, функционирующими на других уровнях. | |
| Независимость от используемых в организации операционных систем и прикладного программного обеспечения, т.к. все они взаимодействуют при помощи универсальных протоколов. | |

**5. Интегрированные подходы**

Как мы уже отмечали выше, до недавнего времени все существующие системы обнаружения атак можно было отнести либо к классу сетевых (network-based), либо к классу узловых (host-based). Однако идеальным решением было бы создание системы, совмещающей в себе обе эти технологии, т.е. на каждый контролируемый узел устанавливался бы агент системы обнаружения атак и контролировал не только атаки на прикладном уровне (уровне ОС, СУБД и уровне приложений), но и сетевые атаки, направленные на данный узел. Этот подход имеет несколько преимуществ по сравнению с существующими решениями.

Во-первых, высокая сетевая скорость уже не представляет проблемы, поскольку указанный агент просматривает только трафик для данного узла вместо всего трафика всей сети. Во-вторых, расшифрование пакетов осуществляет прежде, чем они достигнут прикладного уровня. И, наконец, из-за того, что он размещается непосредственно на каждом контролируемом компьютере, коммутируемые сети также не накладывают ограничений на их использование.

Некоторые системы обнаружения атак объединяют в себе возможности каждого из средств, функционирующих на уровне сети, ОС, СУБД и прикладного ПО. К таким системам можно отнести RealSecure Server Sensor компании ISS и Centrax компании CyberSafe. Эти системы комбинируют характеристики сетевых сенсоров, работающих в реальном масштабе времени, с тактическими преимуществами сенсоров системного уровня.

✓ **Системы обнаружения атак на уровне узла**

Эти системы обнаружения атак выполняются на защищаемом узле и контролируют различные события безопасности. В качестве исходных данных указанные системы, в

большинстве случаев, оперируют регистрационными журналами операционной системы (например, Intruder Alert), приложений (например, RealSecure OS Sensor) или систем управления базами данных. Таким образом, эти системы зависят от содержимого регистрационных журналов и в случае их подмены злоумышленником или неполноты собранных данных система не сможет достоверно определить нападение. Менее распространенные системы обнаружения атак используют модель обнаружения аномального поведения (например, EMERALD), которая статистически сравнивает текущий сеанс пользователя (выполняемые команды и другие параметры) с эталонным профилем нормального поведения. Сложные алгоритмы используются для определения отклонения нормального поведения пользователя от аномального. Однако существуют системы обнаружения, которые оперируют сетевым трафиком, получаемым и отправляемым с конкретного узла (например, RealSecure Server Sensor).

Имеется несколько категорий систем обнаружения атак данного класса, функционирующих на различных уровнях ИС.

✓ ***Системы обнаружения атак на уровне операционной системы***

Эти системы основаны на мониторинге регистрационных журналов операционной системы, заполняемых в процессе работы пользователя или другого субъекта на контролируемом узле (например, RealSecure OS Sensor или swatch). В качестве критериев оценки несанкционированной деятельности используются:

- время работы пользователя;
- число, тип и название создаваемых файлов;
- число, тип и название файлов, к которым осуществляется доступ;
- регистрация в системе и выход из нее;
- запуск определенных приложений;
- изменение политики безопасности (создание нового пользователя или группы, изменение пароля и т.п.);
- и т.д.

События, записываемые в журнал регистрации, сравниваются с базой данных сигнатур при помощи специальных алгоритмов, которые могут меняться в зависимости от реализации системы обнаружения атак. Подозрительные события классифицируются, ранжируются и о них уведомляется администратор. Указанные системы обнаружения атак, как правило, запускаются на сервере, так как их запуск на рабочих станциях нецелесообразен из-за повышенных требований к системным ресурсам.

Иногда системы обнаружения атак этого уровня анализируют деятельность пользователей в реальном режиме времени (например, HostSentry компании Psionic), но этот

механизм реализуется достаточно редко. Обычно эти системы анализируют только журналы регистрации ОС.

Некоторые ОС (например, FreeBSD или Linux) поставляются в исходных текстах и разработчики систем обнаружения атак могут модифицировать ядро ОС для реализации возможности обнаружения несанкционированных действий. Примером таких систем можно назвать OpenWall или LIDS. Эти системы модифицируют ядро ОС Linux, расширяя имеющиеся защитные механизмы. Например, LIDS может обнаруживать и блокировать факт установки анализатора протоколов или изменения правил встроенного межсетевого экрана.

- ✓ **На уровне приложений и СУБД**

Системы данного класса могут быть реализованы двумя путями. В первом случае, они анализируют записи журнала регистрации конкретного приложения или СУБД и в этом случае мало чем отличаются от систем обнаружения атак на уровне ОС. Достоинство такого пути - в простоте реализации и поддержке практически любого прикладного ПО и СУБД, фиксирующего все события в журнале регистрации. Примером такой системы является RealSecure OS Sensor. Однако в этой простоте кроется и основной недостаток. Для эффективной работы такой системы необходимо потратить немало времени на ее настройку под конкретное приложение, так как каждое из них имеет свой, зачастую уникальный формат журнала регистрации. Второй путь реализации этих систем - интеграция их в конкретное прикладное приложение или СУБД. В этом случае они становятся менее универсальными, но зато более функциональными, за счет очень тесной интеграции с контролируемым ПО. Примером такой системы является WebStalker Pro, разработанной в компании Trusted Information Systems (TIS) и 28 февраля 1998 года приобретенной компанией Network Associates. К сожалению, в настоящий момент данная система больше не выпускается, а некоторые ее элементы интегрированы в систему CyberCop Monitor.

- ✓ ***На уровне сети***

Помимо анализа журналов регистрации или поведения субъектов контролируемого узла, системы обнаружения данного класса могут оперировать и сетевым трафиком. В этом случае система обнаружения анализируют не все сетевые пакеты, а только те, которые направлены на контролируемый узел. По этой причине сетевые интерфейсы данных узлов могут функционировать не только в "смешанном", но и в нормальном режиме. Поскольку такие системы контролируют все входящие и исходящие сетевые соединения, то они также могут исполнять роль персональных межсетевых экранов. Примером таких систем можно назвать RealSecure Server Sensor компании ISS или PortSentry компании Psionic.

✓ ***Достоинства систем обнаружения атак на уровне узла:***

1. Подтверждение факта атаки

Так как системы обнаружения атак, анализирующие журналы регистрации, содержат данные о событиях, которые действительно имели место, то системы этого класса могут с высокой точностью определить - действительно ли атака имела место или нет. В этом отношении системы уровня узла идеально дополняют системы обнаружения атак сетевого уровня, которые будут описаны дальше. Такое объединение обеспечивает раннее предупреждение при помощи сетевого компонента и определение "успешности" атаки при помощи системного компонента.

2**. Контроль деятельности конкретного узла**

Эти системы контролирует деятельность пользователя, доступ к файлам, изменения прав доступа к файлам, попытки установки новых программ и попытки получить доступ к привилегированным сервисам. Например, они могут контролировать все системные входы и выхода пользователя. Для системы сетевого уровня очень трудно, а зачастую и невозможно, обеспечить такой уровень детализации событий. Средства обнаружения атак на системном уровне могут также контролировать деятельность администратора, которая обычно никем не отслеживается. Операционные системы регистрируют любое событие, при котором добавляются, удаляются или изменяются учетные записи пользователей. Средства обнаружения атак данного класса могут обнаруживать соответствующее изменение сразу, как только оно происходит.

Кроме того системы обнаружения атак, функционирующие на уровне узла, могут контролировать изменения в ключевых системных или исполняемых файлах. Попытки перезаписать такие файлы или инсталлировать "троянских коней" могут быть своевременно обнаружены и пресечены. Системы сетевого уровня иногда упускают такой тип деятельности.

3. Обнаружение атак, не обнаруживаемых другими средствами

Системы данного класса могут обнаруживать атаки, которые не могут быть обнаружены средствами сетевого уровня. Например, атаки, осуществляемые с самого атакуемого сервера. Кроме того, некоторые системы (например, RealSecure Server Sensor) могут обнаруживать сетевые атаки, направленные на контролируемый узел, но по каким-либо причинам пропущенные системой обнаружения атак на уровне сети.

**4. Работа в коммутированных сетях и сетях с канальным шифрованием**

Поскольку данные средства обнаружения атак устанавливаются на различных узлах сети предприятия, они могут преодолеть некоторые из проблем, возникающие при эксплуатации систем сетевого уровня в коммутируемых сетях и сетях с канальным шифрованием.

Коммутация позволяет управлять крупномасштабными сетями, как несколькими небольшими сетевыми сегментами. В результате бывает трудно определить наилучшее место для установки системы, обнаруживающей атаки в сетевом трафике. Иногда могут помочь специальные порты (mirror ports, managed ports, span ports) на коммутаторах, но не всегда. Обнаружение атак на системном уровне обеспечивает более эффективную работу в коммутируемых сетях, так как позволяет разместить системы обнаружения только на тех узлах, на которых это необходимо.

Канальное шифрование также может являться проблемой для систем обнаружения атак сетевого уровня, так как они могут оставаться "слепыми" к определенным, зашифрованным атакам. Системы, работающие на уровне узла, не имеют этого ограничения, так как на уровень ОС поступает уже расшифрованный трафик.

### 5. Обнаружение и реагирование почти в реальном масштабе времени

Хотя обнаружение атак на системном уровне не обеспечивает реагирования в действительно реальном масштабе времени, оно, при правильной реализации, может быть осуществлено почти в реальном масштабе. В отличие от устаревших систем, которые проверяют статус и содержания журналов регистрации через заранее определенные интервалы, многие современные системы получают прерывание от ОС, как только появляется новая запись в журнале регистрации. Эта новая запись может быть обработана сразу же, значительно уменьшая время между распознаванием атаки и реагированием на нее. Остается задержка между моментом записи операционной системой события в журнал регистрации и моментом распознавания ее системой обнаружения атак, но во многих случаях злоумышленник может быть обнаружен и остановлен прежде, чем он нанесет какой-либо ущерб.

### 6. Низкая цена

Несмотря на то, что системы обнаружения атак сетевого уровня обеспечивают анализ трафика всей сети, очень часто они являются достаточно дорогими. Стоимость одной

системы обнаружения атак может превышать $10000. С другой стороны, системы обнаружения атак на уровне конкретного стоят сотни долларов за один агент и могут приобретаться покупателем по мере наращивания сети.

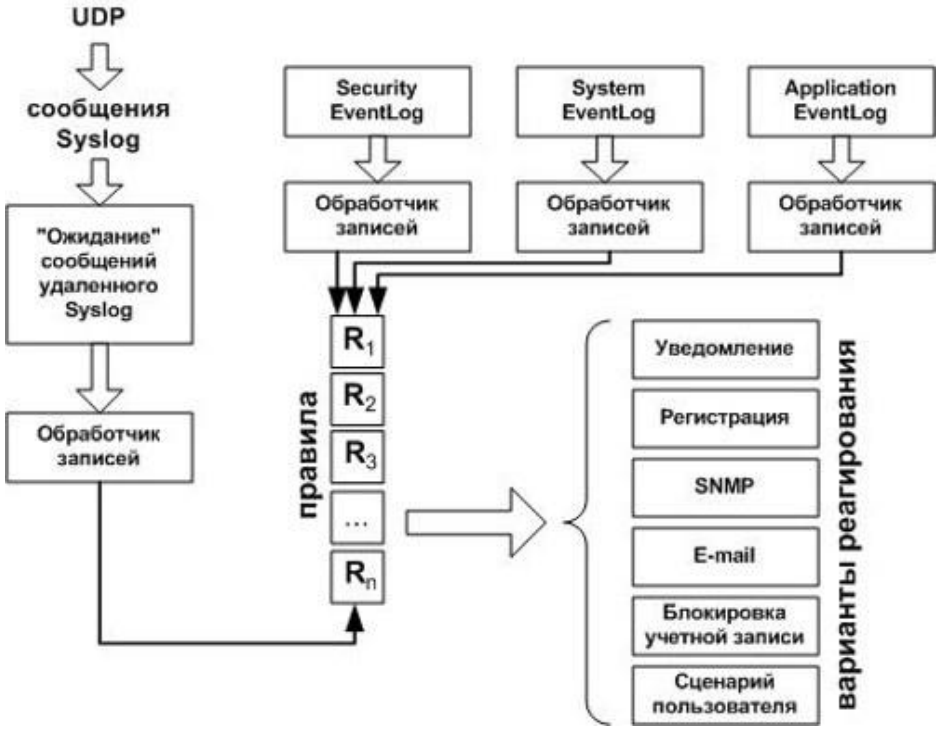



Рисунок 3.6 «Компоненты системы обнаружения атак на уровне узла»

- ✓ **Системы обнаружение атак на уровне сети**

Первоначальные исследования велись в области анализа регистрационных файлов, созданных операционной системой и различными приложениями. Этот анализ проводился с целью поиска записей, характеризующих потенциальное нападение или какую либо аномальную деятельность. Однако на практике оказалось, что системы обнаружения атак на основе регистрационных журналов не позволяют обнаруживать множество атак. Поэтому внимание разработчиков переключилось на сетевой уровень.

Основное ограничение первых разработанных систем обнаружения атак в том, что доступ к регистрационным журналам осуществлялся только на уровне ОС, СУБД и приложений. Развитие сетей, требующих контроля на всех уровнях инфраструктуры информационной системы, привел к созданию так называемых Kernel-based и Network-based систем обнаружения атак, то есть, работающих на уровне ядра ОС и уровне сети.

Система обнаружения атак на уровне сети за счет используемых в ней алгоритмов имеет доступ ко всем данным, передаваемым между узлами сети. Так как такая система выполняется на компьютере, отличном от того, атаки на который контролируются, то никакого снижения эффективности последних не наблюдается.

Как показывает анализ имеющихся сегодня систем обнаружения атак на уровне сети, все они используют в качестве источника данных сетевой трафик, который анализируется на наличие в нем признаков атак. Также возможен анализ журналов регистрации сетевого программно-аппаратного обеспечения (например, маршрутизатор, межсетевой экран или анализатор протоколов), фиксирующего весь обрабатываемый им трафик. В идеале эти средства должны работать в любых сетях, но, как показывает практика, средства обнаружения атак обнаруживают нарушения политики безопасности в сетях с разделяемой средой передачей данных (shared media), в которых одна линия связи используется попеременно несколькими компьютерами. То есть данные системы функционируют в технологиях Ethernet (и, следовательно, Fast Ethernet и Gigabit Ethernet), Token Ring, FDDI. Это связано с тем, что в таких сетях один компьютер может получить доступ ко всем пакетам, передаваемым в сегменте сети. Это существенно удешевляет системы обнаружения атак, так как практически независимо от числа узлов в сегменте сети, трафик между ними может контролироваться всего одной системой обнаружения атак. В случае индивидуальных линий связи между узлами (например, ATM) необходимо устанавливать систему обнаружения атак между каждой парой взаимодействующих узлов, что нецелесообразно по финансовым соображениям. Именно поэтому существующие реализации сетевых систем обнаружения атак поддерживают, в основном, сетевые технологии с разделяемой средой передачей данных. Кроме того системы обнаружения атак имеют еще одно ограничение. Они могут анализировать не любые стеки протоколов, а только самые распространенные. Из всех существующих на сегодняшний день систем обнаружения атак, примерно 95% работают со стеком TCP/IP и 5% - со стеком SMB/NetBIOS. Коммерческих систем, поддерживающих стек IPX/SPX, не говоря уже о других стеках, не известно.

*1. Достоинства систем обнаружения атак на уровне сети*

Системы обнаружения атак сетевого уровня имеют много достоинств, которые отсутствуют в системах обнаружения атак, функционирующих на конкретном узле. Многие покупатели используют систему обнаружения атак сетевого уровня из-за ее низкой стоимости эксплуатации и своевременного реагирования. Ниже представлены основные причины, которые делают систему обнаружение атак на сетевом уровне одним из наиболее важных компонентов эффективной реализации политики безопасности.

**2. Низкая стоимость эксплуатации**

Системы сетевого уровня не требуют, чтобы на каждом хосте устанавливалось программное обеспечение системы обнаружения атак. Поскольку для контроля всей сети число мест, в которых установлены IDS невелико, то стоимость их эксплуатации в сети предприятия ниже, чем стоимость эксплуатации систем обнаружения атак на системном уровне. Кроме того, для контроля сетевого сегмента, необходим только один сенсор, независимо от числа узлов в данном сегменте.

### 3. Обнаружение сетевых атак

Системы, функционирующие на уровне узла, как правило, не работают с сетевыми пакетами, и, следовательно, не могут определять эти типы атак. Исключением являются системы типа RealSecure Server Sensor или Centrax, которые содержат в себе сетевые компоненты, обнаруживающие и сетевые атаки, направленные на конкретный узел. Эти системы обнаружения атак могут исследовать содержание тела данных пакета, отыскивая команды, используемые в конкретных атаках. Например, когда хакер пытается найти серверную часть Back Orifice на системах, которые пока еще не поражены ею, то этот факт может быть обнаружен путем исследования именно содержания тела данных пакета. Как говорилось выше, системы системного уровня не работают на сетевом уровне, и поэтому не способны распознавать такие атаки.

### 4. Невозможность "заметания следов"

Сетевой пакет, будучи ушедшим с компьютера злоумышленника, уже не может быть возвращен назад. Системы, функционирующие на сетевом уровне, используют "живой" трафик при обнаружении атак в реальном масштабе времени. Таким образом, злоумышленник не может удалить следы своей несанкционированной деятельности. Анализируемые данные включают не только информацию о методе атаки, но и информацию, которая может помочь при идентификации злоумышленника и доказательстве в суде. Поскольку многие хакеры хорошо знакомы с механизмами системной регистрации, они знают, как манипулировать этими файлами для скрытия следов своей деятельности, снижая эффективность систем системного уровня, которым требуется эта информация для того, чтобы обнаружить атаку.

### 5. Обнаружение и реагирование в реальном масштабе времени

Данные системы обнаруживают подозрительные события и атаки по мере того, как они происходят, и поэтому обеспечивают гораздо более быстрое уведомление и реагирование,

чем системы, анализирующие журналы регистрации. Например, хакер, инициирующий сетевую атаку типа "отказ в обслуживании" на основе протокола TCP, может быть остановлен системой обнаружения атак сетевого уровня, посылающей TCP-пакет с установленным флагом Reset в заголовке для завершения соединения с атакующим узлом, прежде чем атака вызовет разрушения или повреждения атакуемого узла. Системы анализа журналов регистрации не распознают атаки до момента соответствующей записи в журнал и предпринимают ответные действия уже после того, как была сделана запись. К этому моменту наиболее важные системы или ресурсы уже могут быть скомпрометированы или нарушена работоспособность системы, запускающей систему обнаружения атак на уровне узла. Уведомление в реальном масштабе времени позволяет быстро среагировать в соответствии с предварительно определенными параметрами. Диапазон этих реакций изменяется от разрешения проникновения в режиме наблюдения для того, чтобы собрать информацию об атаке и атакующем, до немедленного завершения атаки.

### 6. Обнаружение неудавшихся атак или подозрительных намерений

Система обнаружения атак на уровне сети, установленная снаружи межсетевого экрана, может обнаруживать атаки, нацеленные на ресурсы, защищаемые МСЭ, даже, несмотря на то, что МСЭ, возможно, отразит эти попытки. Эта информация может быть очень важной при оценке и совершенствовании политики безопасности. Она поможет понять уровень возможностей и квалификацию злоумышленника.

### 7. Независимость от операционных систем, используемых в организации

Системы обнаружения атак, функционирующие на сетевом уровне, не зависят от операционных систем, установленных в корпоративной сети, так как они оперируют сетевым трафиком, которым обмениваются все узлы в корпоративной сети. Системе обнаружения атак все равно, какая ОС сгенерировала тот или иной пакет, если он в соответствие со стандартами, поддерживаемыми системой обнаружения. Например, в сети могут работать ОС Windows 98, Windows NT, Windows 2000, Netware, Linux, MacOS, Solaris и т.д., но если они общаются между собой по протоколу IP, то любая из систем обнаружения атак, поддерживающая этот протокол, сможет обнаруживать атаки, направленные на эти ОС.

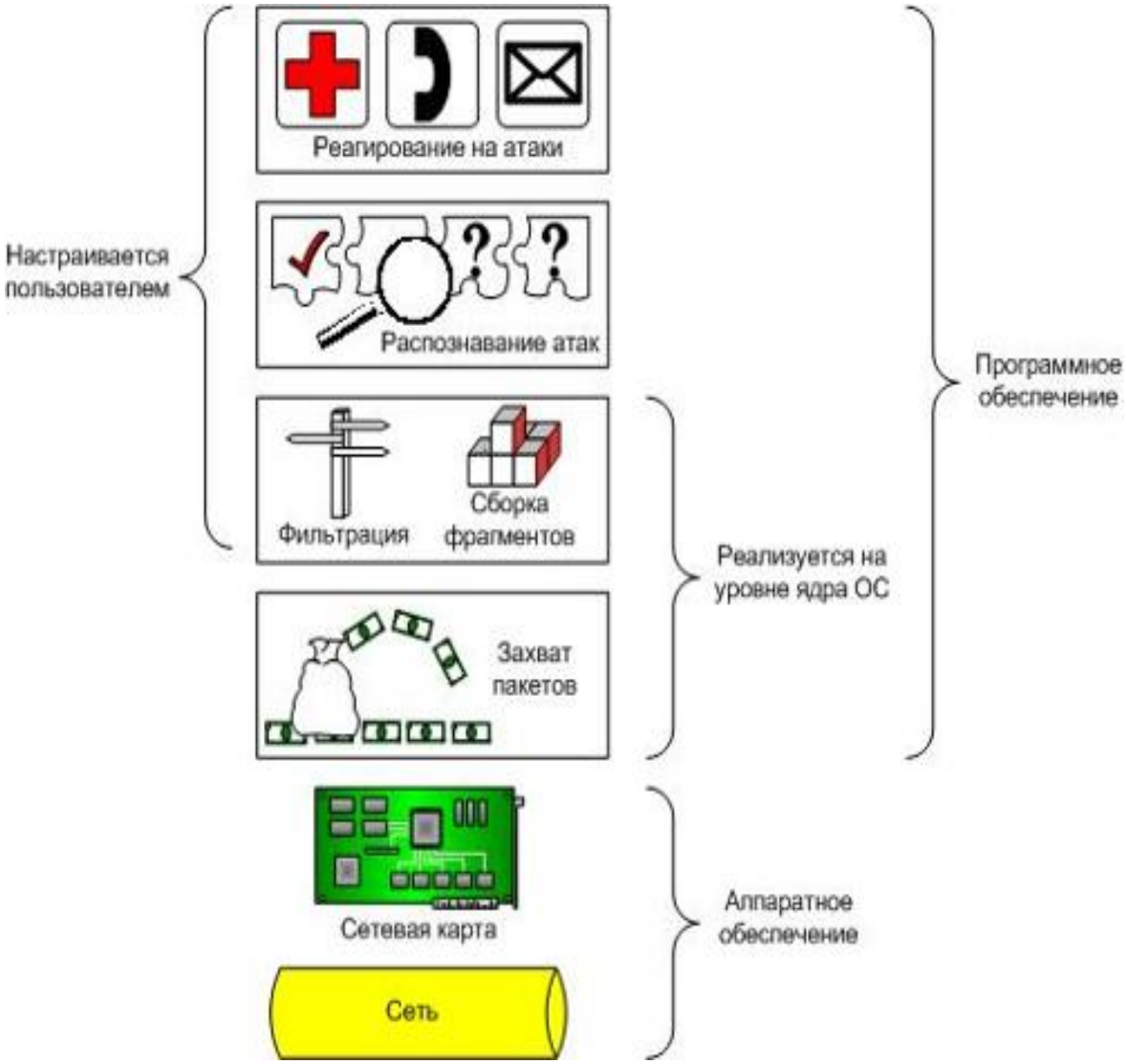



Рисунок 3.7 «Компоненты системы обнаружения атак на уровне сети»

### 3.7 Обманные системы

Обычно, когда речь заходит об обмане в области информационной безопасности, сразу вспоминаются попытки злоумышленников использовать те или иные скрытые лазейки для обхода используемых средств защиты. Будь то кража паролей и работа от имени авторизованного пользователя или несанкционированное использование модемов. Однако обман может сослужить хорошую службу не только для злоумышленников, но и для защитников корпоративных ресурсов. Сразу необходимо отметить, что обман очень редко используется в качестве защитного механизма. Обычно, когда речь заходит о средствах защиты, на ум сразу приходят современнейшие межсетевые экраны, блокирующие любые попытки проникновения хакеров. Или, если обратиться к фантастической литературе, то для защиты от проникновения используются системы с искусственным интеллектом, которые "адаптируются" к нападениям злоумышленников и противопоставляют им адекватные защитные меры. Такие системы описаны в "Лабиринте отражений" Сергея Лукьяненко или "Neuromancer" Уильяма Гибсона. Но "не межсетевым экраном единым". Приходится обращать свое внимание и на другие "нестандартные" защитные механизмы. Это частично собьет с толку злоумышленников и нарушителей, привыкших к широко известным средствам обеспечения информационной безопасности.

Существует множество различных вариантов использования обмана в благих целях. Вкратце перечислю некоторые механизмы обмана, основываясь на классификации Даннигана (Dunnigan) и Ноуфи (Nofi):

1. Сокрытие.
2. Камуфляж.
3. Дезинформация.

В той или иной мере эти механизмы используются в практике работ отделов безопасности. Однако, как правило, эти механизмы используются не для информационной, а для иных областей обеспечения безопасности (физическая, экономическая и т.д.).

В области информационной безопасности наибольшее распространение получил первый метод - сокрытие. Ярким примером использования этого метода в целях обеспечения информационной безопасности можно назвать сокрытие сетевой топологии при помощи межсетевого экрана. Примером камуфляжа можно назвать использование Unix-подобного графического интерфейса в системе, функционирующей под управлением операционной системы Windows NT. Если злоумышленник случайно увидел такой интерфейс, то он будет пытаться реализовать атаки, характерные для ОС Unix, а не для ОС Windows NT. Это существенно увеличит время, необходимое для "успешной" реализации атаки.

Во многих американских фильмах о хакерах, последние, атакуя военные системы Пентагона, мгновенно определяли тип программного обеспечения военной системы лишь взглянув на приглашение ввести имя и пароль. Как правило, каждая операционная система обладает присущим только ей способом идентификации пользователя, отличающимся от своих собратьев цветом и типом шрифта, которым выдается приглашение; текстом самого приглашения, местом его расположения и т.д. Камуфляж позволяет защититься именно от такого рода атак.

И, наконец, в качестве примера дезинформации можно назвать использование заголовков (banner), которые бы давали понять злоумышленнику, что атакуемая им система уязвима. Например, если в сети используется почтовая программа sendmail версии 8.9.3, а возвращаемый ею заголовок утверждает обратное, то нарушитель потратит много времени и ресурсов, чтобы попытаться эксплуатировать уязвимости, присущие ранним версиям sendmail (до 8.9.3).

Рассмотрим только 2 и 3 классы обманных методов, как менее известные и наиболее интересные. Работа систем их реализующих заключается в том, что эти системы эмулируют те или иные известные уязвимости, которых в реальности не существует. Использование средств (deception systems), реализующих камуфляж и дезинформацию, приводит к следующему:

1. Увеличение числа выполняемых нарушителем операций и действий. Так как заранее определить является ли обнаруженная нарушителем уязвимость истинной или нет, злоумышленнику приходится выполнять много дополнительных действий, чтобы выяснить это. И даже дополнительные действия не всегда помогают в этом. Например, попытка запустить программу подбора паролей (например, Crack для Unix или L0phtCrack для Windows) на сфальсифицированный и несуществующий в реальности файл, приведет к бесполезной трате времени без какого-либо видимого результата. Нападающий будет думать, что он не смог подобрать пароли, в то время как на самом деле программа "взлома" была просто обманута.

2. Получение возможности отследить нападающих. За тот период времени, когда нападающие пытаются проверить все обнаруженные уязвимости, в том числе и фиктивные, администраторы безопасности могут проследить весь путь до нарушителя или нарушителей и предпринять соответствующие меры, например, сообщить об атаке в соответствующие судебные инстанции.

Обычно в информационной системе используются от 5 до 10 зарезервированных портов (с номерами от 1 до 1024). К ним можно отнести порты, отвечающие за функционирование сервисов HTTP, FTP, SMTP, NNTP, NetBIOS, Echo, Telnet и т.д. Если обманные системы эмулируют использование еще 100 и более портов, то работа нападающего увеличивается во

стократ. Теперь злоумышленник обнаружит не 5-10, а 100 открытых портов. При этом мало обнаружить открытый порт, надо еще попытаться использовать уязвимости, связанные с этим портом. И даже если нападающий автоматизирует эту работу путем использования соответствующих программных средств (Nmap, SATAN и т.д.), то число выполняемых им операций все равно существенно увеличивается, что приводит к быстрому снижению производительности его работы. И при этом злоумышленник все время находится под дамокловым мечом, опасаясь своего обнаружения.

Есть и другая особенность использования обманных систем. По умолчанию обращение ко всем неиспользуемым портам игнорируется. Тем самым попытки сканирования портов могли быть пропущены используемыми защитными средствами. В случае же использования обманных систем все эти действия будут сразу же обнаружены при первой попытке обращения к ним.

С помощью обманных систем злоумышленников бьют их же оружием и чаша весов склоняется уже не в пользу атакующих, которые раньше почти всегда были на шаг впереди специалистов по защите. Применение обманных систем - это достаточно интересный и при правильном применении - эффективный метод обеспечения информационной безопасности. Однако для большей эффективности можно порекомендовать использовать связку защитных средств "обманные системы - системы обнаружения атак", которая позволит не только обнаружить нападающего сразу же после первой попытки атаки, но и заманить его при помощи обманной системы, тем самым, давая время администраторам безопасности на обнаружение злоумышленника и принятие соответствующих мер.

Существует два класса обманных систем. Первые эмулируют некоторые сервисы или уязвимости только на том компьютере, на котором они запущены. Примером такой системы является Decoy-режим RealSecure OS Sensor, WinDog-DTK или система The Deception Toolkit (DTK). Второй класс систем эмулирует не отдельные сервисы, а сразу целые компьютеры и даже сегменты, содержащие виртуальные узлы, функционирующие под управлением разных ОС. Примером такой системы является CyberCop Sting.

Но не стоит забывать, что обманные системы - это не панацея от всех бед. Они помогают в случае простых нападений, осуществляемых начинающими или неопытными злоумышленниками. В случае квалифицированных и опытных нарушителей обманные системы теряют свою эффективность. Предварительный анализ трафика позволяет злоумышленнику понять, какие из обнаруженных портов фиктивные. Моделирование атак на стенде и сравнивание результатов с тем, что выдается в реальной атакуемой системе, также позволяет обнаружить использование обманных средств. Мало того, неправильная конфигурация обманной системы приведет к тому, что злоумышленник сможет обнаружить факт слежки за ним и прекратит свою несанкционированную деятельность. Однако число

действительно квалифицированных злоумышленников не так велико и поэтому использование обманных средств может помочь в большинстве случаев.

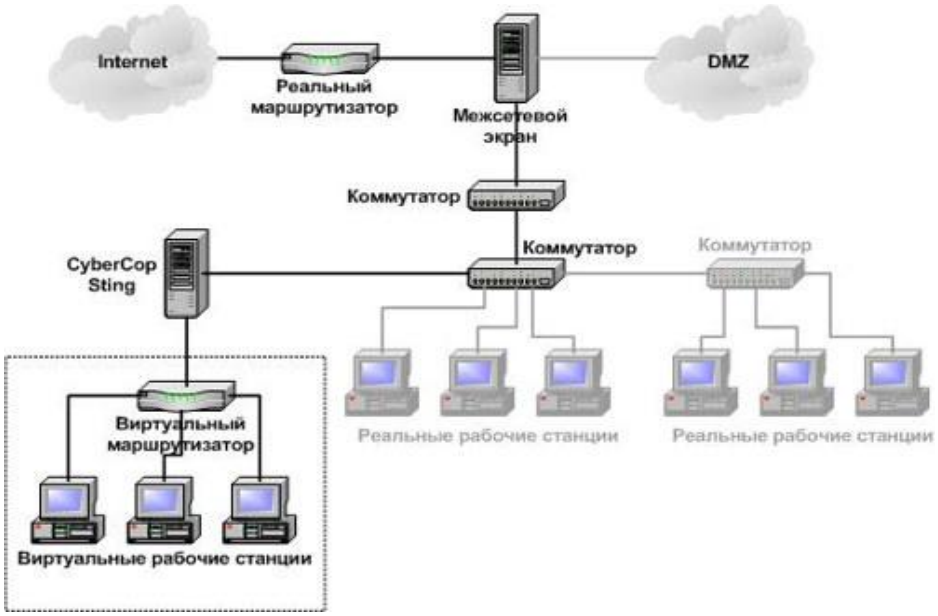



Рисунок 3.8 « Функционирование обманной системы CyberCop Sting»

### 3.8 Создание типовой архитектуры безопасности корпоративной сети

Экспоненциальное развитие информационных технологий в конце 20 века привело к тому, что на сегодняшний день практически все бизнес процессы любой компании основаны на использовании различных автоматизированных систем. Подобная тенденция к всеобщей автоматизации бизнес процессов обусловлена прежде всего конкурентной борьбой: чем ниже себестоимость продукции и, следовательно, - тем выше конкурентоспособность компании. Именно поэтому такое широкое применение в экономике нашли компьютерные сети (в т.ч. Internet) и созданные на их базе различные распределенные вычислительные системы, позволяющие существенно сократить время, необходимое для выполнения различных технологических операций. Анализ ситуации рынка информационных технологий показывает его дальнейший бурный рост в ближайшее десятилетие.

Однако наряду с безусловными позитивными моментами, связанными с всеобщей автоматизацией бизнес процессов, существуют и негативные стороны. К ним прежде всего необходимо отнести вновь возникающие проблемы, связанные с безопасностью обрабатываемой информации в автоматизированных системах компании. Всего существую три классических угрозы безопасности информации - это угрозы раскрытия, целостности и отказа в обслуживании.

Итак, Вы - IT-менеджер компании. Что произойдет, если информация, обрабатываемая в Вашей информационной системе, попадет к конкурентам (угроза раскрытия)? Что случится, если произойдет несанкционированное изменение критично важных для Вашей компании

документов (угроза целостности)? Что произойдет, если внезапно Ваша автоматизированная система будет остановлена (угроза отказа в обслуживании)?

Обратимся лишь к некоторым фактам - статистика нарушений информационной безопасности неумолима:

- 1999г. В США убытки компаний составили 266 млн. $
- 1996-1998 среднегодовые потери составляли 120 млн. $
- выход из строя на 22 часа сайта eBay.com принес компании убытки в размере 5 млн. $

Попробуйте оценить возможный ущерб, который принесет Вашей компании реализация на практике вышеприведенных угроз. Попробовали? Если нанесенный ущерб оказался несущественен, то это означает, что уровень автоматизации бизнес-процессов в Вашей компании на сегодняшний день не высок и вопросы обеспечения информационной безопасности вам предстоит решать только в будущем. Если же стоимость возможного ущерба составила внушительную цифру, то ответ для Вас очевиден - настал момент, когда пренебрежение вопросами безопасности информации может привести к серьезным убыткам для Вашей компании.

Рассмотрим теперь несколько стандартных заблуждений, которые по опыту авторов часто встречаются у IT-менеджеров компаний: "У нас в корпоративной сети защищать нечего!" и "Наша корпоративная сеть не имеет выхода в Интернет - значит нам ничего не угрожает". Поверьте нашему обширному опыту секьюрити-аналитиков с многолетним стажем, во внутренней сети практически любой компании можно с легкостью найти информацию, представляющую для компании большую ценность. Чем определяется ценность информации - убытками, которые понесет компания, если эта информация подвергнется воздействию одной или нескольких угроз, перечисленных в предыдущем абзаце. Простой пример - у каждой компании обычно имеются конкуренты. И у каждой компании обычно имеется база данных собственных клиентов, … которая несомненно может представлять очень большой интерес для конкурента.

Допустим ваша корпоративная сеть не имеет выходов в Интернет. Это что, означает что нам не нужно решать вопросы внутренней информационной безопасности? Вы 100% одинаково доверяете всем своим сотрудникам: от уборщицы до высшего руководства? Почему для 9 из 10 руководителей компаний является очевидным фактом стопроцентная необходимость физического обеспечения внутренней безопасности компании (комплекс физических и технических мер по охране помещений) и те же 9 из 10 руководителей не считают нужным заниматься внутренней безопасностью своих сетей. Почему? Потому что мы с вами, коллеги IT-менеджеры, плохо объясняем руководству, что наличие вооруженного охранника у серверной комнаты ни коим образом не спасет компанию от засланной

конкурентами "простой" уборщицы, которая, подключившись к любому компьютеру внутри вашей сети, может, несмотря на физическую охрану сервера, с легкостью осуществить к нему несанкционированный доступ.

Перейдем теперь от слов к делу и коснемся технической части вопроса. Прежде чем говорить об архитектуре безопасности корпоративной сети, рассмотрим кратко основные имеющиеся на сегодняшний день программно-аппаратные средства информационной защиты, которые могут быть использованы в предлагаемой ниже архитектуре.

| **Средства защиты персонального компьютера** | **Средства сетевой защиты** |
|---|---|
| 1. Антивирусная защита | 1. Межсетевые экраны |
| 2. Идентификация и аутентификация пользователей при входе в систему | 2. VPN-шифраторы |
| 3. Разграничение доступа между пользователями | 3. Средства анализа защищенности |
| 4. Криптографическая защита данных | 4. Средства обнаружения атак |
| 5. Персональный межсетевой экран и система обнаружения атак | 5. Средства антивирусной защиты трафика |
| | 6. Средство анализа содержимого трафика |

На следующем рисунке показана типовая архитектура безопасности корпоративной сети, подключенной к Интернет.

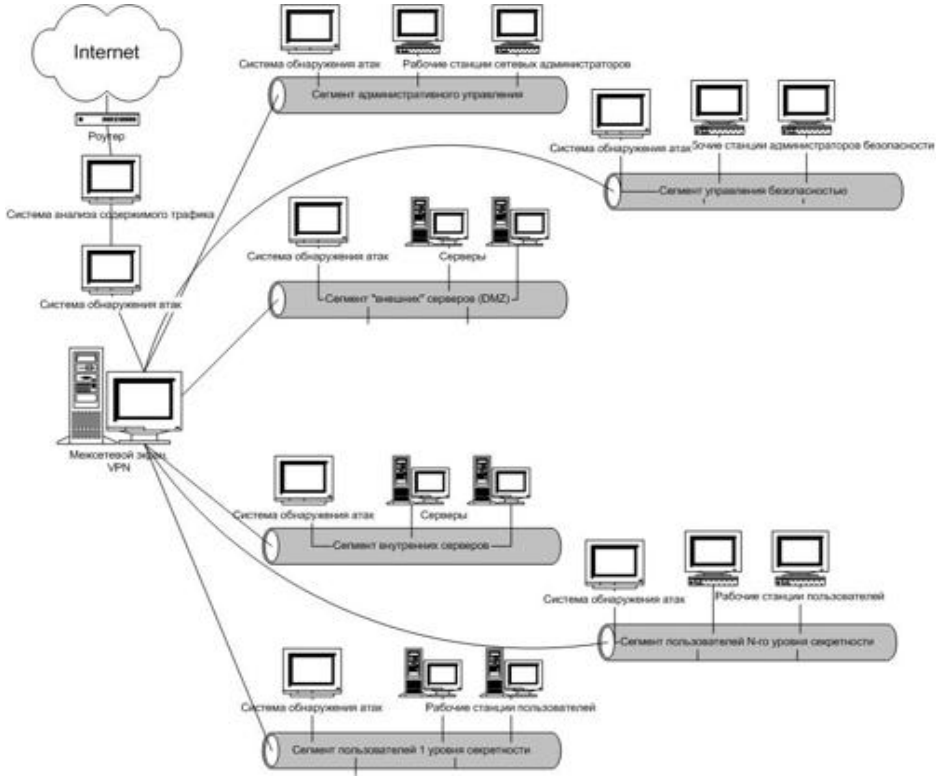



Рисунок 3.9 Типовая архитектура безопасности корпоративной сети, подключенной к Интернет.

Рисунок Типовая архитектура безопасности корпоративной сети, подключенной к Интернет

Рассмотрим основные принципы, которые были в нее заложены:

1. Введение N категорий секретности и создание соответственно N выделенных сетевых сегментов пользователей. При этом каждый пользователь внутри своего сетевого сегмента имеет одинаковый уровень секретности (допущен к информации одного уровня секретности). В этом случае мы всегда на своих семинарах проводим аналогию с секретным заводом, где все сотрудники в соответствии со своим уровнем доступа имеют доступ только к соответствующим этажам. Эта структура объясняется тем, что ни в коем случае нельзя смешивать потоки информации разных уровней секретности. Не менее очевидным объяснением такого разделения всех пользователей на N изолированных сегментов является легкость осуществления атаки внутри одного сегмента сети.

2. Выделение в отдельный сегмент всех внутренних серверов компании. Эта мера также позволяет изолировать потоки информации между пользователями, имеющих различные уровни доступа.

3. Выделение в отдельный сегмент всех серверов компании, к которым будет предоставлен доступ из Интернет (создание DMZ - демилитаризованной зоны для внешних ресурсов).

4. Создание выделенного сегмента административного управления.

5. Создание выделенного сегмента управления безопасности.

Многоуровневая политика безопасности (на всех уровнях модели OSI) для всех сегментов обеспечивается заданием соответствующих правил фильтрации на межсетевом экране. Все сегменты, за исключением сегмента DMZ, с применением технологии адресной трансляции (Network Address Translation - NAT) на межсетевом экране, имеют приватные IP-адреса.

Для обеспечения возможной защищенной связи с другим филиалом компании по открытым каналам Интернет межсетевой экран одновременно выполняет функции VPN-шлюза. Для пользователей высокого уровня секретности необходимо использование VPN-клиентов на каждом компьютере внутри данного пользовательского сегмента. Это позволит обеспечить криптозащищенную связь пользователя с внутренними серверами компании и сделает практически невозможными удаленные атаки между пользователями внутри одного сегмента: простой перехват трафика ничего не даст, подмена абонента соединения будет также не возможна из-за надежных криптографических методов защиты трафика и идентификации/аутентификации абонентов.

В каждом сетевом сегменте находится сетевой агент системы обнаружения удаленных атак, передающий всю информацию об обнаруженных атаках в сегменте на соответствующий сервер обнаружения атак, расположенный на рабочей станции администратора безопасности.

Также не будем забывать, что все рабочие станции и серверы защищены комплексами защиты от НСД и средствами антивирусной защиты.

В случае, когда необходимо предоставление доступа внешним пользователям к ресурсам компании (к DMZ) и требуется обеспечение повышенного уровня защиты необходимо использование двух межсетевых экранов.

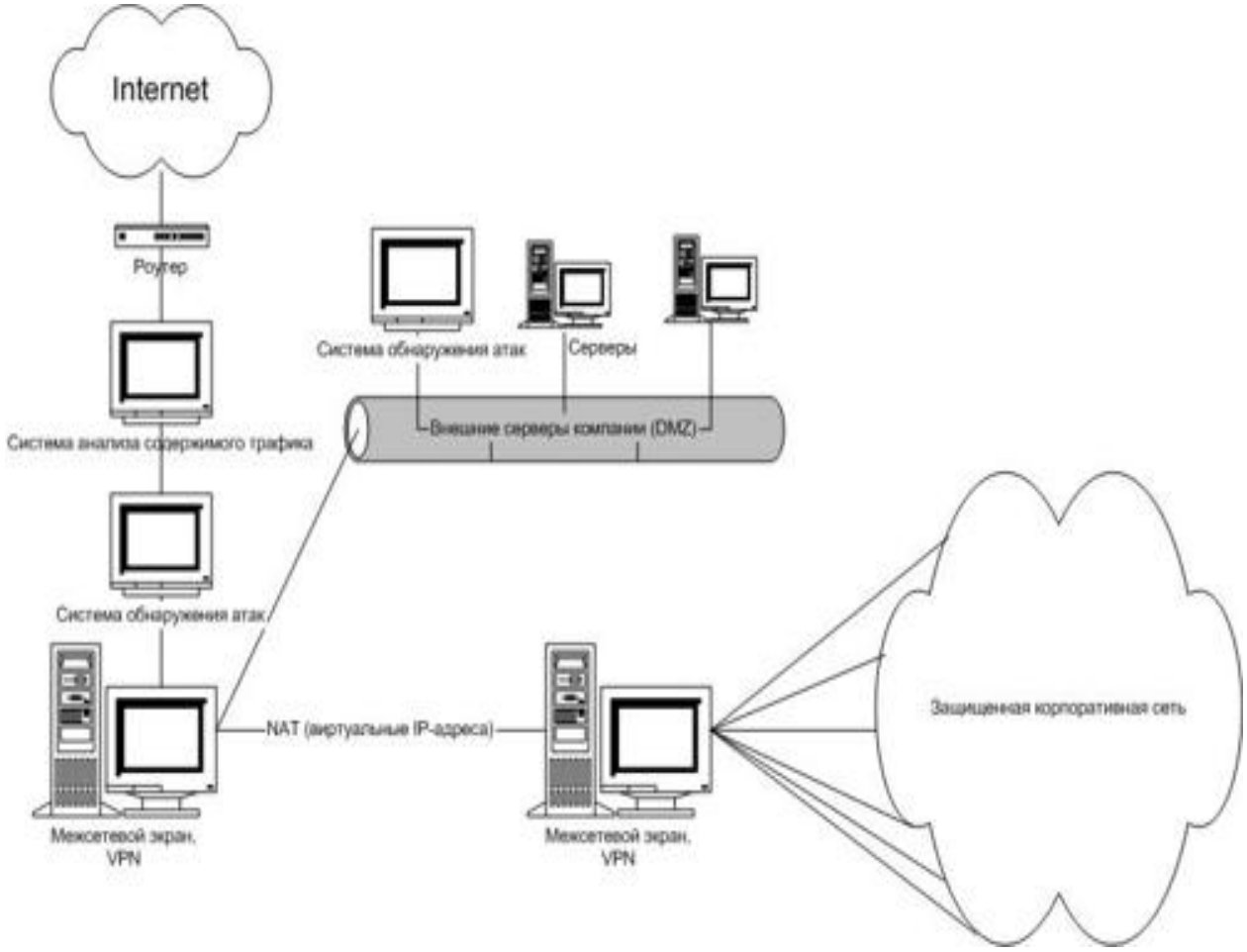



Рисунок 3.10 Обеспечение повышенного уровня сетевой защиты

Безусловно, полное воплощение на практике рассмотренной выше архитектуры сетевой безопасности потребует от компании вложения значительных средств. Поэтому для того, чтобы избежать избыточных расходов, прежде всего, необходимо провести комплексный анализ безопасности информационных ресурсов компании (аудит безопасности) причем желательно силами сторонних независимых аудиторов, которые укажут на слабые места в имеющейся системе обеспечения безопасности и предложат оптимальный комплекс мер по повышению текущего уровня защищенности сети. Почему надо приглашать кого-то, а не воспользоваться своими специалистами, спросите вы. Это еще одно стандартное заблуждение, что все проблемы можно решить своими силами. Во-первых, это очень сложная и комплексная задача и для ее решения нудно иметь как практический опыт решения подобных задач, так и владеть соответствующей методикой и технологией выполнения подобных работ. Поэтому вряд ли вам удастся найти собственного специалиста по безопасности, который имеет подобный опыт решения данных задач - слишком узкая и специфичная сфера деятельности. Кроме того, ни в коем случае нельзя поручать заниматься как обеспечением, так и тем более анализом безопасности тем же специалистам из отдела

ИТ, которые занимаются обычным администрированием системы. В случае обеспечения безопасности это очевидно даже из простых соображений элементарной безопасности: необходимо разделять функции администратора системы и администратора безопасности между разными людьми. Помните об аксиоме безопасности, о которой вы уже читали в этой книге": "Чем автоматизированная система более функциональна, тем она менее безопасна". Иными словами, что хорошо для администратора системы, то плохо для безопасника. Хорошо, скажете вы, пусть аудитом безопасности займется мой собственный специалист по безопасности (положим, он раньше был аудитором и у него есть соответствующий опыт). Вспомним, что в случае необходимости в проведении аудита системы, мы, применительно к аудиту, недаром сделали акцент на слове независимый. Вы хотите получить комплексную независимую оценку состояния безопасности вашей системы, которая не зависит от чьих либо интересов в компании? Вы хотите иметь гарантию, что никто в своих интересах не повлияет на вывод сотрудника вашей компании, который будет заниматься аудитом? Если да, если вам нужна реальная оценка уровня защищенности, то ответ для вас очевиден: необходимо воспользоваться услугами стороннего аудитора. Ведь согласитесь, что бессмысленно заниматься аудитом самих себя, не имея при этом в большинстве случаев еще и необходимого опыта. По нашему опыту, самая сложная задача для аудитора понять, как реализуется ядро бизнес процессов компании на уровне автоматизированной системы и оценить степень их рисков.

## ЗАКЛЮЧЕНИЕ

Защита информации представляет в настоящее время одно из ведущих направлений обеспечения безопасности государства, организации, отдельного человека. Проблемы различных аспектов безопасности все более занимают умы специалистов, так как на собственном опыте люди приходят к выводу, что нельзя обеспечить эффективную деятельность государства и организации, а также достойное «качество» жизни человека, отбиваясь от угроз, как от комаров в болотистом месте - усилий много, а толку мало.

Путь решения проблемы безопасности, как и других проблем, начинается с системного подхода к ней и ее системного анализа.

В практике системного анализа укоренилось мнение, что 50% успеха в решении сложной задачи - ее правильная постановка.

Чем более четко определены источники защищаемой информации, места и условия их нахождения, способы и средства добывания информации злоумышленником, тем конкретнее могут быть сформулированы задачи по защите и требования к соответствующим средствам.

Конкретность задач и требований - необходимое условие целенаправленного и рационального использования выделенных ресурсов.

Источники информации определяются в результате структурирования защищаемой информации, а места и условия их нахождения - на основе результатов моделирования объектов защиты.

Рост числа и видов угроз безопасности информации, сопровождающих повышение значимости информации в жизни общества и человека, представляют собой тенденцию, которую нельзя не учитывать.

Примером этого могут служить последствия широкого внедрения средств подвижной телефонной связи. Наряду с большими преимуществами для пользователей этого сравнительно нового для России вида связи по сравнению с традиционной проводной телефонной связью, возникла очень серьезная проблема по обеспечению конфиденциальности разговора. Если для несанкционированного подслушивания телефонного разговора в проводном канале злоумышленнику надо предпринять ряд довольно сложных и уголовно наказуемых по закону действий, то для подслушивания разговора по сотовой связи достаточно иметь небольшую сумму денег для покупки сканирующего приемника. С помощью такого приемника можно в комфортабельных условиях и безопасно прослушивать и записывать разговоры абонентов этой системы связи.

Поэтому изучение угроз, знание их потенциальных возможностей применительно к конкретным условиям, умение оценивать угрозы количественной мерой и, наконец, формулирование требований к способам и средствам защиты - необходимые и последовательно реализуемые процессы этапа постановки задач по защите информации. Игнорирование этих процессов может привести к несоответствию применяемых способов и средств защиты информации ее угрозам и, как следствие, - к большим затратам от хищения информации и неоправданными расходами на ее защиту.

Сложность выявления и анализа рассмотренных в книге угроз безопасности информации обусловлена многообразием способов и средств добывания информации, высокой динамичностью их изменения и многовариантностью действий злоумышленников. Вследствие этого необходимым условием для грамотной постановки задачи по защите информации является постоянное слежение специалистов за состоянием развития соответствующих областей науки и техники, а также моделирование угроз конкретной защищаемой информации. Чем точнее и полнее учтены в требованиях потенциальные угрозы, тем выше можно обеспечить эффективность защиты информации. Грубые ошибки при анализе угроз нельзя исправить на последующих этапах.

Не менее ответственные и сложные задачи возникают при непосредственном выборе рациональных способов и средств защиты, т. е. таких, которые обеспечивают требуемый

уровень защиты при минимальных затратах, не превышающих ущерб от хищения информации. В нахождении рациональных вариантов, удовлетворяющих этим условиям, состоит основная проблема этапа определения способов и средств зашиты информации. Несмотря на многообразие возможных способов инженерно-технической защиты, их методы можно свести к двум группам: информационному и энергетическому скрытию информации. Независимо от вида и носителя информации информационное скрытие сводится к маскировке и дезинформированию, а энергетическое - к уменьшению энергии носителя или повышению уровня помех на входе приемника злоумышленника. Такой общий подход к защите информации позволяет рассматривать с единых позиций все многообразие способов и реализующих их средств обеспечения безопасности информации и создает основу для преобразования набора эмпирических рекомендаций по инженерно-технической защите информации в соответствующую теорию.

Основными направлениями дальнейшего развития инженерно-технической защиты информации являются:

- в теоретическом плане - разработка теории инженерно-технической защиты информации как составляющей теории информационной безопасности;
- в методологическом плане - автоматизация процессов рационального решения задач защиты информации в рамках экспертной системы по защите информации;
- в практическом плане - комплексирование способов и средств защиты информации в единую систему защиту для конкретной организационной структуры.

Прогресс в области развития средств вычислительной техники, программного обеспечения и сетевых технологий дает сильный толчок к развитию средств обеспечения безопасности, что требует во многом предусмотреть научную парадигму информационной безопасности. Теория информационной безопасности – одна из самых развивающихся естественных наук.

Основными положениями информационной безопасности являются:

Исследование и анализ причин нарушения безопасности информационных систем.

Разработка эффективных моделей безопасности, адекватных современной степени развития программных и аппаратных средств, а также возможностям злоумышленников и разрушающим программным средствам.

Создание методов и средств корректного внедрения моделей безопасности в существующие АС, с возможностью гибкого управления безопасностью в зависимости от выдвигаемых требований, допускаемого риска и расхода ресурсов.

Необходимость разработки средств анализа безопасности информационных систем с помощью осуществления тестовых воздействий.

Особую роль в развитии теории информационной безопасности как науки так и отрасли промышленности играют центры компьютерной безопасности. К ним относятся государственные, общественные и коммерческие организации, а также неформальные объединения, основное направление деятельности которых – координация усилий, направленных на актуализацию проблем защиты информации, проведение теоретических исследований и разработка конкретных практических решений в области безопасности, аналитическая деятельность и прогнозирование.

В Российской Федерации такими центрами являются Государственная техническая комиссия при президенте Российской Федерации, Институт криптографии, связи и информатики Академии федеральной службы безопасности, Академия криптографии Российской Федерации.

## ЛИТЕРАТУРА

1. Щербаков А.Ю. Введение в теорию и практику компьютерной безопасности. – М.: издатель Молгачева С.В., 2001. - 352 с.

2. Девянин П.Н., Михальский О.О., Правиков Д.И., Щербаков А.Ю. Теоретические основы компьютерной безопасности. - М.: Радио и связь, 2000. – 192 с.

3. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2000. – 452 с.

4. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах. – М.: Горячая линия – Телеком, 2001. – 148 с.

5. Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации. - М.: Издательство Агенства "Яхтсмен", 1996.

6. Теория и практика обеспечения информационной безопасности. Под редакцией Зегжды П.Д. - М.: Издательство Агенства "Яхтсмен", 1996.

7. Баранов А.П., Зегжда Д.П., Ивашко А.М., Корт С.С. Теоретические основы информационной безопасности (дополнительные главы). Учебное пособие – ЦОП СпбГУ, Санкт-Петербург, 1998.

8. Department of Defence Trusted Computer System Evaluation Criteria (TCSEC), DOD, 1985.

9. Сборник руководящих документов по защите информации от несанкционированного доступа. - М.: Гостехкомиссия, 1998.

10. Основы информационной безопасности / Галатенко В.А. Под редакцией члена-корреспондента РАН В.Б. Бетелина / - М.: ИНТУИТ.РУ «Интернет-Университет Информационных Технологий», 2003. – 280 с.

11. Петренко С.А., Петренко А.А. Аудит безопасности Intranet. – М.: ДМК Пресс, 2002. – 416 с.

12. Завгородний В.И. Комплексная защита информации в компьютерных системах: Учебное пособие. – М.: Логос, 2001. – 264 с.