I. ИЗУЧЕНИЕ МЕЖДУНАРОДНОГО СТАНДАРТА БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ISO 17799

Содержание

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 создает один 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 использования), 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.

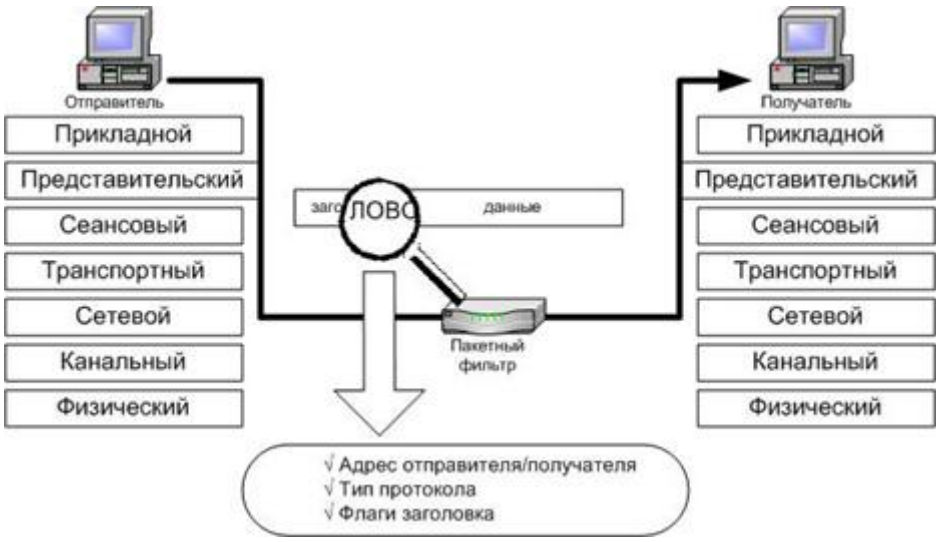

Рисунок 1.1 Пакетный фильтр

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.	

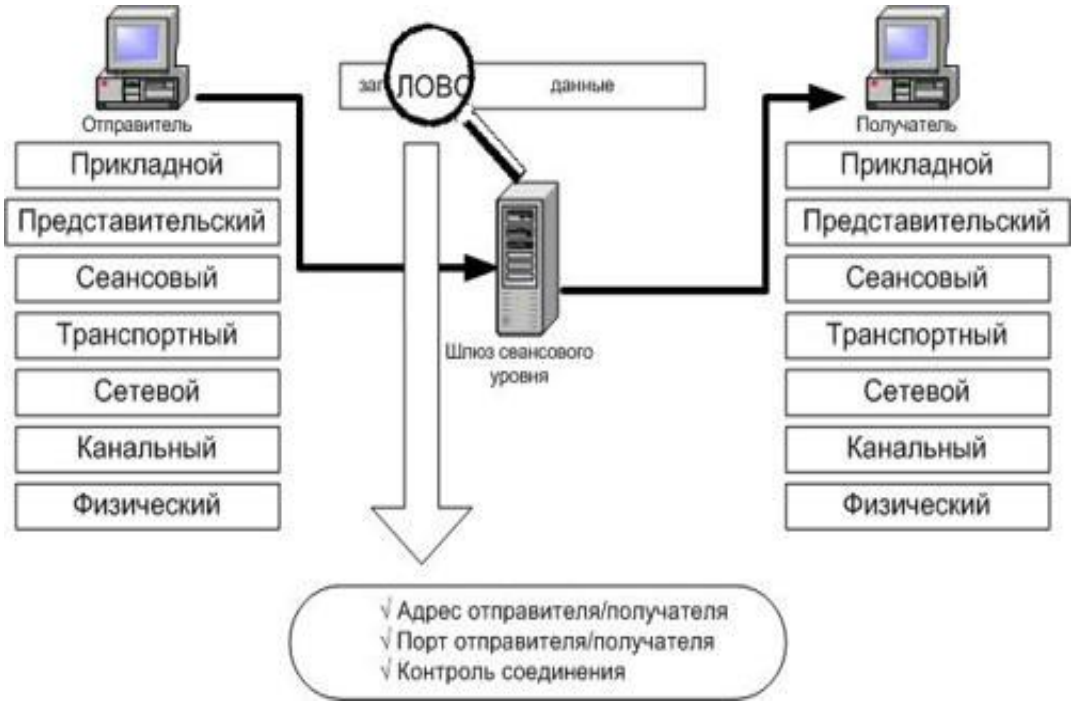

Рисунок 1.2 Шлюз сеансового уровня

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.

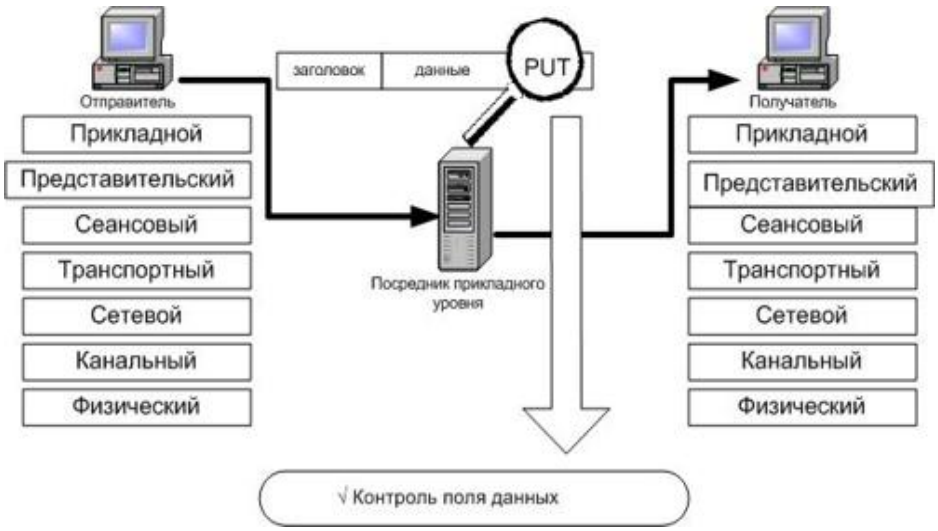

Рисунок 1.3 Посредник прикладного уровня

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.

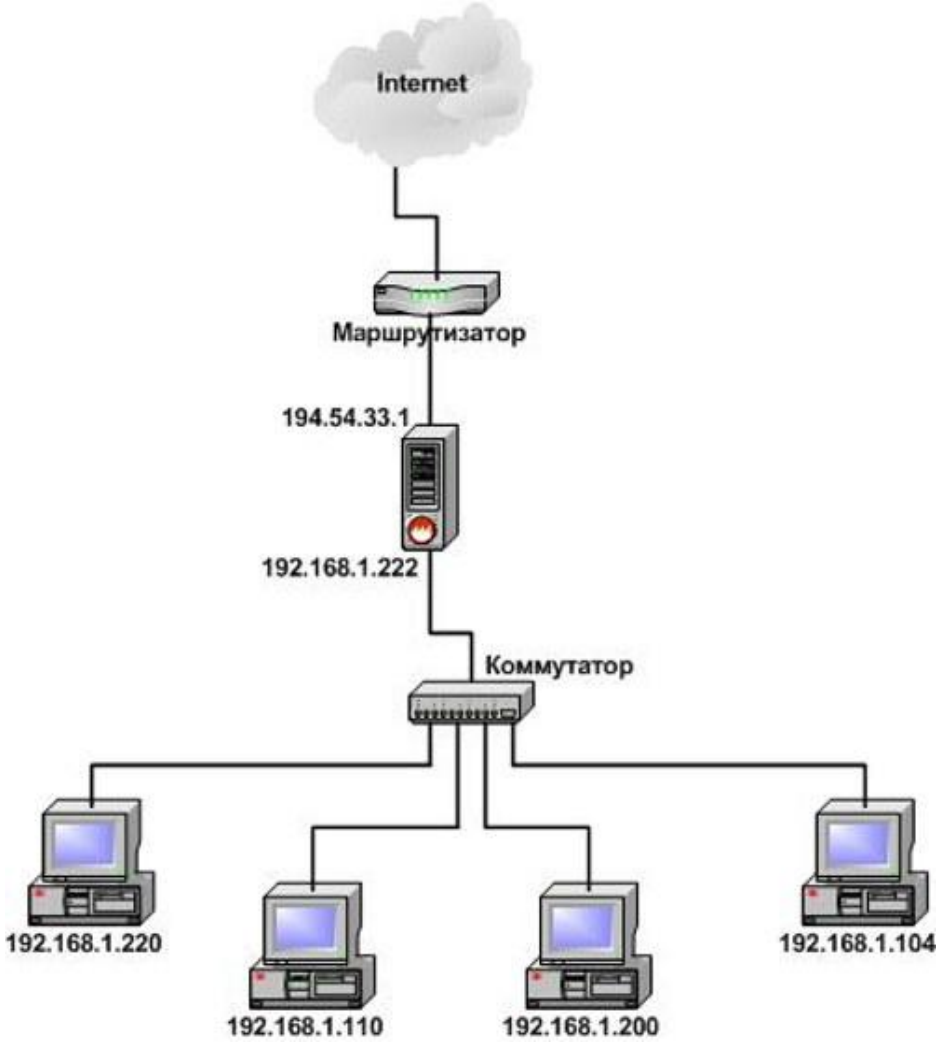

Рисунок 1.4 Трансляция сетевых адресов

✓ **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.

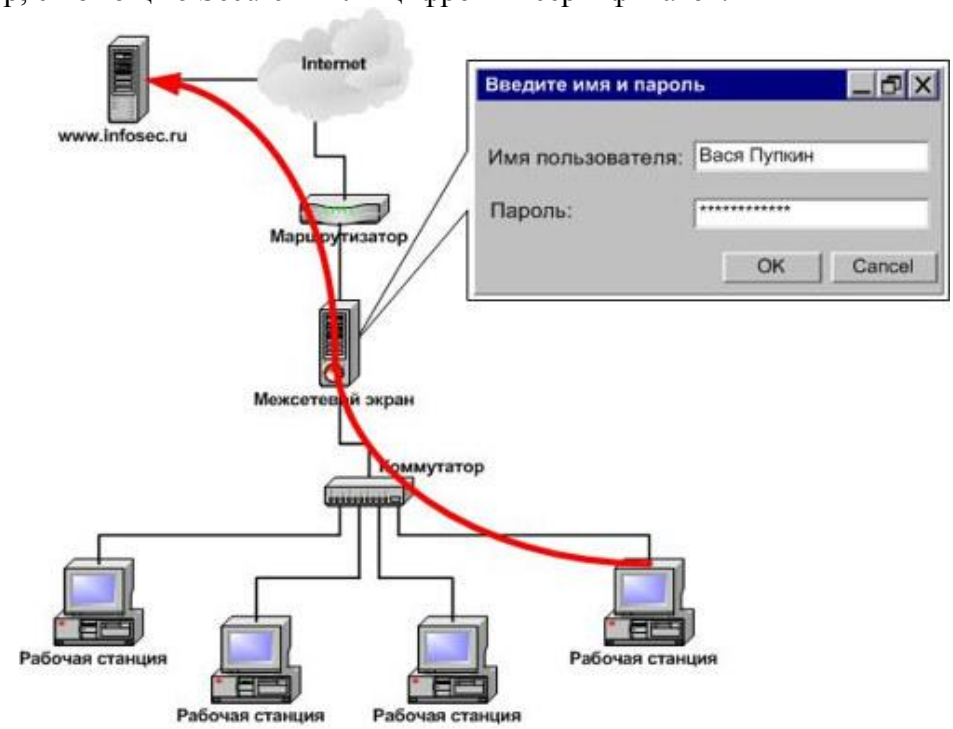

Рисунок 1.5 Аутентификация

✓ **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 2. Простота внедрения 3. Простота управления 4. Отказоустойчивость
Недостатки	1. Средняя производительность 2. Уязвимости ОС 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 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.	Поскольку современные реализации 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 контролировать доступ к информации в виде "кто получил доступ и к чему".	Уязвимости ОС могут подорвать 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	Расходы на стоимость эксплуатации и управление, связанные со средствами

важные, узлы.	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.

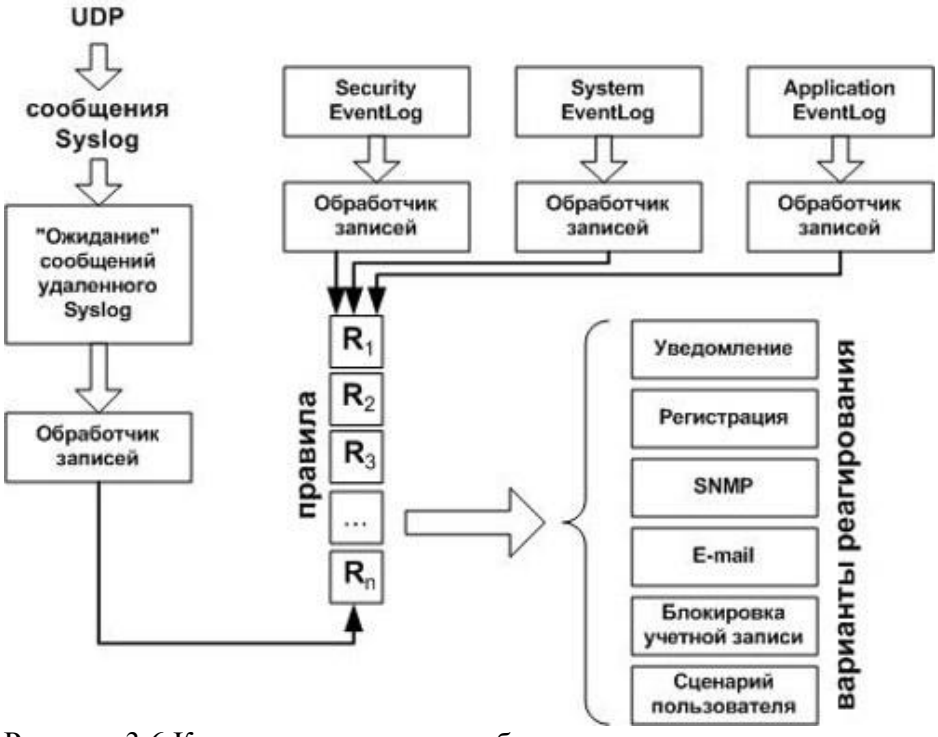

Рисунок 3.6 Компоненты системы обнаружения атак на уровне узла

✓ **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.

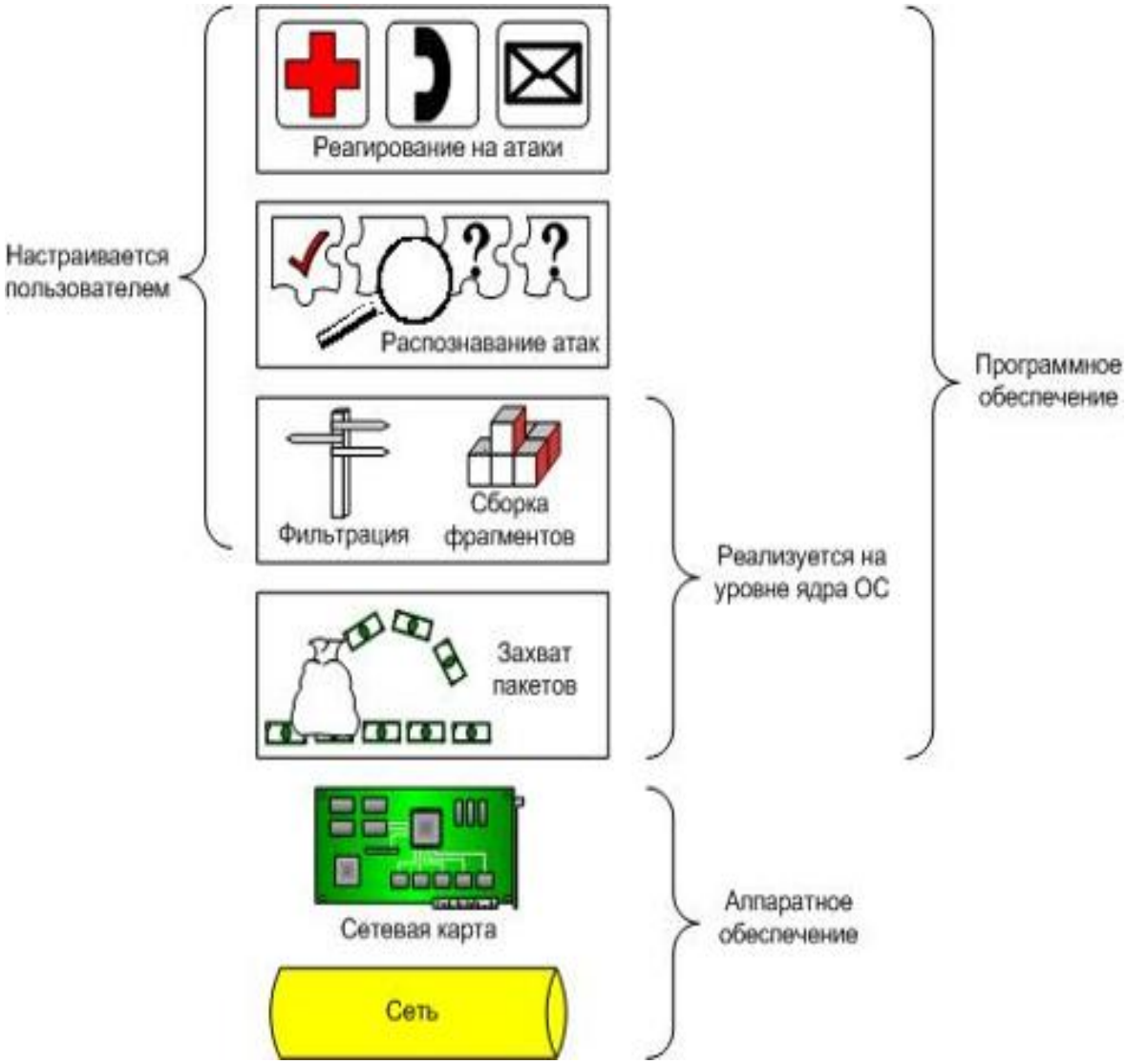

Рисунок 3.7 Компоненты системы обнаружения атак на уровне сети

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.

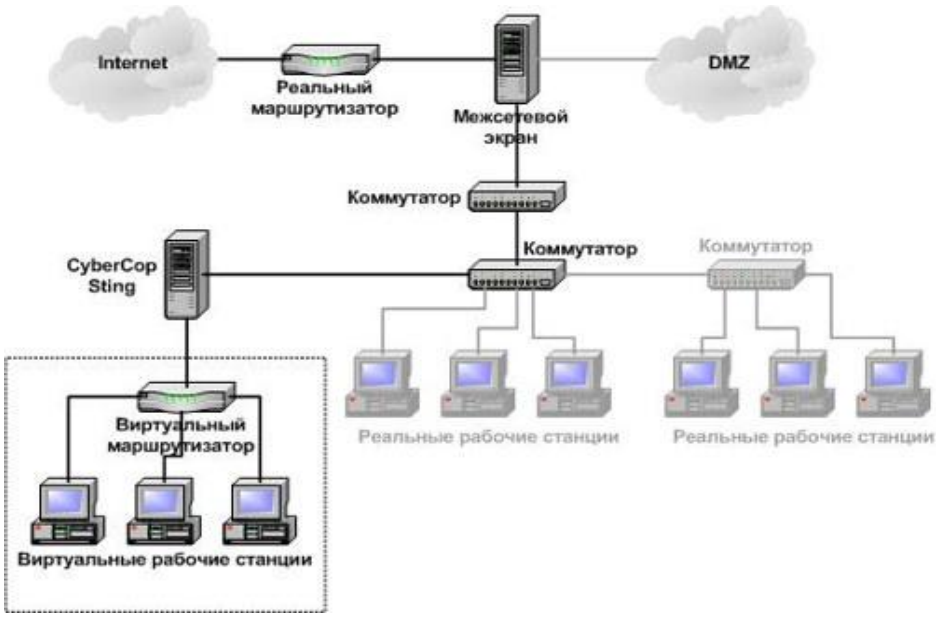

Рисунок 3.8 Функционирование обманной системы CyberCop Sting

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.

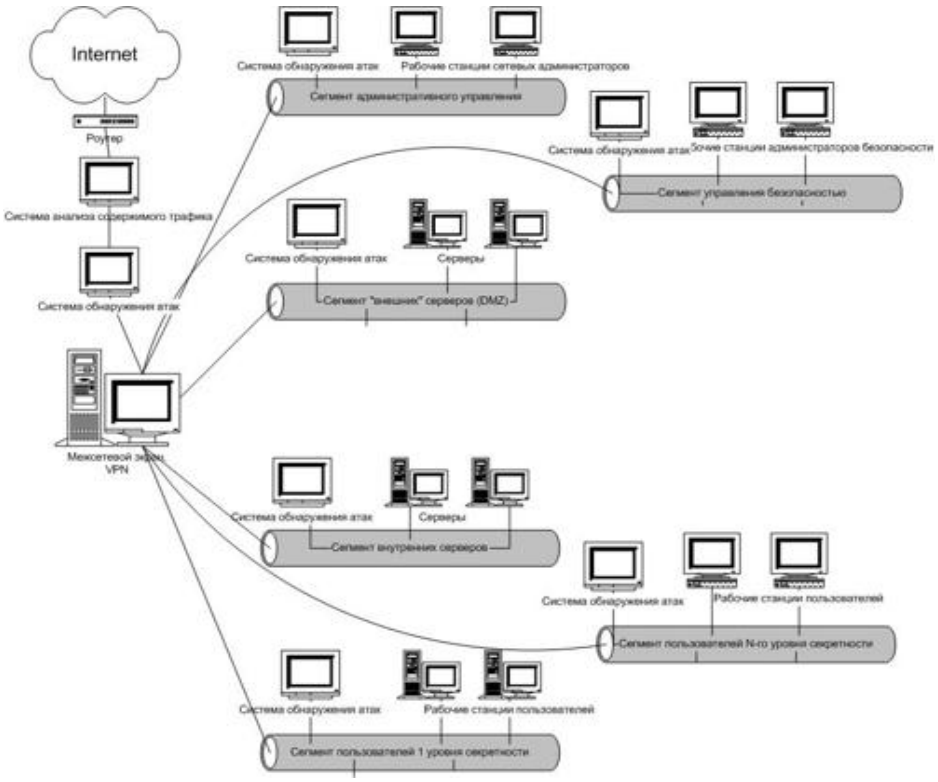

Рисунок 3.9 Типовая архитектура безопасности корпоративной сети, подключенной к Интернет.

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.

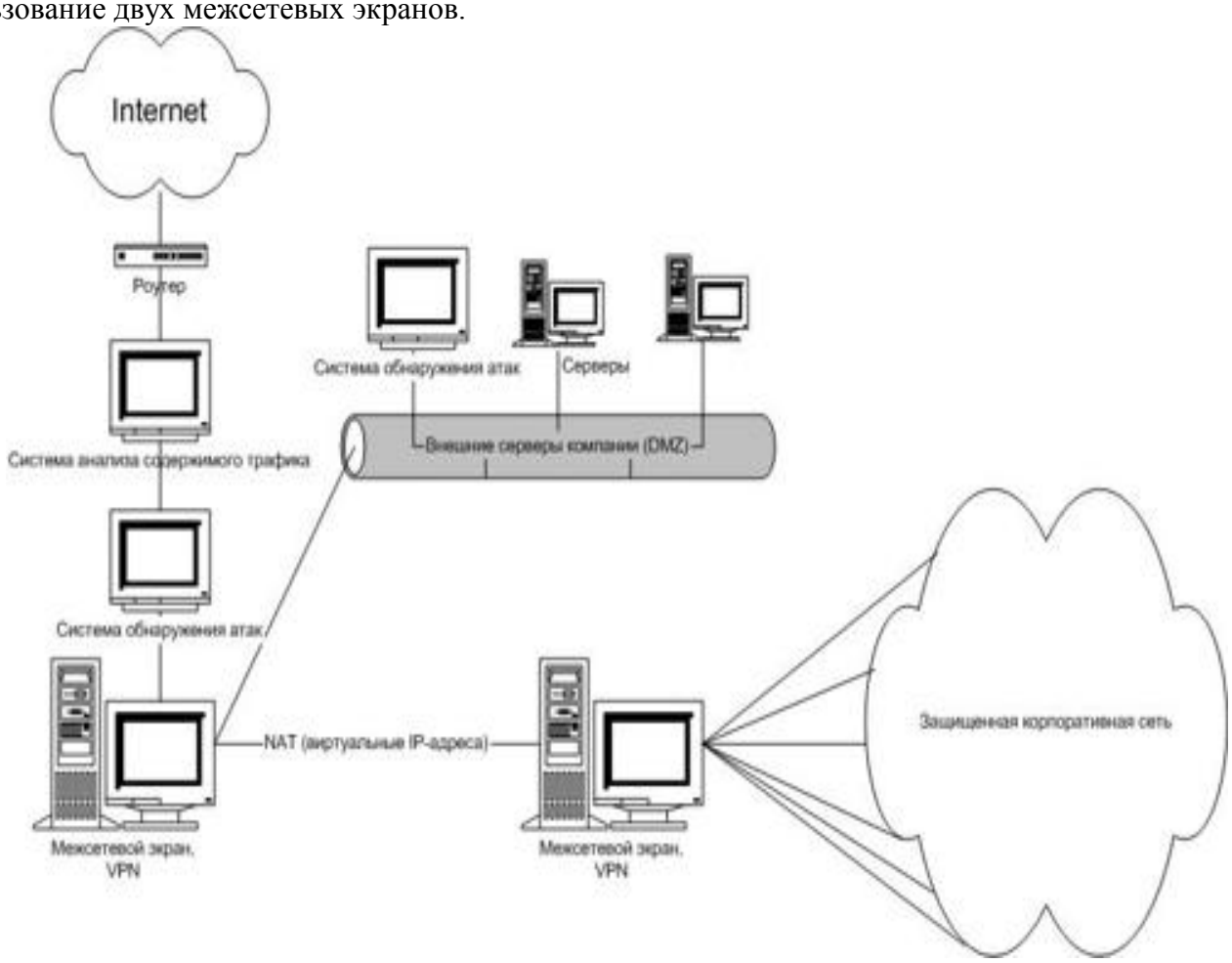

Рисунок 3.10 Обеспечение повышенного уровня сетевой защиты

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.

Контрольные задания и вопросы

1. Дайте определение ПБ. Что должен включать в себя документ определяющий ПБ?
2. Опишите организационные меры по обеспечению безопасности.
3. Опишите дайте определение понятию «Управление ресурсами».
4. Что включает в себя понятие «Безопасность персонала».
5. Что включает в себя понятие «Физическая безопасность».
6. Что включает в себя «Управление коммуникациями и процессами» для обеспечения безопасности информационных систем?
7. Что включает в себя политика контроля доступа и какие существуют правила контроля доступа?
8. Что включает в себя управление доступом пользователем и в чем заключается проверка прав пользователей?
9. Как производится контроль управления сетевого доступа, что такое ложная маршрутизация и что такое контроль над сетевыми соединениями?
10. Как производится контроль доступа в операционную систему? Опишите процедуру входа в систему (log on). Как производится использование системных утилит?
11. Как обеспечивается безопасность мобильных компьютеров и пользователей (удаленной работы)?
12. Как обеспечивается безопасность приложений? Что включает в себя политика использования криптографических средств?
13. Что включает в себя типовая политика информационной безопасности?
14. Дайте классификацию межсетевых экранов (МЭ).
15. Опишите работу пакетного фильтра.
16. Опишите работу шлюза сеансового уровня.
17. Опишите работу посредника прикладного уровня.
18. Опишите достоинства и недостатки аппаратной и программной реализации МЭ.
19. Как работают персональные МЭ?
20. Опишите работу систем контроля содержания.
21. Опишите работу систем целостности.
22. Дайте классификацию VPN.
23. Опишите варианты построения VPN.
24. Дайте классификацию систем обнаружения атак по этапам осуществления атаки.
25. Дайте классификацию систем обнаружения атак по принципу реализации атаки.
26. Опишите работу системы обнаружения атаки на уровне узла и ОС.