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

УТВЕРЖДАЮ

Заведующий кафедрой
«Управление инновациями»

_____ /*А.Ф.Уваров*
(подпись) *(ФИО)*
"_____" _____ 2012 г.

Вводятся в действие с «01» сентября 2012 г.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ К ПРАКТИЧЕСКИМ ЗАНЯТИЯМ

по дисциплине

«ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ»

Составлены кафедрой «Управление инновациями»

Для студентов, обучающихся
по направлению подготовки 222000.68 «Инноватика».
Магистерская программа «Управление инновациями в электронной технике»

Форма обучения очная

Составитель
к.ф-м.н., доцент каф. УИ Годенова Евгения Геннадьевна

"_18_" _июня_ 2012 г.

Томск, 2012

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Методические рекомендации содержат материалы, необходимые для выполнения практических работ по курсу «Защита информации в компьютерных системах», входящего в учебный план подготовки магистров по направлению 222000.68 «Инноватика».

Быстрые темпы развития информационных технологий и сети Интернет способствовали формированию особой информационной среды. Ни одна современная компания сегодня не может полноценно функционировать без корпоративной информационной системы. Корпоративные информационные системы (КИС) позволяют осуществить переход от традиционных форм бизнеса к электронному бизнесу. Электронный бизнес, который использует глобальную сеть Интернет и современные информационные технологии для повышения эффективности всех сторон деятельности компании, является одним из приоритетных направлений для создания и развития малых инновационных компаний.

Но, как известно, для полноценного существования электронного бизнеса необходимо обеспечение его информационной безопасности, под которой понимается защищенность корпоративной информации и поддерживающей инфраструктуры от случайных и преднамеренных воздействий, которые могут нанести вред владельцам или пользователям информации. Иногда, при самом неблагополучном исходе, такой вред может проявляться в виде полного прекращения деятельности компании.

Без знаний и квалифицированного применения современных информационных технологий, стандартов, протоколов и средств защиты информации невозможно обеспечить компании требуемый уровень информационной безопасности компьютерных систем и сетей. Для малых компаний, только начинающих свое развитие и набирающих обороты экономического роста, данная проблема является гораздо более актуальной и острой, чем для крупных фирм и корпораций.

Дисциплина «Защита информации в компьютерных системах» относится к вариативной части профессионального цикла (М2) согласно ФГОС. Данная дисциплина играет важную роль при обучении студентов по направлению магистерской подготовки 222000.68 «Инноватика» (профиль «Управление инновациями в электронной технике»).

1. ЦЕЛИ И ЗАДАЧИ ПРАКТИЧЕСКИХ РАБОТ

Цель изучения дисциплины заключается в формировании у студентов целостного представления о методах, средствах, способах и необходимости защиты информации, обрабатываемой в компьютерных системах.

Задачи курса:

- ✓ Ознакомить обучающихся с основными видами, классификациями, типами угроз безопасности информации, существующих в современных компьютерных системах;
- ✓ Продемонстрировать студентам важность своевременной защиты компьютерной информации;
- ✓ Ознакомить обучающихся с нормативно-правовым обеспечением в области защиты информации международного и отечественного уровней;
- ✓ Освоить существующие методики и способы защиты информации в компьютерных системах и сетях.

2. ТРЕБОВАНИЯ К УРОВНЮ ПОДГОТОВКИ СТУДЕНТОВ

Для успешного выполнения практических работ студентам необходимо

знать:

- ✓ лекционный материал;
- ✓ теоретическую часть методических рекомендаций к каждому практическому занятию;
- ✓ понятийный аппарат области информационных технологий и информационной безопасности;

уметь:

- ✓ составлять запросы для поиска информации в глобальной сети Internet;
- ✓ работать с текстами государственных стандартов, федеральных законов, регламентирующей документаций;
- ✓ работать со стандартными офисными пакетами

3. ФОРМЫ ОРГАНИЗАЦИИ ЗАНЯТИЙ ПО ДИСЦИПЛИНЕ

Занятия по дисциплине проходят в форме лекционных и практических занятий. Для углубленного изучения и освоения материала целесообразно организовывать также самостоятельную работу студентов. Контроль знаний осуществляется в виде проверки

письменных отчетов по результатам практических занятий, ответах на контрольные вопросы, тестированиях, опросах, проверке конспектов лекций.

Выполнение практических заданий позволит понять теоретические и практические вопросы существующих угроз безопасности информации, подбору и применению современных методов и способов защиты информации, понять логику построения систем защиты информации и научиться применять полученные знания для защиты информационных ресурсов как домашнего пользования (базовый уровень), так и более глобальных ресурсов (экономические, промышленные системы).

Для успешного выполнения и защиты практических занятий необходимо изучать теоретический материал к каждому практическому занятию. Данные материал не дублирует лекционные занятия и способствует получению студентами дополнительных знаний. Кроме того, ряд практических занятий построены таким образом, что студентам необходимо искать нужные сведения в сети Интернет. В процессе поиска они прочитывают много дополнительной информации, закрепляют навык фильтрации информации.

Практические занятия организуются как в форме индивидуальных работ, так и в интерактивных формах. Преимущественными интерактивными формами проведения практических занятия являются деловая игра и работа в малых группах, что обусловлено спецификой самой дисциплины.

Изучение дисциплины и выполнение практических занятий формирует знания, умения и навыки, необходимые специалистам в области защиты интеллектуальной собственности, специалистам в области внедрения инновационных разработок на рынок и продвижения наукоемких технологий.

Для проведения практических занятий необходим компьютерный класс с доступом в сеть Интернет. При посещении занятий студентам рекомендуется иметь тетрадь и USB флеш-карту.

4. ТЕМАТИКА ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Практическое занятие № 1

Тема «Изучение международных стандартов информационной безопасности»

Цели занятия: изучить существующие стандарты международного и отечественного уровня в области защиты информации.

Оборудование для проведения практического занятия: компьютер с проектором.

Форма организации занятия: представление доклада малой группой.

Ход занятия

Для практического занятия необходимо заранее подготовить устный доклад. Темы для доклада выдаются предварительно. Для подготовки каждой темы студентам необходимо сформировать малые группы, в рамках которых выполнить распределение работы по подготовке материала. Необходимо разобрать материал и представить его в виде логических блоков. Каждому из студентов дается 5-7 минут для доклада, в процессе которого он должен указать наиболее важные компоненты под запись остальным студентам.

В конце занятия студенты коллективно должны сформулировать основные выводы по прослушанному материалу, описать основные различия международных и российских стандартов в области информационной безопасности. Кроме того требуется ответить письменно на контрольные вопросы.

Темы для подготовки докладов

1. Стандарты ISO/IEC 15408. Критерии оценки безопасности информационных технологий;
2. Стандарты ISO/IEC 17799/27002 и 27001
3. Стандарт ГОСТ Р ИСО/МЭК 17799:2005 "Информационная технология. Практические правила управления информационной безопасностью"
4. Стандарт ГОСТ Р ИСО/МЭК 27001-2006 "Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования".
5. Нормативные документы РФ в области информационной безопасности.
6. Международные стандарты безопасности для сети Internet;
7. Международные стандарты безопасности для беспроводных сетей;

Контрольные вопросы

1. Что предполагает информационное обеспечение любой компании в целом?
2. Назвать 5-6 из 11 существующих функциональных требований стандарта ISO/IEC 15408.
3. Для чего служить профиль защиты согласно стандарту ISO/IEC 15408?
4. Какой из рассмотренных стандартов рассматривает вопросы информационной безопасности с точки зрения экономического эффекта?
5. Какой стандарт предусматривает защиту WLAN, используя целый комплекс мер безопасности передачи данных.
6. Какой из стандартов наиболее оптимален для построения политики безопасности малой инновационной компании (творческий ответ в форме эссе).

Практическое занятие № 2

Тема «Анализ внутренней сети»

Цели занятия: получить навык проведения анализа локальной сети для формирования политики безопасности предприятия.

Оборудование для проведения практического занятия: компьютер с операционной системой Windows, наличие системной утилиты 10-Strike LanState Pro, наличие доступа к ресурсам глобальной сети Internet.

Форма организации занятия: индивидуальное занятие на ЭВМ.

Теоретическая часть

Роль анализа рисков для создания корпоративной системы защиты информации в компьютерной сети предприятия можно наглядно показать на примере модели Lifecycle Security (название можно перевести как "жизненный цикл безопасности"), разработанной компанией Axent, впоследствии приобретенной Symantec[1].

Lifecycle Security - это обобщенная схема построения комплексной защиты компьютерной сети предприятия. Выполнение описываемого в ней набора процедур позволяет системно решать задачи, связанные с защитой информации, и дает возможность оценить эффект от затраченных средств и ресурсов. С этой точки зрения, идеология Lifecycle Security может быть противопоставлена тактике "точечных решений", заключающейся в том, что все усилия сосредотачиваются на внедрении отдельных частных решений (например, межсетевых экранов или систем аутентификации пользователей по смарт-картам). Без предварительного анализа и планирования, подобная тактика может привести к появлению в компьютерной системе набора разрозненных продуктов, которые не стыкуются друг с другом и не позволяют решить проблемы предприятия в сфере информационной безопасности.

Lifecycle Security включает в себя семь основных компонентов, которые можно рассматривать как этапы построения системы защиты (рис. 1.1).

[1] *Нестеров С.А. Анализ и управление рисками в операционных системах на базе операционных систем Microsoft. Лекция 3. «Методики построения систем защиты информации». – Интернет университет информационных технологий ИНТУИТ. - URL: http://www.intuit.ru/department/itmngt/riskanms/3/5.html (Режим доступа: требуется регистрация);*

Рис. 1.1. Компоненты модели Lifecycle Security

Примечание: **Assess risk** – оценка риска; **design security roadmap** - построение политики безопасности; **select & implement solutions** – принятие и исполнение решений; **conduct training** – проведение тренингов; **monitor security** – слежение за безопасностью, **implement incident responses & recovery –** фиксация воздействий и лечение.

Перечень выделяемых уровней незначительно различается в различных документах. Возможные варианты представлены на рис. 1.2[2].

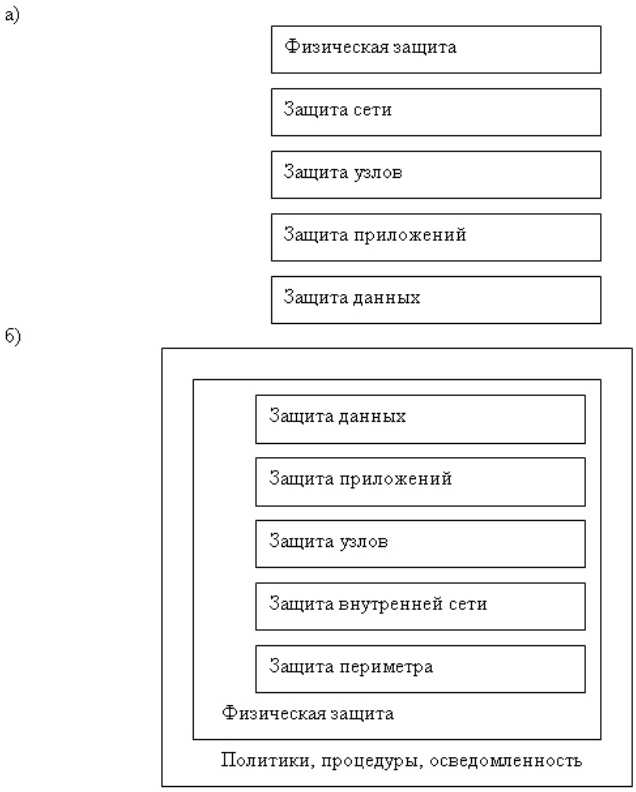


Рис. 1.2. Модель многоуровневой защиты

[2] Там же.

Политика безопасности должна описывать все аспекты работы системы с точки зрения обеспечения информационной безопасности. Поэтому **уровень политики безопасности** можно рассматривать как базовый. Этот уровень также подразумевает наличие документированных организационных мер защиты (процедур) и порядка информирования о происшествиях, обучение пользователей в области информационной безопасности и прочие меры аналогичного характера (например, рекомендуемые стандартом ISO/IEC 17799).

Уровень физической защиты включает меры по ограничению физического доступа к ресурсам системы - защита помещений, контроль доступа, видеонаблюдение и т.д. Сюда же относятся средства защиты мобильных устройств, используемых сотрудниками в служебных целях.

Уровень защиты периметра определяет меры безопасности в "точках входа" в защищаемую сеть из внешних, потенциально опасных. Классическим средством защиты периметра является межсетевой экран (англ. термин - firewall), который на основании заданных правил определяет, может ли проходящий сетевой пакет быть пропущен в защищаемую сеть. Другие примеры средств защиты периметра - системы обнаружения вторжений, средства антивирусной защиты для шлюзов безопасности и т.д.

Уровень защиты внутренней сети "отвечает" за обеспечение безопасности передаваемого внутри сети трафика и сетевой инфраструктуры. Примеры средств и механизмов защиты на этом уровне - создание виртуальных локальных сетей (VLAN) с помощью управляемых коммутаторов, защита передаваемых данных с помощью протокола IPSec и т.д. Нередко внутри сети также используют средства, характерные для защиты периметра, например, межсетевые экраны, в том числе и персональные (устанавливаемые на защищаемый компьютер). Связано это с тем, что использование беспроводных сетевых технологий и виртуальных частных сетей (VPN) приводит к "размыванию" периметра сети. Например, если атакующий смог подключиться к точке беспроводного доступа внутри защищаемой сети, его действия уже не будут контролироваться межсетевым экраном, установленным "на границе" сети, хотя формально атака будет производиться с внешнего по отношению к нашей сети компьютера. Поэтому иногда при анализе рассматривают **"уровень защиты сети"**, включающий и защиту периметра, и внутренней сети.

Следующим на схеме идет **уровень защиты узлов**. Здесь рассматриваются атаки на отдельный узел сети и, соответственно, меры защиты от них. Может учитываться функциональность узла и отдельно рассматриваться защита серверов и рабочих станций. В первую очередь, необходимо уделять внимание защите на уровне операционной

системы - настройкам, повышающим безопасность конфигурации (в том числе, отключению не использующихся или потенциально опасных служб), организации установки исправлений и обновлений, надежной аутентификации пользователей. Исключительно важную роль играет антивирусная защита.

Уровень защиты приложений отвечает за защиту от атак, направленных на конкретные приложения - почтовые серверы, web-серверы, серверы баз данных. В качестве примера можно назвать SQL-инъекции - атаки на сервер БД, заключающиеся в том, что во входную текстовую строку включаются операторы языка SQL, что может нарушить логику обработки данных и привести к получению нарушителем конфиденциальной информации. Сюда же можно отнести модификацию приложений компьютерными вирусами. Для защиты от подобных атак используются настройки безопасности самих приложений, установка обновлений, средства антивирусной защиты.

Уровень защиты данных определяет порядок защиты обрабатывающихся и хранящихся в системе данных от несанкционированного доступа и других угроз. В качестве примеров контрмер можно назвать разграничение доступа к данным средствами файловой системы, шифрование данных при хранении и передаче.

В процессе идентификации рисков определяется, что является целью нарушителя, и на каком уровне или уровнях защиты можно ему противостоять. Соответственно выбираются и контрмеры. Защита от угрозы на нескольких уровнях снижает вероятность ее реализации, а значит, и уровень риска. В продолжение темы инвентаризации активов информационной системы (ИС), является целесообразным рассмотреть средства, позволяющие получить данные о составе и топологии сети. ***Топология*** - это физическая конфигурация сети в совокупности с ее логическими характеристиками. Топология - это стандартный термин, который используется при описании основной компоновки сети. В качестве примера в данной лабораторной работе будет использоваться утилита 10-Strike LanState Pro. **10-Strike LANState** - программа для администраторов сетей Microsoft Windows. Полностью функционирует под ОС WINDOWS NT / 2000 / XP / Server 2003 / Vista / 7.

Основное предназначение: строит и отображает в наглядном представлении карту сети с условными обозначениями, связями и областями, с возможностью отслеживания в реальном времени состояния устройств (работает/не работает), состояния портов удаленных машин (открыт/закрыт), состояния различных служб, файлов и т.д. Включает в себя ряд полезных функций для получения информации об удаленных машинах:

- IP - адреса;

- MAC - адреса (номера сетевых адаптеров);
- Текущий пользователь;
- Принадлежность к домену, серверу;
- Установленная операционная система;
- Список дисков;
- Текущие дата и время;
- Доступные сетевые ресурсы;
- Текущие подключения;
- Системный реестр;
- Службы и устройства;
- Учетные записи;
- Группы пользователей;
- Открытые порты;
- Выполняемые процессы;
- Журналы событий;
- Полная информация о домене или рабочей группе;
- Список установленного ПО;
- SNMP-информация.

Позволяет:

- Моделировать в графическом виде локальную сеть, автоматически рисовать условные соединительные линии, области, помещения с названиями и телефонами, а затем сохранять полученный результат в виде карты, графического изображения и выводить на печать;
- Получать разнообразную информацию из сетевых устройств по SNMP-протоколу;
- Отслеживать использование ваших сетевых ресурсов пользователями сети с поддержкой "черного списка";
- Просматривать загруженность вашей сетевой карты (входящий/исходящий трафик);
- Управлять допусками к ресурсам вашего компьютера;
- Пинговать любой компьютер сети (ICMP и TCP);
- Выполнять трассировку маршрутов пакетов в сети;
- Получать имя компьютера по адресу хоста;
- Посылать обычные и анонимные сообщения любому компьютеру сети или группе пользователей;

- Выключать, включать и перезагружать компьютер сети (при соответствующих правах на удаленной машине);
- Осуществлять мониторинг различных сетевых сервисов на удаленных компьютерах, оповещать о событиях выполнением нескольких функций, в том числе отправкой SMS и E-MAIL, перезапуском служб и компьютера;
- Выполнять с устройствами действия через настраиваемое контекстное меню;
- Сканировать сеть по IP-адресам (максимально широкий диапазон);
- Осуществлять поиск устройств в сети и на карте;
- Создавать HTML-отчеты по составу системы удаленных компьютеров (информация о системе).
- Создавать HTML-отчеты по устройствам на карте с отображением их основных сетевых атрибутов (таблица соответствия DNS имен, IP и MAC-адресов);
- Ведение логов доступа к сетевым ресурсам, сигнализации, отправленных/принятых сообщений;
- Открывать и осуществлять навигацию по нескольким картам.

При запуске программы предлагается выбор - строить новую карту сети или открыть существующую. При запуске Мастера построения новой карты надо указать, какая подсеть документируется. При загрузке программы LanState Pro по умолчанию загружается стандартная картина «мнимой» топологии сети (рис. 1.3).

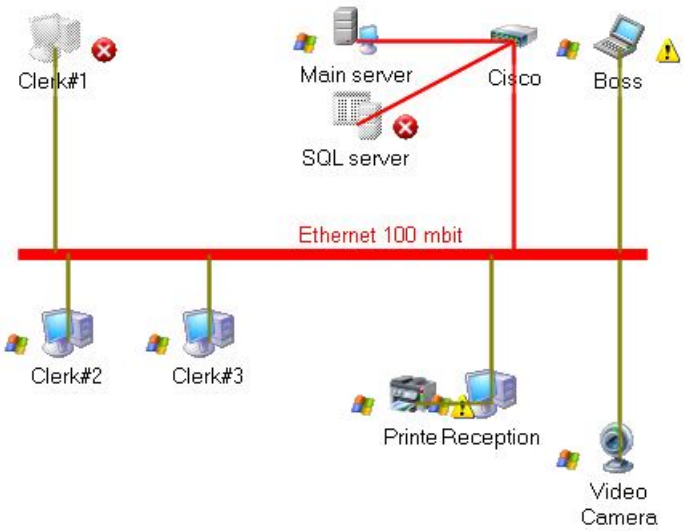


Рис. 1.3. Стандартный пример топологии сети

На рисунке 1.3 видно, что в сеть входят три рабочих компьютера с сетевыми именами Clerk1, Clerk2 и Clerk3. При этом на момент проверки компьютер с именем

Clerk3 был недоступен. Сеть содержит два сервера: главный (Main server) и сервер баз данных (SQL server). Также в сети имеется сетевой принтер с собственным IP-адресом, ноутбук с сетевым именем Boss с камерой. На рисунке также видно наличие коммутатора (свитча) Cisco. Мастер создания топологии сети позволяет строить сеть на основе диапазона IP-адресов или на основе Импорта из ближайшего окружения. При этом необходимо наличие этого окружения, иначе карта сети будет пустой. На рис. 1.4 показана карта сети, полученная путем импорта из ближайшего сетевого окружения внутренней сети СБИ. Как видно на рис. 1.4., помимо двух сетевых принтеров в сети имеется принтер, подключенный непосредственно к компьютеру, с которого производилась проверка сети - Xerox Phaser 3100 MFP.

Данная утилита позволяет получать широкий круг отчетов по состоянию сети. Для этого используется пункт меню Отчеты. Для того чтобы узнать имя компьютера по его IP-адресу нужно использовать пункт меню Сервис.

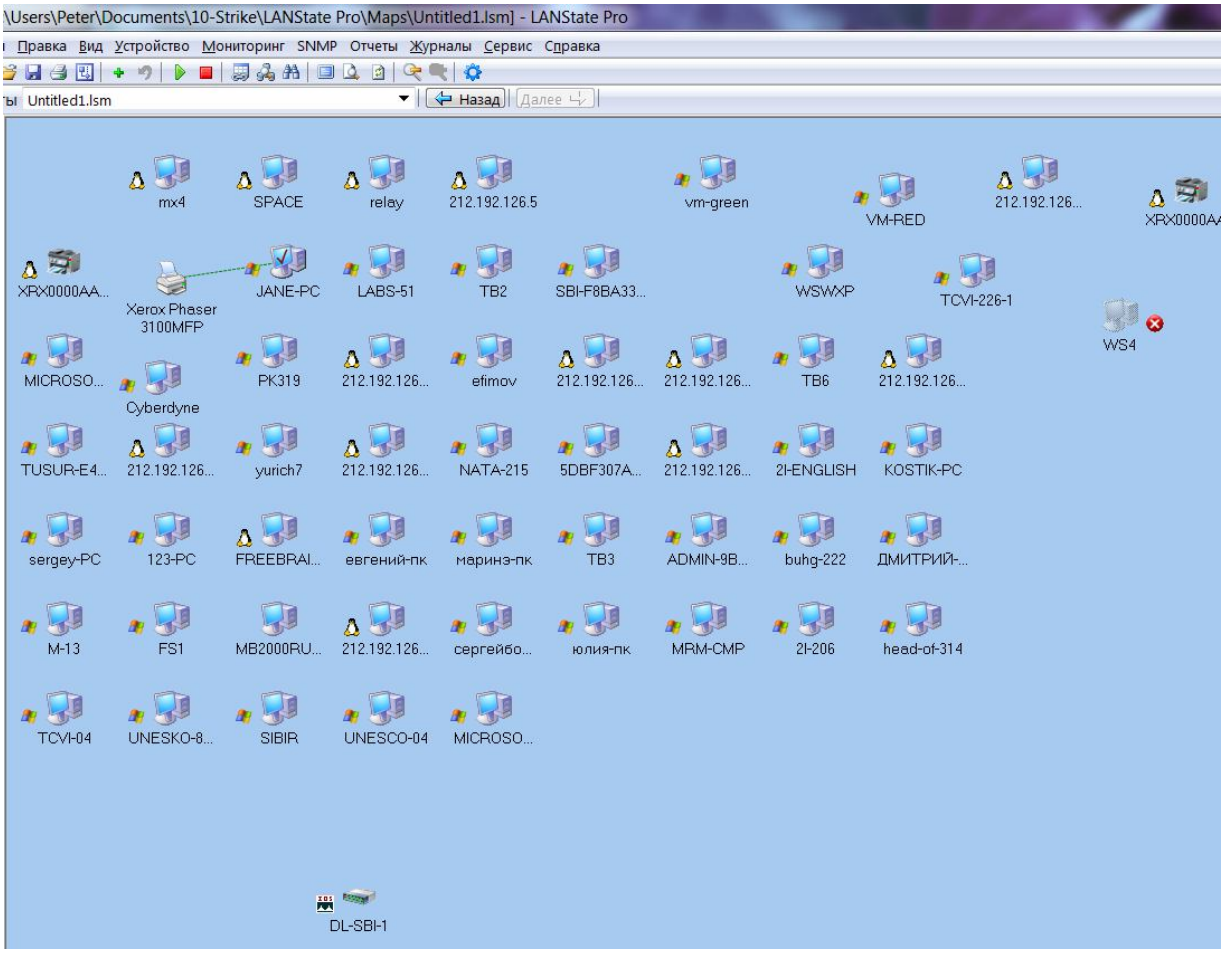
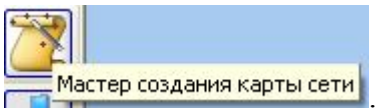


Рис. 1.4. Результат работы Мастера построения новой карты сети во внутренней сети СБИ

Задание к практической работе

1 Запустите утилиту 10-Strike LanState Pro и постройте карту сети учебной лаборатории при помощи меню Файл – Мастер новой карты сети или иконки 

.

2 Перечислите используемые сетевые устройства и укажите, какие последствия могут возникнуть при выходе из строя (или некорректной работе) каждого из них.

3 Укажите число компьютеров, входящих в сеть.

4 Укажите, какие операционные системы установлены на компьютерах сети.

5 Определите Общие ресурсы, используемые в данной сети;

6 Сколько принтеров используется в данной сети?

7 Создайте список устройств карты и сохраните полученный отчет;

8 Узнайте имя компьютера ваших соседей слева и справа;

9 Выберите любое устройство на карте сети и определите его сетевой трафик.

10 Используя возможность программы соединять линиями, компьютеры и создавать выделенные области  , создайте эффективную, по вашему мнению, карту сети, объединив компьютеры в группы по определенным функциям.

11 Создайте общий отчет в формате doc, где будут отображены отчеты из всех пунктов заданий с 1 по 8. В отчете приведите примеры, к какому из найденных устройств необходимо применять физический уровень защиты, уровень периметра, узлов, приложений и т.д.

Контрольные вопросы

1) В чем заключается смысл понятия Lifecycle Security?
2) К какому уровню защиты относится уровень политики безопасности?
3) Какие меры включает в себя уровень физической защиты?
4) Какие меры включает в себя уровень защиты периметра?
5) Какие меры выполняются на уровне защиты узлов?
6) Какие меры выполняются на уровне защиты внутренней сети?
7) Какие меры входят в уровень защиты данных?
8) Дайте определение топологии сети
9) Для чего необходимо строить карту сети?

Практическое занятие № 3

Тема «Методики оценки рисков и политика безопасности. Методика оценки рисков Microsoft»

Цели занятия: получить навык выявления рисков в системе безопасности предприятия, изучить существующие методики управления рисками, их достоинства и недостатки.

Оборудование для проведения практического занятия: компьютер с операционной системой Windows, программа Microsoft Security Assessment (MSAT).

Форма организации занятия: деловая игра, работа в малых группах.

Теоретическая часть

Существует несколько разновидностей методик для оценки рисков, которые в основном отличаются уровнем оценки. Выделяют три типа методик:

- ✓ методики, использующие оценку риска на качественном уровне (например, по шкале "высокий", "средний", "низкий"). К таким методикам, в частности, относится FRAP;
- ✓ количественные методики (риск оценивается через числовое значение, например размер ожидаемых годовых потерь). К этому классу относится методика RiskWatch;
- ✓ методики, использующие смешанные оценки (такой подход используется в CRAMM, методике Microsoft и т.д.)[3]

Методика CRAMM

Это одна из первых методик анализа рисков в сфере ИБ - работа над ней была начата в середине 80-х гг. центральным агентством по компьютерам и телекоммуникациям (ССТА) Великобритании. В основе метода CRAMM лежит комплексный подход к оценке рисков, сочетающий количественные и качественные методы анализа. Метод является универсальным и подходит как для крупных, так и для малых организаций, как правительственного, так и коммерческого сектора. Версии программного обеспечения CRAMM, ориентированные на разные типы организаций, отличаются друг от друга своими базами знаний (profiles). Для коммерческих организаций имеется Коммерческий профиль (Commercial Profile), для правительственных организаций - Правительственный профиль (Government profile). Правительственный вариант профиля, также позволяет проводить аудит на соответствие требованиям американского стандарта ITSEC ("Оранжевая книга").

[3] *Нестеров С.А. Анализ и управление рисками в информационных системах на базе операционных систем Microsoft. – Интернет-университет информационных технологий ИНТУИТ. - URL: http://www.intuit.ru/department/itmngt/riskanms/4/7.html. (Режим доступа: требуется регистрация)*

Методика FRAP

Методика "Facilitated Risk Analysis Process (FRAP)" предлагаемая компанией Peltier and Associates (сайт в Интернет http://www.peltierassociates.com/) разработана Томасом Пелтиером (Thomas R. Peltier) и опубликована в (фрагменты данной книги доступны на сайте, приведенное ниже описание построено на их основе). В методике, обеспечение ИБ ИС предлагается рассматривать в рамках процесса управления рисками. Управление рисками в сфере ИБ - процесс, позволяющий компаниям найти баланс между затратами средств и сил на средства защиты и получаемым эффектом. Управление рисками должно начинаться с оценки рисков: должным образом оформленные результаты оценки станут основой для принятия решений в области повышения безопасности системы. После завершения оценки, проводится анализ соотношения затрат и получаемого эффекта (англ. cost/benefit analysis), который позволяет определить те средства защиты, которые нужны, для снижения риска до приемлемого уровня.

Методика OCTAVE

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) - методика поведения оценки рисков в организации, разрабатываемая институтом Software Engineering Institute (SEI) при университете Карнеги Меллон (Carnegie Mellon University). Полное описание методики доступно в Интернет на сайте www.cert.org/octave.

Особенность данной методики заключается в том, что весь процесс анализа производится силами сотрудников организации, без привлечения внешних консультантов. Для этого создается смешанная группа, включающая как технических специалистов, так и руководителей разного уровня, что позволяет всесторонне оценить последствия для бизнеса возможных инцидентов в области безопасности и разработать контрмеры.

Методика Risk Watch

Компания RiskWatch разработала собственную методику анализа рисков и семейство программный средств, в которых она в той либо иной мере реализуется. В семейство RiskWatch входят программные продукты для проведения различных видов аудита безопасности:

- ✓ RiskWatch for Physical Security - для анализа физической защиты ИС;
- ✓ RiskWatch for Information Systems - для информационных рисков;
- ✓ HIPAA-WATCH for Healthcare Industry - для оценки соответствия требованиям стандарта HIPAA (US Healthcare Insurance Portability and Accountability Act), актуальных в основном для медицинских учреждений, работающих на территории США;

- ✓ RiskWatch RW17799 for ISO 17799 - для оценки соответствия ИС требованиям стандарта международного стандарта ISO 17799.

В методе RiskWatch в качестве критериев для оценки и управления рисками используются ожидаемые годовые потери (Annual Loss Expectancy, ALE) и оценка возврата инвестиций (Return on Investment, ROI). RiskWatch ориентирована на точную количественную оценку соотношения потерь от угроз безопасности и затрат на создание системы защиты. В основе продукта RiskWatch находится методика анализа рисков, которая состоит из четырех этапов.

Методика Microsoft

Проведение оценки рисков в соответствии с методикой Microsoft

Процесс управления рисками, предлагаемый корпорацией Майкрософт, разбивает этап оценки рисков на следующие три шага:

1. **Планирование**. Разработка основы для успешной оценки рисков.
2. **Координированный сбор данных**. Сбор информации о рисках в ходе координированных обсуждений рисков.
3. **Приоритизация рисков**. Ранжирование выявленных рисков на основе непротиворечивого и повторяемого процесса.

Для проведения оценки требуется собрать данные о:

- ✓ Активах организации.
- ✓ Угрозах безопасности.
- ✓ Уязвимостях.
- ✓ Текущей среде контроля (прим. в принятой авторами перевода руководства терминологии средства и меры защиты информации называются элементами контроля, соответственно, среда контроля - совокупность элементов).
- ✓ Предлагаемые элементы контроля.

Активами считается все, что представляет ценность для организации. К материальным активам относится физическая инфраструктура (например, центры обработки данных, серверы и имущество). К нематериальным активам относятся данные и другая ценная для организации информация, хранящаяся в цифровой форме (например, банковские транзакции, расчеты платежей, спецификации и планы разработки продуктов).

Процесс управления рисками безопасности, предлагаемый корпорацией Майкрософт, определяет следующие три качественных класса активов:

- ✓ **высокое влияние на бизнес** (ВВБ) - влияние на конфиденциальность, целостность и доступность этих активов может причинить организации значительный или

катастрофический ущерб. Например, к этому классу относятся конфиденциальные деловые данные.

- ✓ **среднее влияние на бизнес** (СВБ) - влияние на конфиденциальность, целостность и доступность этих активов может причинить организации средний ущерб. Средний ущерб не вызывает значительных или катастрофических изменений, однако нарушает нормальную работу организации до такой степени, что это требует проактивных элементов контроля для минимизации влияния в данном классе активов. К этому классу могут относиться внутренние коммерческие данные, такие как перечень сотрудников или данные о заказах предприятия.
- ✓ **низкое влияние на бизнес** (НВБ) - активы, не попадающие в классы ВВБ и СВБ, относятся к классу НВБ. К защите подобных активов не выдвигаются формальные требования, и она не требует дополнительного контроля, выходящего за рамки стандартных рекомендаций по защите инфраструктуры. Например, это могут быть общие сведения о структуре организации.

Далее определяется перечень угроз и уязвимостей и выполняется оценка уровня потенциального ущерба, называемого степенью подверженности актива воздействию. Оценка ущерба может проводиться по различным категориям:

- ✓ Конкурентное преимущество.
- ✓ Законы и регулятивные требования.
- ✓ Операционная доступность.
- ✓ Репутация на рынке.

Оценку предлагается проводить по следующей шкале:

- ✓ **Высокая подверженность воздействию**. Значительный или полный ущерб для актива.
- ✓ **Средняя подверженность воздействию**. Средний или ограниченный ущерб.
- ✓ **Низкая подверженность воздействию**. Незначительный ущерб или отсутствие такового.

Следующий шаг - оценка частоты возникновения угроз:

- ✓ **Высокая**. Вероятно возникновение одного или нескольких событий в пределах года.
- ✓ **Средняя**. Влияние может возникнуть в пределах двух-трех лет.
- ✓ **Низкая**. Возникновение влияния в пределах трех лет маловероятно.

Данные собираются в приведенный ниже шаблон (рис. 1.5).

Для угроз указывается уровень воздействия в соответствии с концепцией многоуровневой защиты (уровни - физический, сети, хоста, приложения, данных).

Шаблон сбора данных

Определите активы, за разработку, поддержку, управление и сопровождение которых несет ответственность ваша группа

Название актива	Классификация актива (высокое, среднее или низкое влияние на деятельность)
1.	

Для каждого актива укажите следующие значения

Многоуровневая защита	Чего необходимо избежать (угрозы)	Пути возникновения (уязвимости)	Уровень подверженности воздействию (В, С, Н)	Описания текущих элементов контроля	Вероятность (В, С, Н)	Назначение контроля, потенциальные новые
Физический уровень						
Приложения						
Узлы						
Сеть						
Данные						

Рис. 1.5 Снимок экрана шаблона

В столбце текущие элементы контроля описываются использующиеся средства и меры защиты, противостоящие данной угрозе. На основе собранных данных заполняется таблица, пример которой представлен на рис. 1.6.

Актив				Подверженность воздействию			
Дата обнаружения	Название актива	Класс актива	Применимые уровни многоуровневой защиты	Описание угрозы	Описание уязвимости	Уровень подверженности воздействию (В, С, Н)	Уровень влияния (В, С, Н)
Дата	Информация о финансовых инвестициях заказчиков	ВВБ	Узлы	Несанкционированный доступ к информации о заказчиках путем хищения учетных данных консультантов по финансовым вопросам	Хищение учетных данных с управляемых компьютеров локальной сети вследствие несвоевременного обновления баз данных антивирусных средств или конфигураций узлов либо несвоевременной установки обновлений системы безопасности	С	В
Дата	Информация о финансовых инвестициях заказчиков	ВВБ	Узлы	Несанкционированный доступ к информации о заказчиках путем хищения учетных данных консультантов по финансовым вопросам	Хищение учетных данных с управляемых удаленных компьютеров вследствие несвоевременного обновления баз данных антивирусных средств или конфигураций узлов либо несвоевременной установки обновлений системы безопасности	С	В
Дата	Информация о финансовых инвестициях заказчиков	ВВБ	Данные	Несанкционированный доступ к информации о заказчиках путем хищения учетных данных консультантов по финансовым вопросам	Хищение учетных данных доверенным сотрудником с помощью подслушивания, методов социальной инженерии и других методов без использования технических средств	Н	С

Рис. 1.6 Пример заполненного шаблона

Следующий шаг этапа оценки рисков - приоритизация рисков, т.е. создание упорядоченного по приоритетам списка рисков. Формирование данного списка сначала предлагается выполнить на обобщенном уровне, после чего описания наиболее существенных рисков детализируются.

Исходя из значения класса актива и оценки подверженности актива воздействию по таблице, приведенной на рис. 1.7. определяется уровень влияния.

Рис. 1.7. Определение уровня влияния по классу актива и уровню подверженности воздействию

Итоговый уровень риска определяется исходя из уровня влияния и оценки частоты возникновения риска, для которой используется шкала:

- ✓ **Высокая**. Вероятно возникновение одного или нескольких влияний в течение года;
- ✓ **Средняя**. Влияние может хотя бы один раз возникнуть в течение двух или трех лет;
- ✓ **Низкая**. Возникновение влияния в течение трех лет маловероятно.

Рис. 1.8. Определение итогового уровня риска

Полученные оценки заносятся в таблицу, пример которой приведен на рис. 1.9.

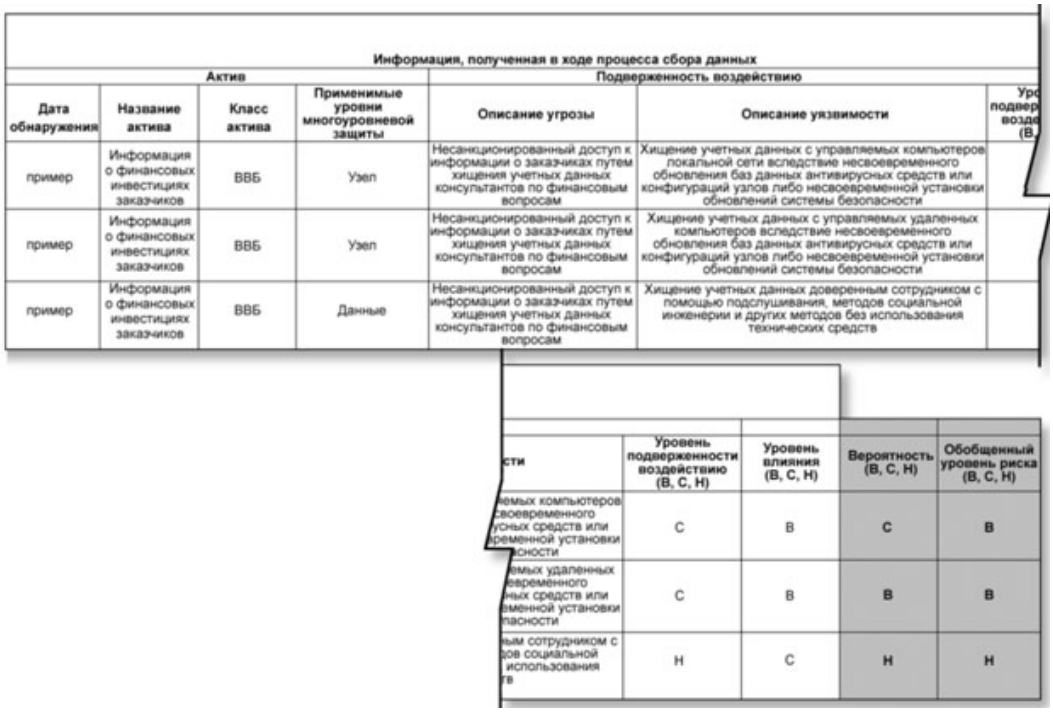
Для детального изучения (составления "перечня на уровне детализации") отбираются риски, отнесенные по результатам оценки на обобщенном уровне к одной из трех групп:

- риски высокого уровня;
- граничные риски: риски среднего уровня, которые необходимо снижать;
- противоречивые риски: риск является новым и знаний об этом риске у организации недостаточно или различные заинтересованные лица оценивают этот риск по-разному.

Формирование перечня рисков на уровне детализации является последней задачей процесса оценки рисков. В этом перечне каждому риску в итоге сопоставляется оценка в числовой (денежной) форме.

Вновь определяются:

- величина влияния и подверженности воздействию;
- текущие элементы контроля;
- вероятности влияния;
- уровень риска.



Информация, полученная в ходе процесса сбора данных						
Актив				Подверженность воздействию		
Дата обнаружения	Название актива	Класс актива	Применимые уровни многоуровневой защиты	Описание угрозы	Описание уязвимости	Уро подвер возде (В,
пример	Информация о финансовых инвестициях заказчиков	ВВБ	Узел	Несанкционированный доступ к информации о заказчиках путем хищения учетных данных консультантов по финансовым вопросам	Хищение учетных данных с управляемых компьютеров локальной сети вследствие несвоевременного обновления баз данных антивирусных средств или конфигураций узлов либо несвоевременной установки обновлений системы безопасности	
пример	Информация о финансовых инвестициях заказчиков	ВВБ	Узел	Несанкционированный доступ к информации о заказчиках путем хищения учетных данных консультантов по финансовым вопросам	Хищение учетных данных с управляемых удаленных компьютеров вследствие несвоевременного обновления баз данных антивирусных средств или конфигураций узлов либо несвоевременной установки обновлений системы безопасности	
пример	Информация о финансовых инвестициях заказчиков	ВВБ	Данные	Несанкционированный доступ к информации о заказчиках путем хищения учетных данных консультантов по финансовым вопросам	Хищение учетных данных доверенным сотрудником с помощью подслушивания, методов социальной инженерии и других методов без использования технических средств	

сти	Уровень подверженности воздействию (В, С, Н)	Уровень влияния (В, С, Н)	Вероятность (В, С, Н)	Обобщенный уровень риска (В, С, Н)
емых компьютеров своевременного русных средств или временной установки асности	С	В	С	В
емых удаленных своевременного ных средств или еменной установки пасности	С	В	В	В
ным сотрудником с ов социальной использования тв	Н	С	Н	Н

Рис. 1.9. Пример перечня рисков на обобщенном уровне

Уровень подверженности воздействию оценивается по пятибалльной шкале. Шкала для угрозы целостности и конфиденциальности приведена на рис. 1.10. Для угрозы отказа в обслуживании – на рис. 1.11. В качестве итогового уровня подверженности воздействию выберите максимальное значение.

Уровень подверженности воздействию	Конфиденциальность или целостность актива
5	Серьезные повреждения или полный выход актива из строя (например, видимые снаружи и влияющие на прибыльность или успешность ведения бизнеса)
4	Серьезные повреждения, не приводящие к полному выходу актива из строя (например, влияющие на прибыльность или успешность ведения бизнеса и, возможно, видимые снаружи)
3	Средние повреждения или ущерб (например, влияющие на внутренние рекомендации по ведению бизнеса и способные вызвать увеличение эксплуатационных затрат или уменьшение доходов)
2	Незначительные повреждения или ущерб (например, влияющие на внутренние рекомендации по ведению бизнеса, но не вызывающие существенного роста затрат)
1	Небольшие изменения в активе или отсутствие изменений

Рис. 1.10. Уровни подверженности воздействию для угроз конфиденциальности и целостности

Уровень подверженности воздействию	Дата выпуска	Описание
5	Прекращение работы	Большие эксплуатационные затраты или нарушение коммерческих обязательств
4	Прерывание работы	Значительное увеличение эксплуатационных затрат или задержка при выполнении коммерческих обязательств
3	Задержки в работе	Заметное влияние на величину эксплуатационных затрат и производительность.
2	Отвлечение от работы	Измеримое влияние на деятельность компании отсутствует; небольшое увеличение эксплуатационных затрат или затрат на инфраструктуру
1	Не влияет на обычный ход бизнес-операций	Измеримое влияние на эксплуатационные затраты, производительность и коммерческие обязательства отсутствует

Рис. 1.11. Уровни подверженности воздействию для доступности

После определения уровня подверженности воздействию производится оценка величины влияния. Каждому уровню подверженности воздействию сопоставляется значение в процентах, отражающее величину ущерба, причиненного активу, и называемое фактором подверженности воздействию. Майкрософт, рекомендует использовать линейную шкалу подверженности воздействию от 100 до 20%, которая может изменяться в соответствии с требованиями организации. Кроме того, каждой величине влияния сопоставляется качественная оценка: высокая, средняя или низкая. На рис. 1.12 показаны возможные значения для каждого класса влияния.

Класс влияния	Значение класса влияния (З)
ВВБ	10
СВБ	5
НВБ	2

Уровень подверженности воздействию	Фактор подверженности воздействию (ФПВ)	Уровень влияния (З * ФПВ)	Диапазон влияния	Обобщенное сравнение
5	100%		7 - 10	Выс.
4	80%		4 - 6	Средн.
3	60%		0 - 3	Низк.
2	40%			
1	20%			

Рис. 1.12. Определение величин влияния

Далее описываются "элементы контроля", используемые в организации для снижения вероятностей угроз и уязвимостей, определенных в формулировке влияния.

Следующая задача - определение вероятности влияния. Результирующий уровень вероятности определяется на основании двух значений. Первое значение определяет вероятность существования уязвимости в текущей среде. Второе значение определяет вероятность существования уязвимости исходя из эффективности текущих элементов контроля. Каждое значение изменяется в диапазоне от 1 до 5. Определение оценки проводится на основе ответов на вопросы, перечень которых представлен на рис. 1.13, с последующим переходом к результирующей оценке (рис. 1.14). При этом разработчики

руководства указывают, что оценка вероятности взлома имеет субъективный характер и предлагают при проведении оценки уточнять приведенный перечень.

Определения вероятностей для уязвимостей
Высокая
Большое число злоумышленников — любители и компьютерные хулиганы
Удаленное выполнение
Возможность использования анонимного доступа
Общеизвестный метод взлома
Автоматизированность
5, если выполняется хотя бы одно из условий
Средняя
Среднее число злоумышленников — специалисты и эксперты
Невозможность удаленного выполнения
Необходимость наличия привилегий уровня пользователя
Метод взлома не является общеизвестным
Атака не автоматизирована
3, если выполняется хотя бы одно из условий
Низкая
Небольшое число злоумышленников — необходима внутренняя информация
Невозможность удаленного выполнения
Необходимость наличия привилегий уровня администратора
Метод взлома не является общеизвестным
Атака не автоматизирована
1, если выполняются все условия

Рис. 1.13. Оценка уязвимости

Результирующая оценка уязвимости	
Атрибуты подверженности воздействию (выберите из числа указанных выше)	
высокая	5
средняя	3
низкая	1
уровень вероятности (1, 3 или 5)	

Рис. 7.14. Оценка уровня вероятности

Рис. 1.15 приведена шкала оценки эффективности текущих мер и средств защиты. Меньший результат означает большую эффективность элементов контроля и их способность уменьшать вероятность взлома.

Насколько эффективны текущие элементы контроля?	
Да — 0, Нет — 1	
Эффективно ли определена и реализована ответственность?	1,0
Эффективно ли осуществляется информирование?	1,0
Эффективно ли определены и реализованы процессы?	1,0
Эффективно ли существующие технологии или элементы контроля снижают угрозы?	1,0
Обеспечивают ли существующие методы аудита обнаружение злоупотреблений и недостатка контроля?	1,0
Сумма атрибутов контроля (0–5) =	

Рис. 1.15. Оценка эффективности текущего контроля

Полученные значения суммируются и заносятся в шаблон для уровня детализации.

Сумма уровней уязвимости и эффективности контроля (0–10) =	

Рис.1.16. Результирующая оценка

Пример заполненного шаблона представлен на рис. 1.17.

Прим. Рисунок взят из перевода описания, в который закралась неточность - в предпоследнем столбце первой строки следует читать "Уязвимость: 5, Контроль: 1", в предпоследнем столбце второй строки - "Уязвимость: 5, Контроль: 5".

Базовый риск (текущий)									
Актив		Подверженность воздействию							
Название актива	Уровень класса влияния	Многоуровневая защита	Описание угрозы	Описание уязвимости	Уровень подверженности воздействию (1–5)	Уровень подверженности воздействию (1–10)	Описания текущих элементов контроля	Уровень вероятности с контролем (1–10)	Уровень риска с контролем (0–100)
Информация о финансовых инвестициях заказчиков	10 (ВВБ)	Узлы	Несанкционированный доступ к информации о заказчиках путем хищения учетных данных консультантов по финансовым вопросам	Хищение учетных данных с управляемых компьютеров локальной сети вследствие несвоевременного обновления баз данных антивирусных средств или конфигураций узлов либо несвоевременной установки обновлений системы безопасности	4 (80%)	8	1. Каждый консультант имеет доступ только к информации о своих клиентах. Таким образом, подверженность воздействию составляет менее 100%. 2. Уведомления об обновлениях и исправлениях, отправляемые по электронной почте. 3. В локальной сети каждые несколько часов выполняется установка требуемых обновлений, что уменьшает временной интервал, в течение которого узлы локальной сети уязвимы перед взломом.	Уязвимость: 5 Контроль: 1 Всего = 6	48
Информация о финансовых инвестициях заказчиков	10 (ВВБ)	Узлы	Несанкционированный доступ к информации о заказчиках путем хищения учетных данных консультантов по финансовым вопросам	Хищение учетных данных с управляемых удаленных компьютеров вследствие несвоевременного обновления баз данных антивирусных средств или конфигураций узлов либо несвоевременной установки обновлений системы безопасности	4 (80%)	8	1. Каждый консультант имеет доступ только к информации о своих клиентах. Таким образом, подверженность воздействию составляет менее 100%. 2. Уведомления об обновлениях и исправлениях, отправляемые по электронной почте. — Отсутствует решение, позволяющее обеспечить соответствие требованиям за пределами локальной сети.	Контроль: 5 Всего = 10	80

Рис. 1.17. Перечень рисков на уровне детализации (SRMGTool3)

На приведенном выше рисунке показаны уровни риска и соответствующие элементы данных. Уровень риска определяется как произведение оценок уровня влияния (со значением от 1 до 10) и уровня вероятности (со значением от 0 до 10). В результате уровень риска может принимать значения от 0 до 100. Переход от числовой оценки к оценке по шкале "высокий", "средний" или "низкий" можно сделать в соответствии с таблицей, представленной на рис. 1.18.

В заключение процедуры оценки рисков, проводится количественный анализ. Чтобы определить количественные характеристики, необходимо выполнить следующие задачи.

- ✓ Сопоставить каждому классу активов в организации денежную стоимость.
- ✓ Определить стоимость актива для каждого риска.
- ✓ Определить величину ожидаемого разового ущерба (single loss expectancy - SLE).
- ✓ Определить ежегодную частоту возникновения (annual rate of occurrence - ARO).
- ✓ Определить ожидаемый годовой ущерб (annual loss expectancy - ALE).

Рис. 1.18. Результирующее качественное ранжирование

Количественную оценку предлагается начать с активов, соответствующих описанию класса ВВБ. Для каждого актива определяется денежная стоимость с точки зрения его материальной и нематериальной ценности для организации. Также учитывается:

- ✓ Стоимость замены.
- ✓ Затраты на обслуживание и поддержание работоспособности.
- ✓ Затраты на обеспечение избыточности и доступности.
- ✓ Влияние на репутацию организации.
- ✓ Влияние на эффективность работы организации.
- ✓ Годовой доход.
- ✓ Конкурентное преимущество.
- ✓ Внутренняя эффективность эксплуатации.
- ✓ Правовая и регулятивная ответственность.
- ✓ Процесс повторяется для каждого актива в классах СВБ и НВБ.

Каждому классу активов сопоставляется одно денежное значение, которое будет представлять ценность класса активов. Например, наименьшее среди активов данного класса. Данный подход уменьшает затраты времени на обсуждение стоимости конкретных активов.

После определения стоимостей классов активов необходимо определить и выбрать стоимость каждого риска.

Следующей задачей является определение степени ущерба, который может быть причинен активу. Для расчетов предлагается использовать ранее определенный уровень подверженности воздействию, на основе которого определяется фактор подверженности

воздействию (рекомендуемая формула пересчета - умножение значения уровня (в баллах) на 20%).

Последний шаг состоит в получении количественной оценки влияния путем умножения стоимости актива на фактор подверженности воздействию. В классической количественной модели оценки рисков это значение называется величиной ожидаемого разового ущерба (SLE). На рис. 1.19 приведен пример реализации такого подхода.

Величина высокого влияния на деятельность = $ M			Уровень подверженности воздействию	Фактор подверженности воздействию, %
			5	100
Класс актива			4	80
Значение ВВБ	**$ M**		3	60
Значение СВБ	**$ M/2**		2	40
Значение НВБ	**$ M/4**		1	20
Оценочное значение риска =	Значение класса актива × Фактор подверженности воздействию (%) = Ожидаемый разовый ущерб			

Рис. 1.19. Количественная оценка ожидаемого разового ущерба

Описание риска	Значение класса актива	Уровень подверженности воздействию	Величина подверженности воздействию	Ожидаемый разовый ущерб
Риск для узла локальной сети	$ 10	4	80%	$ 8
Риск для удаленного узла	$ 10	4	80%	$ 8

Рис. 1.20. Пример определения ожидаемого разового ущерба (суммы указаны в миллионах долларов)

Далее делается оценка ежегодной частоты возникновения (ARO). В процессе оценки ARO используются ранее полученные качественные оценки рис. 1.21.

Качественный уровень	Описание	Диапазон ежегодной частоты возникновения	Примеры описаний
Высокий	Очень вероятно	>= 1	Влияние раз в год или чаще
Средний	Вероятно	От 0,99 до 0,33	Не менее одного раза каждые 1–3 года
Низкий	Маловероятно	< 0,33	Реже, чем один раз в 3 года

Рис.1.21. Количественная оценка ежегодной частоты возникновения

Для определения ожидаемого годового ущерба (ALE) значения SLE и ARO перемножаются.

$$ALE = SLE \times ARO$$

Величина ALE характеризует потенциальные годовые убытки от риска. Хотя данный показатель может помочь в оценке ущерба заинтересованным лицам, имеющим финансовую подготовку, группа управления рисками безопасности должна напомнить,

что влияние на организацию не ограничивается величиной годовых издержек - возникновение риска может повлечь за собой причинение ущерба в полном объеме.

Подводя итог, можно еще раз отметить, что процесс управления рисками безопасности, предлагаемый корпорацией Майкрософт, использует комбинированный подход включающий оценку рисков на качественном уровне на начальном этапе и количественную оценку - на заключительном.

Практическая часть

В ходе данной лабораторной работы мы познакомимся с разработанной Microsoft программой для самостоятельной оценки рисков, связанных с безопасностью - Microsoft Security Assessment Tool (MSAT). Она бесплатно доступна на сайте Microsoft по ссылке http://www.microsoft.com/downloads/details.aspx?displaylang=ru&FamilyID=cd057d9d-86b9-4e35-9733-7acb0b2a3ca1.

В ходе работы, пользователь, выполняющий роль аналитика, ответственного за вопросы безопасности, отвечает на две группы вопросов.

Первая из них посвящена бизнес-модели компании, и призвана оценить риск для бизнеса, с которым компания сталкивается в данной отрасли и в условиях выбранной бизнес-модели. Создается так называемый профиль риска для бизнеса (ПРБ).

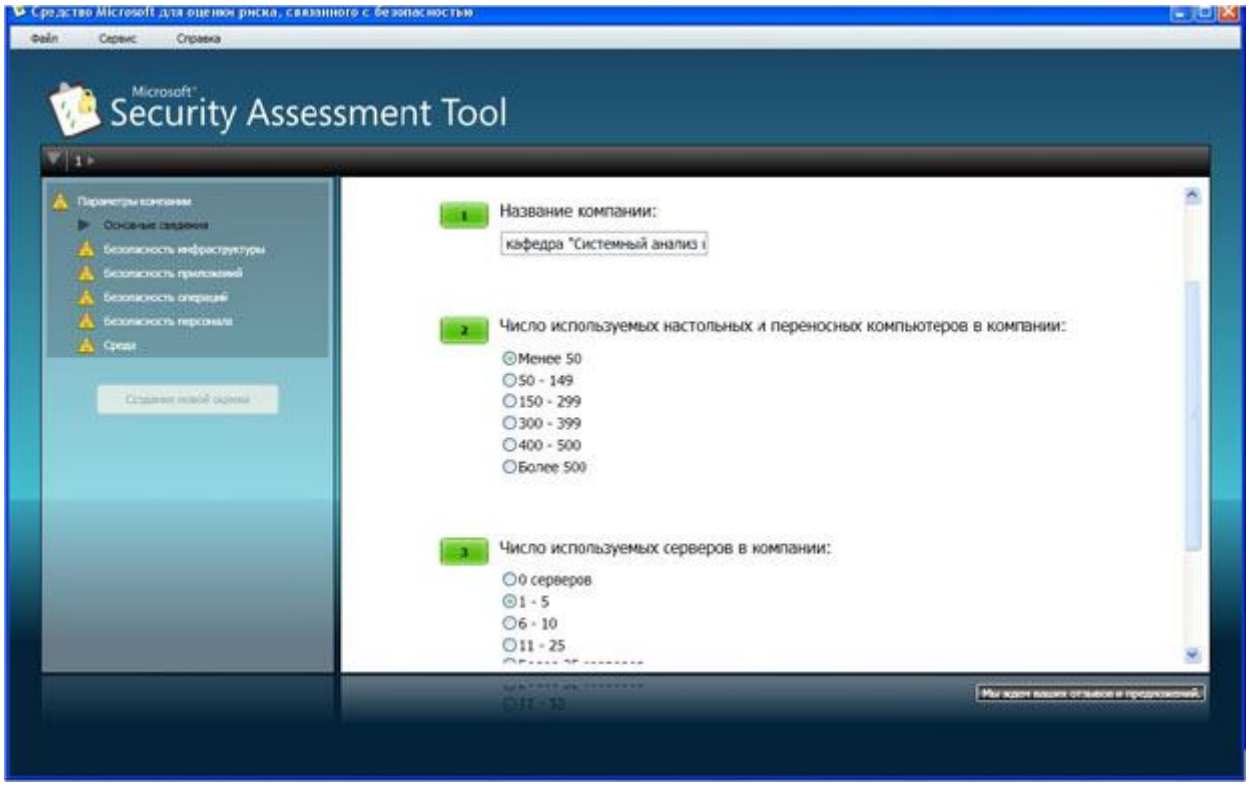


Рис. 1.22. Информация о компании

Вопросы этого этапа разбиты на 6 групп. Первая (рис. 1.22) касается общих сведений о компании - название, число компьютеров, серверов и т.д. Вторая группа вопросов озаглавлена "Безопасность инфраструктуры". Примеры вопросов - "использует ли

компания подключение к Интернет", "размещаются ли службы, используемые как внешними, так и внутренними клиентами, в одном и том же сегменте" и т.д. Остальные группы - "Безопасность приложений", "Безопасность операций", "Безопасность персонала", "Среда".

Надо отметить, что при локализации не все вопросы первого этапа были качественно переведены с английского. Чего стоит вопрос: "Прошла ли ваша организация через "копирование и замена" касающиеся любого основного компонента технологии, за последние 6 месяцев ?"! Однако во всех случаях можно из контекста понять, о чем идет речь (в приведенном примере вопрос был, относительно того, менялись ли используемые технологии обработки информации).

Когда проведен первый этап оценки, полученная информация обрабатывается (для этого требуется подключение к Интернет), после чего начинается второй этап анализа. Для технических специалистов он будет более интересен, т.к. касается используемых в компании политик, средств и механизмов защиты (рис. 1.23). Стоит сказать, что и перевод вопросов второго этапа выполнен существенно лучше.

Рис. 1.23 Анализ используемых механизмов защиты

Вопросы организованы в соответствии с концепцией многоуровневой (эшелонированной) защиты. Сначала рассматривается защита инфраструктуры (защита периметра, аутентификация…), затем вопросы защиты на уровне приложений, далее проводится анализ безопасности операций (определена ли политика безопасности,

политика резервного копирования и т.д.), последняя группа вопросов касается работы с персоналом (обучение, проверка при приеме на работу и т.д.).

Во многом тематика вопросов соответствует разделам стандартов ISO 17799 и 27001, рассмотренных в теоретической части курса.

После ответа на все вопросы программа вновь обращается к удаленному серверу и генерирует отчеты. Наибольший интерес для технических специалистов представляет "Полный отчет". В частности, он содержит предлагаемый список приоритетных действий. Фрагмент списка представлен в табл. 1.1

Таблица 1.1. Список предлагаемых действий

Список приоритетных действий	
Предмет анализа	**Рекомендация**
Высокий приоритет	
Операции > Управление средствами исправления и обновления > Управление средствами исправления	Наличие политики исправлений и обновлений для операционных систем является полезным начальным шагом, однако необходимо разработать такую же политику и для приложений. Разработайте такую политику, пользуясь сведениями, доступными в разделе, посвященном передовым методикам. Сначала установите исправления для внешних приложений и приложений Интернета, затем для важных внутренних приложений и, наконец, для не особо важных приложений.

Задание к практической работе

Работа выполняется в малых группах (2-3 человека), в которых необходимо распределить обязанности. Обязанности распределяются по следующим ролям: руководитель, специалист по работе с персоналом, IT-специалист.

1) Ознакомьтесь с теоретическим материалом лабораторной работы;

2) Составьте сводный отчет в форме таблицы о существующих методиках оценки рисков. Отчет должен содержать набор параметров, по которым будет произведено сравнение. Таблица должна содержать методики CRAMM, FRAP, OCTAVE, RiskWatch, Microsoft. Кроме того необходимо самостоятельно найти 1-2 методики и также описать в таблице.

3) Выбрать любую компанию и кратко описать ее деятельность (использовать ресурсы интернет).

4) Опишите 5-7 активов выбранной компании разного класса влияния исходя из определения понятия «актив». За основу используйте таблицу 1.5. Определить класс

актива, уровень подверженности воздействию, уровень влияния. Результаты представить в форме таблицы.

5) Выполните их приоретизацию на основе таблицы 1.6. Выпишите активы с рисками высокого уровня, на основе таблиц 1.7 и 1.8.

6) Проведите оценку риска от влияния на активы при помощи программы Microsoft Assessment Tool (MSAT). Для этого необходимо из меню Пуск запустить соответствующий ярлык.

7) Задайте название своей компании, выберите профиль компании ПРБ (бизнес-профиль) и ответьте на поставленные вопросы.

8) С целью экономии времени предлагается распределить вопросы по соответствующим ролям.

9) После получения итогового отчета программы необходимо сохранить его и скопировать в тестовый файл. (Можно открывать полученные отчеты в программе MSAT при помощи пункта меню Файл – Управление оценками)

10) Далее работа разделяется между участниками группы. Руководитель должен описать деятельности фирмы, специалист по работе с персоналом – выписать 5-8 вопросов из программы относительно персонала, IT-специалист – 5-8 вопросов по организации информационной среды предприятия.

11) Из отчета, полученного в программе MSAT, необходимо выбрать рекомендации, касающиеся деятельности специалиста и оформить отчет

12) Руководитель составляет итоговое описание.

13) Таким образом, результатом выполнения лабораторной работы является письменный отчет, содержащий следующую информацию:

а) Титульный лист (в свободной форме с указание рабочей группы и ролей);

б) Сравнительная характеристика программных продуктов для оценки рисков;

в)Описание деятельности предприятия (3-4 предложения);

г) Описание активов предприятия (3-4 актива) на примере таблицы 1.5.

д) Уровни подверженности воздействию, уязвимости на примере таблицы 1.6.

е) Список приоретизации активов;

ж) Вопросы из программы MSAT по тематике: общие вопросы организации; вопросы об организации работы с персоналом; вопросы об организации информационной среды предприятия.

з) Отчет из программы и рекомендации из программы MSAT по тематике: отчет о рисках, связанных с организацией работы с персоналом и информационной среды предприятия.

и) Итоговый отчет руководителя.

Контрольные вопросы

1) Назовите методики для оценки рисков по уровню?
2) Опишите особенности методики CRAMM?
3) Опишите особенности методики FRAP?
4) Опишите особенности методики OCTAVE?
5) Опишите особенности методики Microsoft?
6) Каким образом можно оценить возможные потери от нарушения информационной безопасности?

Практическое занятие № 4

Тема «Метод перестановки для шифрования текстов. Шифрование по методу Виженера»

Цели занятия: изучить метод перестановки для шифрования открытого текста, изучить метод многоалфавитной одноконтурной обыкновенной подстановки для шифрования открытого текста.

Форма организации занятия: индивидуальная работа.

Теоретическая часть

Шифрование является одним из эффективных способов защиты текстовой информации. При шифровании существуют следующие понятия [4].

Открытый текст – информация, содержание которой может быть понятно любому субъекту.

Шифрование – процесс преобразования открытого текста в шифротекст или криптограмму с целью сделать его содержание непонятным для посторонних лиц. В общем виде процесс шифрования описывается выражением вида $C=E_k(P)$ где С – шифротекст; Е – функция шифрования; k – ключ шифрования; P – открытый текст.

Расшифрование – процесс обратного преобразования шифротекста в открытый текст. В общем виде процесс расшифрования описывается выражением вида $P=D_{k'}(C)$ где D – функция расшифрования; k' – ключ расшифрования.

Криптосистема – совокупность алгоритмов, реализуемых функциями E и D, множества ключей k, $'k$ и шифротекстов.

---

[4] *Системы автоматизированного расчёта в управлении качеством и при защите информации : лабораторные работы / сост.: П.В. Балабанов, С.В. Пономарёв. – Тамбов : Изд-во Тамб. гос. техн. ун-та, 2009. – 32 с. URL: http://www.234555.ru/publ/12-1-0-408 (Режим доступа свободный).*

Криптограмма (загадочное письмо или тайнопись) – наука о защите информации с помощью шифрования.

Криптоанализ – наука о методах дешифрования.

Криптостойкость – характеристика надёжности шифротекста от вскрытия.

Криптостойкость шифра характеризуют двумя величинами:

1) минимальным объёмом шифротекста, статическим анализом которого можно его вскрыть и получить открытый текст без знания ключа;

2) числом MIPS-часов (лет) – временем работы условного криптоаналитического компьютера производительностью 1 000 000 операций в секунду, необходимым для вскрытия шифротекста.

Данная работа состоит из двух частей. В первой части необходимо выполнить задание на шифрование текста по методу обыкновенной перестановки, во второй части – по методу многоалфавитной одноконтурной обыкновенной перестановки.

Часть I. Шифрование по методу обыкновенной перестановки

В настоящее время известно множество методов шифрования, одним из которых является метод перестановки. В соответствии с этим методом биты (или символы) открытого текста переставляются в соответствии с задаваемым ключом шифрования правилом

$$1 \le i \le n,\ C_i = P_{k[i]}, \tag{1.1}$$

где $P = \{P_1,\ P_2,\ P_3, \ldots P_i,\ \ P_n\}$ – открытый текст; n – длина открытого текста (количество символов текста); $C = \{C_1,\ C_2,\ C_3, \ldots C_i,\ \ C_n\}$ – шифротекст; $k = \{k_1,\ k_2,\ k_3, \ldots k_i,\ k_n\}$ – ключ шифрования.

При расшифровании используется обратная перестановка:

$$P_{k[i]} = C_i. \tag{1.2}$$

Как видно из приведенных выражений, ключ должен удовлетворять условиям: $k_i \neq k_j,\ 1 \le k_i \le n$

Рассмотрим пример шифрования слова «Пример» методом перестановки. Зададим ключ, который должен быть равен 6-ти символам (количеству символов в шифруемом слове) в виде $k = \{1, 2, 3, 4, 5, 6\}$. В данном примере зададим следующий ключ $k = \{1, 4, 6, 2, 3, 5\}$. Для удобства запишем все данные для шифрования в одну таблицу (таблица 1.2).

Таблица 1.2. Данные для шифрования

Символы открытого текста	П	Р	И	М	Е	Р
	P_1	P_2	P_3	P_4	P_5	P_6

Цифровые символы ключа	1	4	6	2	3	5
	k_1	k_2	k_3	k_4	k_5	k_6

Запишем открытый текст в виде P = {П Р И М Е Р}, далее необходимо получить шифротекст в виде C = *{C_1, C_2, C_3, C_5, C_6}*.

Применим формулу (1.1) с выбранным ключом *k* к слову «Пример». Получим следующие выражения:

$$C_1 = P_{k[1]} = P_1 = 'П'; \quad C_2 = P_{k[2]} = P_4 = 'м'; \quad C_3 = P_{k[3]} = P_6 = 'р';$$

$$C_4 = P_{k[4]} = P_2 = 'р'; \quad C_5 = P_{k[5]} = P_3 = 'и'; \quad C_6 = P_{k[6]} = P_5 = 'е';$$

В конечном итоге получим шифротекст C = Пмррие

Очевидно, что применив другой ключ, получим другой вид шифрованного текста.

При дешифровании используем обратную операцию по формуле (1.2):

Выпишем данные для дешифрования в виде таблицы 1.3:

Таблица 1.3. Данные для дешифрования

Символы шифротекста	П	м	р	р	и	е
	C_1	C_2	C_3	C_4	C_5	C_6
Цифровые символы ключа	1	4	6	2	3	5
	k_1	k_2	k_3	k_4	k_5	k_6
Порядок формирования дешифруемого текста	P_1	P_2	P_3	P_4	P_5	P_6

Следует учесть, что при расшифровании необходимо получить не только исходное значение зашифрованного символа, но и его порядковый номер P_i в исходном тексте.

$$P_{k[1]} = P_1 = C_1 = 'П'; \quad P_{k[2]} = P_4 = C_2 = 'м'; \quad P_{k[3]} = P_6 = C_3 = 'р';$$

$$P_{k[4]} = P_2 = C_4 = 'р'; \quad P_{k[5]} = P_3 = C_5 = 'и'; \quad P_{k[6]} = P_5 = C_6 = 'е';$$

Таким образом, получим *P = {P_1, P_2, P_3, P_4, P_5, P_6}* = {Пример}.

Если требуется зашифровать достаточно длинный текст длиной *n*, то его можно разбить на блоки, длина которых равна длине ключа *m*. Открытый текст записывают в таблицу с числом столбцов, равным длине ключа (каждый блок открытого текста записывается в столбец таблицы). Затем столбцы полученной таблицы переставляются в соответствии с ключом перестановки, а шифротекст считывается из строк таблицы последовательно.

Пусть требуется зашифровать открытый текст «этот пример шифрования». Длина текста (вместе с пробелами n = 22). Выберем ключ шифрования в виде *k = {3, 5, 4, 2, 1}* (*m = 5*).

Разбиваем строку «этот пример шифрования» на пять блоков, каждый из который располагаем в таблицу:

э	п	р	р	и
т	р		о	я
о	и	ш	в	
т	м	и	а	
	е	ф	н	

Переставляем столбцы полученной таблицы в соответствии с ключом *k = {3, 5, 4, 2, 1}*. Получим

р	и	р	п	э
	я	о	р	т
ш		в	и	о
и		а	м	т
ф		н	е	

Считываем последовательно текст из строк таблицы. Получим следующий шифр: *рирпэ яортш виои амтф не.*

Для расшифрования шифротекст записывают в таблицу того же размера по строкам, затем производится обратная перестановка столбцов в соответствии с ключом, после чего расшифрованный текст считывается из таблицы по столбцам. Ниже приведены этапы расшифровывания: а) запись шифротекста в таблицу; б) перестановка столбцов в соответствии с ключом; в) считывание символов по столбцам.

Этап а

р	и	р	п	э

Этап б

э	п	р	р	и

	я	о	р	т
ш		в	и	о
и		а	м	т
ф		н	е	

т	р		о	я
о	и	ш	в	
т	м	и	а	
	е	ф	н	

Результатом считывания данных таблицы этапа б будет фраза «этот пример шифрования».

Если в качестве ключа перестановки использовать последовательность не цифр, а произвольных символов (например, пароль пользователя), то его необходимо предварительно преобразовать в последовательность целых чисел от 1 до *m*.

Например, пользователь ввел пароль «Петров».

Отсортируем символы в алфавитном порядке.

Получим Петров=>веопрт. Каждому символу присвоим порядковый номер:

в е о п р т

1 2 3 4 5 6

Заменим символы введённого пароля цифрами и получим ключ: 426531.

Задание к практической работе

1. Изучить теоретические основы метода перестановки.

2. Зашифровать (расшифровать) слово открытого текста ключом, длина которого равна длине шифруемого слова (задание выдается преподавателем).

3. Зашифровать и расшифровать фразу (выдается преподавателем) при помощи ключа.

4. Придумать символьный пароль, преобразовать его в ключ и зашифровать (расшифровать) фразу из задания № 3 с помощью этого ключа.

Оформление результатов выполнения лабораторной работы

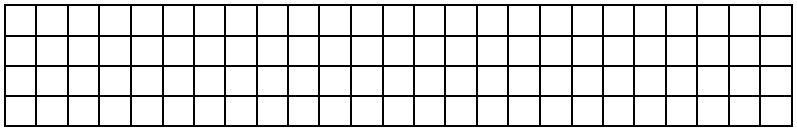
Ответы к заданиям оформляются в письменном виде или в текстовом редакторе Microsoft Word с последующим сохранением в файл. Название файла формируется из фамилии и номера лабораторной работы, например Иванов_11.doc. В тексте ответа должны быть приведены все промежуточные расчеты.

Исходное слово для шифрования: Ключ шифрования:

Результат шифрования Символьный пароль

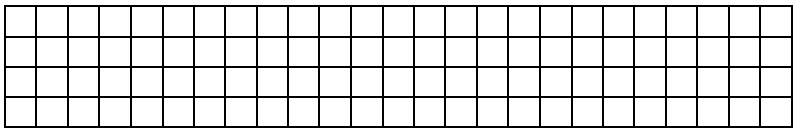
Цифровой пароль _ _ _ _ _ _ _ _ _ _

Фраза для шифрования



Этап а Этап б

Результат шифрования



Часть II. Шифрование по методу многоалфавитной одноконтурной обыкновенной перестановки

В течение столетий использование простого одноалфавитного шифра замены было достаточным, чтобы обеспечить секретность. Последующее развитие частного анализа, вначале арабами, а затем в Европе, разрушило его стойкость. Трагическая казнь Марии Стюарт, королевы Шотландии, явилась драматической иллюстрацией слабостей одноалфавитной замены. Ряд ученых эпохи возрождения трудились над созданием нового шифра, однако только в 1549 г. Французский дипломат Блез де Виженер смог объединить труды многих людей и представить миру новый методы шифрования при помощи многоалфавитной одноконтурной перестановки.

Стойкость шифра Виженера состоит в том, что для зашифрования сообщения в нем используется не один, а несколько различных шифроалфавитов (для английского языка –

26, для русского – 33). Шифрование начинается с так называемого квадрата Виженера, пример которого показан в таблице 1.4.: алфавит открытого текста с последующими 26 шифроалфавитами, каждый из которых сдвинут на одну букву относительно предыдущего алфавита. [5]

Таблица 1.4. Квадрат Виженера

Открытый алфавит	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Верхний ряд квадрата, со строчными буквами, представляет буквы алфавита открытого текста. Вы можете зашифровать каждую букву открытого текста с помощью любого из 26 шифроалфавитов. Например, есил используется шифроалфавит номер 2, то буква a зашифровывается как C, если же используется шифроалфавит номер 12, тогда a преобразуется в M.

Чтобы показать, как применяется ключевое слово с квадратом Виженера для защифровывания короткого сообщения, зашифруем следующую короткую фразу **divert troops to east ridge** с помощью ключевого слова **WHITE**. Прежде всего, ключевое слово записывается над сообщением буква за буквой, и его повторяют до тех пор, пока каждой букве в сообщении не будет сопоставлена буква ключевого слова. Далее приступаем к созданию шифротекста, что делается следующим образом:

[5] Сингх С. Книга шифров. Тайная история шифров и их расшифровки. – М.: АСТ: Астрель, 2009. 447 с.

1. чтобы зашифровать первую букву d, определим вначале букву ключа над ней, W, которая в свою очередь задает строку в квадрате Виженера. Именно строка, начинающаяся с буквы W, - двадцать вторая строка, - и является шифроалфвавитом, который будет использован для шифрования буквы d открытого текста.
2. смотрим, где столбец с буквой d в первой строке пересекается со строкой, начинающейся с буквы W – это будет буква Z. Следовательно, буква d в открытом тексте будет буквой Z в шифротексте.
3. точно также шифруем букву I открытого текста - это будет буква P шифротекста.
4. широтекст записывается под исходным текстом буква под буквой, пример показан на рис. 1.24.

Ключевое слово	W H I T E W H I T E W H I T E W H I T E W H I
Исходный текст сообщения	d i v e r t t r o o p s t o e a s t r i d g e
Зашифрованный текст сообщения	Z P D X V P A Z H S L Z B H I W Z B K M Z N M

Рис. 1.24. Пример записи ключевого слова, исходного текста и шифротекста.

На рис. 1.25. приведен квадрат Виженера с пятью выделенными строками (т.е. пятью шифроалфавитами), которые определяются ключевым словом WHITE.

Открытый алфавит	a b c d e f g h i j k l m n o p q r s t u v w x y z
1	B C D E F G H I J K L M N O P Q R S T U V W X Y Z A
2	C D E F G H I J K L M N O P Q R S T U V W X Y Z A B
3	D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
4	E F G H I J K L M N O P Q R S T U V W X Y Z A B C D
5	F G H I J K L M N O P Q R S T U V W X Y Z A B C D E
6	G H I J K L M N O P Q R S T U V W X Y Z A B C D E F
7	H I J K L M N O P Q R S T U V W X Y Z A B C D E F G
8	I J K L M N O P Q R S T U V W X Y Z A B C D E F G H
9	J K L M N O P Q R S T U V W X Y Z A B C D E F G H I
10	K L M N O P Q R S T U V W X Y Z A B C D E F G H I J
11	L M N O P Q R S T U V W X Y Z A B C D E F G H I J K
12	M N O P Q R S T U V W X Y Z A B C D E F G H I J K L
13	N O P Q R S T U V W X Y Z A B C D E F G H I J K L M
14	O P Q R S T U V W X Y Z A B C D E F G H I J K L M N
15	P Q R S T U V W X Y Z A B C D E F G H I J K L M N O
16	Q R S T U V W X Y Z A B C D E F G H I J K L M N O P
17	R S T U V W X Y Z A B C D E F G H I J K L M N O P Q
18	S T U V W X Y Z A B C D E F G H I J K L M N O P Q R
19	T U V W X Y Z A B C D E F G H I J K L M N O P Q R S
20	U V W X Y Z A B C D E F G H I J K L M N O P Q R S T
21	V W X Y Z A B C D E F G H I J K L M N O P Q R S T U
22	W X Y Z A B C D E F G H I J K L M N O P Q R S T U V
23	X Y Z A B C D E F G H I J K L M N O P Q R S T U V W
24	Y Z A B C D E F G H I J K L M N O P Q R S T U V W X
25	Z A B C D E F G H I J K L M N O P Q R S T U V W X Y
26	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Рис. 1.25. Методика шифрования с использованием квадрата Вижинера.

Одним из главных достоинств шифра Виженера является то, что он неуязвим для частотного анализа. Это обусловлено тем, что одна и та же буква в открытом тексте, может быть зашифрована многими другими буквами в шифротексте.

Помимо того, что шифр Виженера неуязвим для частотного анализа, он подразумевает использование гигантского количества ключей. Отправитель и получатель могут договориться об использовании любого слова из словаря, любой комбинации слов или даже придумать свои слова. А криптоаналитик, не сможет дешифровать сообщение перебором всех возможных ключей, так как число возможных вариантов просто огромно.

Контрольные вопросы

1) Дать определение шифротекста
2) Дать определение открытого текста
3) Дать определение криптосистемы
4) Дать определение криптоанализа
5) Что такое криптостойкость и чем она характеризуется?
6) В чем заключается метод шифрования текста перестановкой?
7) Какие еще существуют методы шифрования текста?
8) Где можно использовать шифрование текста?
9) Объяснить, почему получил свое название метод шифрования «Одноконтурная многоалфавитная обыкновенная перестановка».
10) Объяснить суть шифрования по методу Вижинера?
11) Чем определяется стойкость шифра по методу Вижинера?
12) **Творческое задание:** попробуйте расшифровать шифротекст при помощи ключа.

Практическое занятие № 5

*Тема «*Исследование электронной цифровой подписи на основе алгоритма RSA*»*

Цель занятия: изучить методику построения электронной цифровой подписи на основе алгоритма RSA.

Форма организации занятия: индивидуальная работа.

Теоретическая часть

Технология применения электронной цифровой подписи (ЭЦП) предполагает наличие сети абонентов, обменивающихся подписанными электронными документами. При обмене электронными документами по сети значительно снижается затраты, связанные с их обработкой, хранением и поиском [6].

Одновременно при этом возникает проблема, как аутентификации автора электронного документа, так и самого документа, т.е. установление подлинности автора и отсутствие изменений в полученном электронном сообщении.

[6] *Системы автоматизированного расчёта в управлении качеством и при защите информации : лабораторные работы / сост.: П.В. Балабанов, С.В. Пономарёв. – Тамбов : Изд-во Тамб. гос. техн. ун-та, 2009. – 32 с. URL: http://www.234555.ru/publ/12-1-0-408 (Режим доступа свободный).*

В алгоритмах ЭЦП, как и в асимметричных системах шифрования, используются однонаправленные функции. ЭЦП используется для аутентификации текстов, передаваемых по телекоммуникационным каналам. ЭЦП представляет собой относительно небольшой объем дополнительной цифровой информации, передаваемой вместе с подписанным текстом.

Концепция формирования ЭЦП основана на обратимости асимметричных шифров, а также на взаимосвязанности содержимого сообщения, самой подписи и пары ключей. Изменение хотя бы одного из этих элементов сделает невозможным подтверждение подлинности подписи, которая реализуется при помощи асимметричных алгоритмов шифрования и хэш-функций.

Система ЭЦП содержит две процедуры:

- ✓ Формирование цифровой подписи;
- ✓ Проверку цифровой подписи;

В процедуре формирования подписи используется секретный ключ отправителя сообщения, в процедуре проверки подписи – открытый ключ отправителя[7].

Алгоритм RSA (слово образовано от заглавных букв создателей алгоритма Rivest, Shamir и Adleman) – криптографический алгоритм с открытым ключом. RSA стал первым алгоритмом такого типа, пригодным и для шифрования, и для цифровой подписи. Алгоритм используется в большом числе криптографических приложений. Безопасность системы RSA определяется вычислительной трудностью разложения на множители больших целых чисел. Недостатком алгоритма цифровой подписи RSA является уязвимость ее к мультипликативной атаке. Другими словами, алгоритм ЭЦП на основе RSA позволяет хакеру без знания секретного ключа сформировать подписи под теми документами, в которых результат хэширования можно вычислить как произведение результата хэширования уже подписанных документов [8].

Обобщенная схема формирования и проверки электронной цифровой подписи приведена на рис. 1.26.

[7] Там же.
[8] Там же.

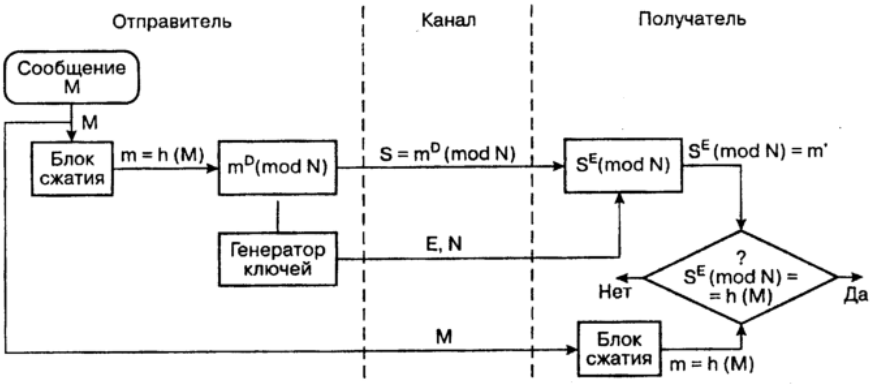


Рис. 1.26. Схема RSA электронной цифровой подписи

Изучение алгоритма RSA электронной цифровой подписи

Определение открытого «e» и секретного «d» ключей

Действие отправителя

1. Выбрать два взаимно простых числа p и q;
2. Определить их произведение $n = p \cdot q$;
3. Определить функцию Эйлера $\varphi(n) = (p - 1)(q - 1)$;
4. Выбрать секретный ключ d с учетом условий: $1 < d \leq \varphi(n)$; $НОД(d, \varphi(n)) = 1$;
5. Определить значение открытого ключа e: $e < n$, $e \cdot d \equiv 1 \ (mod \ \varphi(n))$.

Формирование электронной цифровой подписи

1. Вычислить хэш-сообщение M: $m = h(M)$;
2. Для получения ЭЦП шифруем хэш-значение m с помощью секретного ключа d и отправляем получателю цифровую подпись $S = m^d \ (mod \ n)$ и открытый текст сообщения M.

Аутентификация сообщения – проверка подлинности подписи

1. Расшифровкать цифровую подпись S с помощью открытого ключа e и вычислить ее хэш-значения $m' = S^e \ (mod \ n)$
2. Вычислить хэш-значение принятого открытого текста M

$$m = h(M)$$

3. Сравнить хэш-значения m и m', если $m = m'$, то цифровая подпись S - достоверна.

Пример вычисления хэш-сообщения M: m=h(M)

а) Хэшируемое сообщение M представим как последовательности целых чисел 312. В соответствии с приведенным выше алгоритмом формирования ЭЦП на основе RSA выбираем два взаимно простых числа $p = 3$ и $q = 11$, вычисляем значение $n = p \cdot q = 3 \cdot 11 = 33$, выбираем значение секретного ключа $d = 7$ и вычисляем значение открытого ключа $e = 3$. Вектор инициализации H_0 выбираем равным 6 (выбор производится случайным образом).

Хэш-код сообщения *M = 312* формируется следующим образом:

$H_1 = (M_1 + H_0)^2 \pmod n = (3+6)^2 \pmod{33} = 81 \pmod{33} = 15$;

$H_2 = (M_2 + H_1)^2 \pmod n = (1+15)^2 \pmod{33} = 256 \pmod{33} = 25$;

$H_3 = (M_3 + H_2)^2 \pmod n = (2+25)^2 \pmod{33} = 729 \pmod{33} = 3$, *m = 3*.

б) Для получения ЭЦП шифруем хэш-значение *m* с помощью секретного ключа *d* и отправляем получателю цифровую подпись

$S = m^d \ (mod\ n)$ и открытый текст сообщения *M*

$S = 3^7 \ (mod\ 33) = 2187 \ (mod\ 33) = 9$

в) Проверка подлинности ЭЦП

Расшифровка *S* (т.е. вычисление её хэш-значения *m′*) производится с помощью открытого ключа e.

$$m' = S^e \pmod n = 9^3 \pmod{33} = 729 \pmod{33} = 3$$

г) Сравниваем значения *m* и *m′, е*сли *m = m′,* то подпись достоверна.

Задание для практического занятия

На основе теоретического материала, указанного алгоритма и рассмотренного примера сформировать электронную цифровую подпись (значение чисел выдается преподавателем).

Контрольные вопросы

1) Откуда получил название алгоритм RSA?
2) Рассказать основной принцип, на котором основан алгоритм RSA.
3) Назовете процедуры, которые составляют систему электронной цифровой подписи.
4) Основное назначение электронной цифровой подписи и условие ее существования.
5) На чем основана концепция формирования ЭЦП?
6) Дать пояснения к блок-схеме алгоритма RSA.

Практическое занятие № 6

Тема «Выявление уязвимостей в компьютерных системах и построение локальной политики паролей»

Цель занятия: получить навык выявления уязвимостей операционной системы и разработки локальной политики паролей.

Оборудование: компьютер с операционной системой Windows, программа Microsoft Baseline Security analyzer, наличие доступа к ресурсам глобальной сети Internet.

Форма организации занятия: индивидуальная работа.

Теоретическая часть

Термин «уязвимость» часто упоминается в связи с компьютерной безопасностью, во множестве самых различных контекстов.

В общем случае, уязвимость ассоциируется с нарушением политики безопасности, вызванным неправильно заданным набором правил или ошибкой в обеспечивающей безопасность компьютера программе. Стоит отметить, что теоретически все компьютерные системы имеют уязвимости. Но то, насколько велик потенциальный ущерб от вирусной атаки, использующей уязвимость, позволяет подразделять уязвимости на активно используемые и не используемые вовсе.

Предпринималось много попыток четко определить термин «уязвимость» и разделить два его значения. MITRE, исследовательская группа, финансируемая федеральным правительством США, занимающаяся анализом и разрешением критических проблем с безопасностью, разработала следующие определения:

[...] Уязвимость — это состояние вычислительной системы (или нескольких систем), которое позволяет[9] :

- ✓ исполнять команды от имени другого пользователя;
- ✓ получать доступ к информации, закрытой от доступа для данного пользователя;
- ✓ показывать себя как иного пользователя или ресурс;
- ✓ производить атаку типа «отказ в обслуживании».

Предпринималось много попыток четко определить термин «уязвимость» и разделить два его значения.

Считается, что атака, производимая вследствие слабой или неверно настроенной политики безопасности, лучше описывается термином «открытость» (exposure).

Открытость — это состояние вычислительной системы (или нескольких систем), которое не является уязвимостью, но:

- ✓ позволяет атакующему производить сбор защищенной информации;
- ✓ позволяет атакующему скрывать свою деятельность;
- ✓ содержит возможности, которые работают корректно, но могут быть легко использованы в неблаговидных целях;
- ✓ является первичной точкой входа в систему, которую атакующий может использовать для получения доступа или информации.

Когда хакер пытается получить неавторизованный доступ к системе, он производит сбор информации (расследование) о своем объекте, собирает любые доступные данные и

[9] *1) Энциклопедия безопасности Касперского. URL: http://www.securelist.com/ru/threats/detect (Режим доступа: свободный);*

затем использует слабость политики безопасности («открытость») или какую-либо уязвимость. Существующие уязвимости и открытости являются точками, требующими особенно внимательной проверки при настройке системы безопасности против неавторизованного вторжения.

Примеры распространенных уязвимостей

Наиболее распространенная в настоящее время на подключенных к интернету компьютерах операционная система Microsoft Windows содержит множественные опасные уязвимости. Чаще всего хакерами используются уязвимости в IIS, MS SQL и Internet Explorer, а также системах обработки файлов и сервисах сообщений самой операционной системы[10].

Уязвимость в IIS, подробно описанная в Microsoft Security Bulletin MS01-033, является одной из наиболее часто используемых уязвимостей Windows. В последние годы было написано множество сетевых червей, пользующихся данной уязвимостью, но одним из наиболее известных является CodeRed. CodeRed был впервые обнаружен 17 июля 2001 года, и, по некоторым оценкам, заразил около 300 тысяч компьютеров, помешал работе множества предприятий и нанес значительный финансовый ущерб компаниям по всему миру. Хотя Microsoft и выпустила вместе с бюллетенем MS01-033 патч, закрывающий используемую червем уязвимость, некоторые версии CodeRed до сих пор продолжают распространяться.

Сетевой червь Spida, обнаруженный спустя почти год после появления CodeRed, использовал для своего распространения открытость в MS SQL. Некоторые стандартные инсталляции MS SQL не защищали паролем системный эккаунт «SA», позволяя любому человеку с доступом к системе через сеть запускать на ней на исполнение произвольные команды. При использовании этой уязвимости, червь открывает эккаунту «Guest» полный доступ к файлам компьютера, после чего производит загрузку самого себя на заражаемый сервер.

Сетевой червь Slammer, обнаруженный в конце января 2003 года, использовал более простой способ заражения компьютеров под управлением Windows с работающим сервером MS SQL, а именно — уязвимость при переполнении буфера в одной из подпроцедур обработки UDP-пакетов. Поскольку червь был достаточно мал — всего 376 байт — и использовал протокол UDP, предназначенный для быстрой пересылки малых объемов данных, Slammer распространялся с невероятной скоростью. По некоторым

[10] *Нестеров С.А. Анализ и управление рисками в операционных системах на базе операционных систем Microsoft. Лекция 3. «Методики построения систем защиты информации». - Интернет университет информационных технологий . ИНТУИТ. - URL: http://www.intuit.ru/department/itmngt/riskanms/3/5.html (Режим доступа: требуется регистрация).*

оценкам, Slammer поразил порядка 75 тысяч компьютеров по всему миру за первые 15 минут эпидемии.

Выявление уязвимостей с помощью Microsoft Baseline Security Analyzer. Настройка локальной политики паролей

Microsoft Baseline Security analyzer - программа, позволяющая проверить уровень безопасности установленной конфигурации операционной системы (ОС) Windows 2000, XP, Server 2003, Vista Server 2008. Также проверяется и ряд других приложений разработки Microsoft. Данное средство можно отнести к разряду систем анализа защищенности. Оно распространяется бесплатно и доступно для скачивания с web-сервера Microsoft (адрес страницы данной утилиты на момент подготовки описания был: http://technet.microsoft.com/ru-ru/security/cc184924(en-us).aspx).

В процессе работы BSA проверяет наличие обновлений безопасности операционной системы, офисного пакета Microsoft Office(для версий XP и более поздних), серверных приложений, таких как MS SQL Server, MS Exchange Server, Internet Information Server и т.д. Кроме того, проверяется ряд настроек, касающихся безопасности, например, действующая политика паролей [11].

Интерфейс программного продукта.

При запуске открывается окно, позволяющее выбрать объект проверки - один компьютер (выбирается по имени или ip-адресу), несколько (задаваемых диапазоном ip-адресов или доменным именем) или просмотреть ранее сделанные отчеты сканирования системы (рис. 1.27) [12]. При выборе сканирования отдельного компьютера по умолчанию подставляется имя локальной станции, но можно указать имя или ip-адрес другого компьютера.

Можно задать перечень проверяемых параметров. На рис. 1.28 представлен выбор вариантов проверки:

- ✓ проверка на наличие уязвимостей Windows, вызванных некорректным администрированием;
- ✓ проверка на "слабые" пароли (пустые пароли, отсутствие ограничений на срок действия паролей и т.д.);
- ✓ проверка на наличие уязвимостей web-сервера IIS, вызванных некорректным администрированием;
- ✓ аналогичная проверка в отношении СУБД MS SQL Server;
- ✓ проверка на наличие обновлений безопасности.

[11] Там же.
[12] Там же.

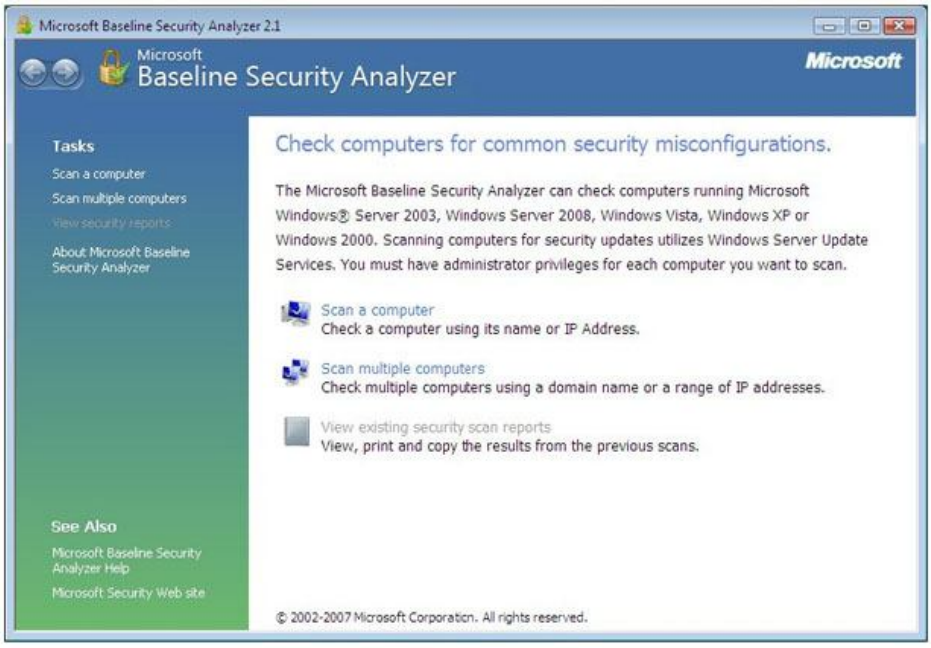


Рис. 1.27. Выбор проверяемого компьютера

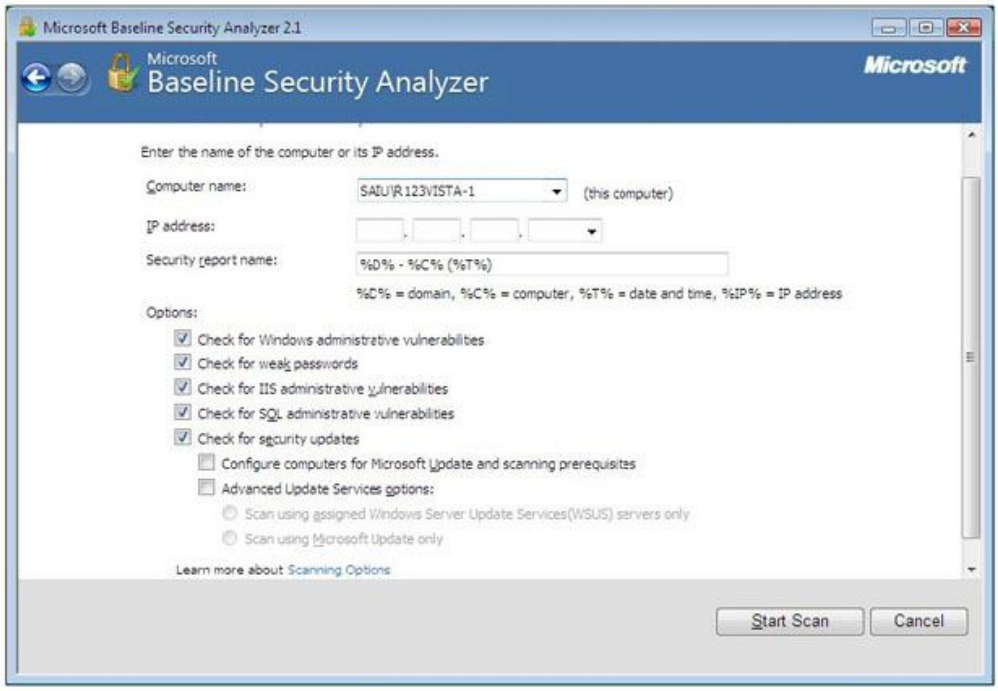


Рис. 1.28. Задание параметров проверки

Перед началом работы программа обращается на сервер Microsoft для получения перечня обновлений для ОС и известных уязвимостей. Если на момент проведения проверки компьютер не подключен к Интернет, база уязвимостей не будет обновлена, программа об этом сообщит и дальнейшие проверки выполняться не будут. В подобных случаях нужно отключать проверку обновлении безопасности (сбросив соответствующую галочку на экране рис. 1.28 или с помощью ключа при использовании утилиты командной строки, о чем речь пойдет ниже).

Для успешной проверки локальной системы необходимо, чтобы программа выполнялась от имени учетной записи с правами локального администратора. Иначе проверка не может быть проведена и о чем будет выдано сообщение: "You do not have sufficient permissions to perform this command. Make sure that you are running as the local administrator or have opened the command prompt using the 'Run as administrator' option".

По результатам сканирования формируется отчет, вначале которого дается общая оценка уровня безопасности конфигурации проверяемого компьютера. В приведенном на рис. 1.29 примере уровень риска оценивается как "серьезный" (Severe risk) [13].

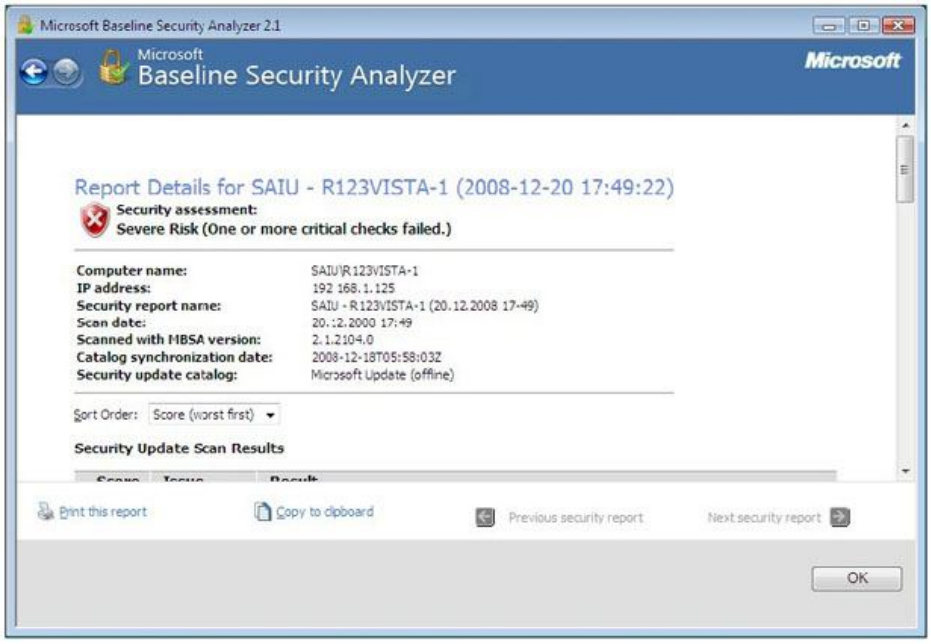


Рис. 1.29. Заголовок отчета

Далее приводится перечень обнаруженных уязвимостей, разбитый на группы: результаты проверки установки обновлений, результаты проверки Windows и т.д. Надо отметить, что выпускаемые Microsoft обновления бывают различных типов:

Security updates - собственно обновления безопасности, как правило, посвященные исправлению одной уязвимости программного продукта;

Update rollups - набор исправлений безопасности, который позволяет одновременно исправить несколько уязвимостей. Это упрощает обслуживание процесса обновления программного обеспечения (ПО);

Service packs - набор исправлений, как связанных, так и несвязанных с безопасностью. Установка Service pack, как правило, исправляет все уязвимости, обнаруженные с момента выхода предыдущего Service pack, таким образом устанавливать промежуточные обновления уже не надо.

[13] Там же.

В описании рассматриваемого результата проверки (рис. 1.30) можно выбрать ссылку **Result details** и получить более подробное описание найденных проблем данной группы. При наличии подключения к Интернет, перейдя по приводимой в отчете ссылке, можно получить информацию об отсутствующем обновлении безопасности и скачать его из сети.

Нужно отметить, что установка обновлений для систем с высокими требованиями в области непрерывности работы, требует предварительной тщательной проверки совместимости обновлений с использующимися приложениями. Подобная проверка обычно производится на тестовых системах с близкой конфигурацией ПО. В то же время, для небольших организаций и пользователей домашних компьютеров такая проверка зачастую неосуществима. Поэтому надо быть готовым к тому, чтобы восстановить систему после неудачного обновления. Для современных ОС семейства Windows это можно сделать, например, используя специальные режимы загрузки ОС - безопасный режим или режим загрузки последней удачной конфигурации.

Также надо отметить еще одну особенность. На данный момент **baseline security analyzer** не существует в локализованной русскоязычной версии. И содержащиеся там ссылки на пакеты обновлений могут указывать на иные языковые версии, что может создать проблемы при обновлении локализованных продуктов.

Аналогичным образом проводится работа по анализу других групп уязвимостей (рис. 1.31). Описывается уязвимость, указывается ее уровень критичности, даются рекомендации по исправлению. На рис. 1.32 представлено подробное описание результатов (ссылка **result details**) проверки паролей. Указывается, что 3 учетные записи имеют пароли, неограниченные по сроку действия [14].

[14] Там же.

Рис. 1.30. Перечень неустановленных обновлений (по группам)

Рис. 1.31. Уязвимости, связанные с администрированием операционной системы

Кроме версии программы с графическим интерфейсом, существует также утилита с интерфейсом командной строки. Называется она mbsacli.exe и находится в том же каталоге, куда устанавливался Baseline security analyzer, например, **"C:\Program Files\Microsoft Baseline Security Analyzer 2"**. У утилиты есть достаточно много ключей, получить информацию, о которых можно запустив ее с ключом **"/?"**.

Рис. 1.32 Результаты проверки паролей

Запуск без ключей приведет к сканированию локального компьютера с выводом результатов на консоль. Чтобы сохранить результаты сканирования, можно перенаправить вывод в какой-либо файл. Например: mbsacli > mylog.txt. Следует еще раз обратить внимание на то, что при настройках по умолчанию сначала утилита обращается на сайт Майкрософт за информацией об обновлениях. Если соединение с Интернет отсутствует, то утилиту надо запускать или с ключом /nd (указание "не надо скачивать файлы с сайта Майкрософт") или с ключом /n Updates (указание "не надо проводить проверку обновлений").

Запуск с ключом /xmlout приводит к запуску утилиты в режиме проверки обновлений (т.е. проверка на уязвимости, явившиеся результатом неудачного администрирования, проводиться не будет), при этом, отчет формируется в формате xml. Например:

```
mbsacli /xmlout > c:\myxmlog.xml
```

Локальная политика паролей

Рассмотрим, какие настройки необходимо сделать, чтобы пароли пользователей компьютера были достаточно надежны. В теоретической части курса мы рассматривали рекомендации по администрированию парольной системы. Потребовать их выполнения можно с помощью политики безопасности. Настройка делается через **Панель управления Windows**.

Откройте **Панель управления** → **Администрирование** → **Локальная политика безопасности**. Выберите в списке **Политика учетных записей** и **Политика паролей**. Для

Windows Vista экран консоли управления будет выглядеть так, как представлено на рис. 1.33.

Значения выбранного параметра можно изменить (рис. 1.34).

Надо понимать, что не все требования политики паролей автоматически подействуют в отношении всех учетных записей. Например, если в свойствах учетной записи стоит "Срок действия пароля не ограничен", установленное политикой требование максимального срока действия пароля будет игнорироваться. Для обычной пользовательской учетной записи, эту настройку лучше не устанавливать. Но в некоторых случаях она рекомендуется. Например, если в учебном классе нужна "групповая" учетная запись, параметры которой известны всем студентам, лучше поставить для нее **"Срок действия пароля не ограничен"** и **"Запретить смену пароля пользователем"**.

Свойства учетной записи можно посмотреть в **Панель управления** → **Администрирование** → **Управление компьютером**, там выберите **Локальные пользователи и группы** и **Пользователи** (или запустив эту же оснастку через **Пуск** → **Выполнить** → **lusrmgr.msc**).

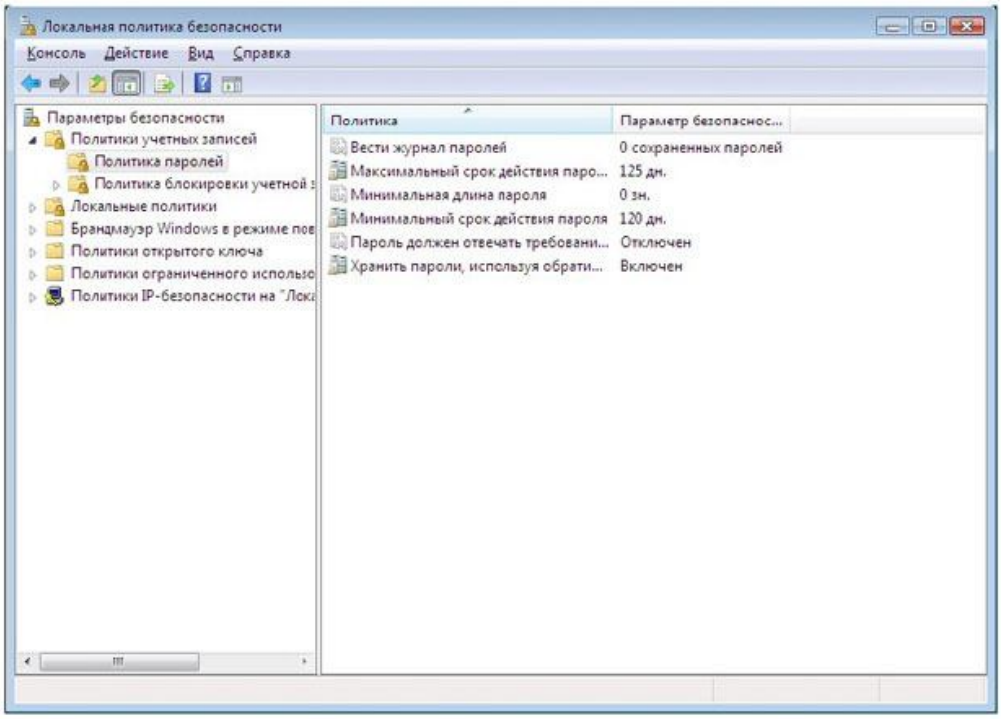


Рис. 1.33. Настройка политики паролей

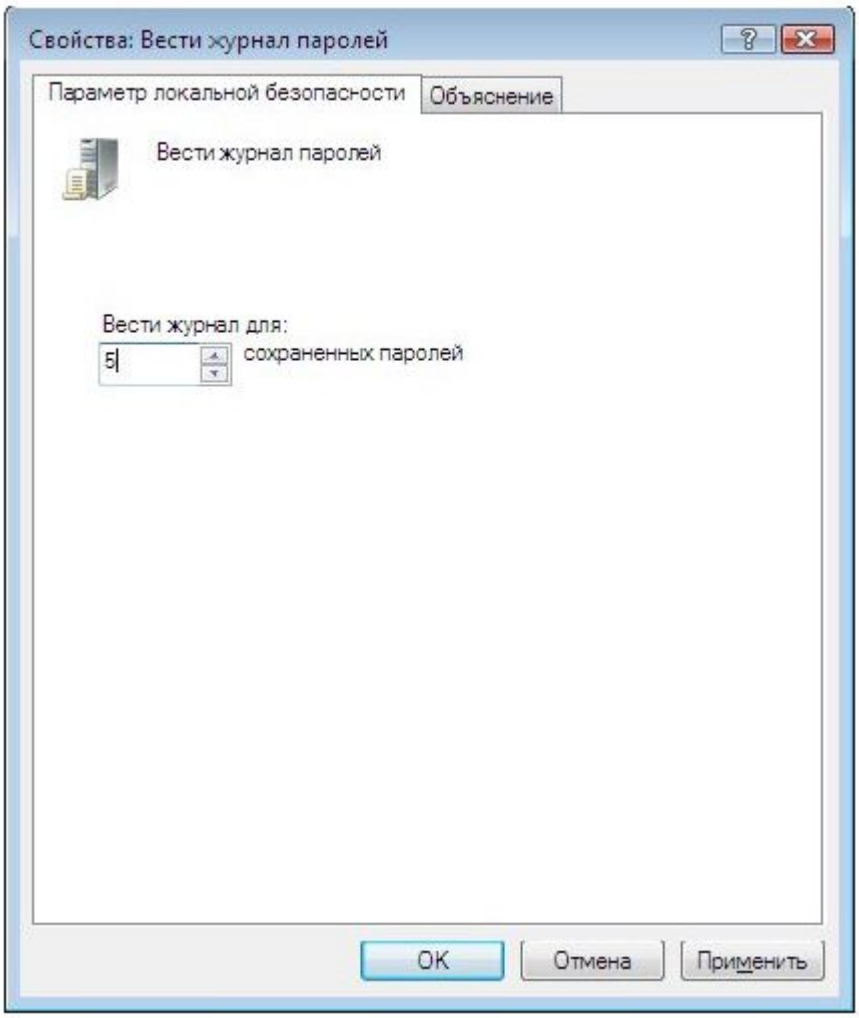


Рис. 1.34. Установка требования ведения журнала паролей

Задание к практической работе

1. Выполните проверку Вашего компьютера с помощью Microsoft Baseline security analyzer. В отчете о выполнении лабораторной работы необходимо указать следующее:
   - ✓ как оценен уровень уязвимости Вашего компьютера;
   - ✓ какие проверки проводились, в какой области обнаружено наибольшее количество уязвимостей;
   - ✓ опишите наиболее серьезные уязвимости каждого типа, выявленные на Вашем компьютере.
2. Проведите анализ результатов - какие уязвимости можно устранить, какие - нельзя из-за особенностей конфигурации ПО или использования компьютера.
3. Выполните удаленную проверку соседнего компьютера из сети лаборатории. Опишите наиболее серьезные уязвимости.
4. Выполните проверку нескольких компьютеров с помощью утилиты mbsacli. Для этого, предварительно создайте текстовый файл с перечнем имен компьютеров или

ip-адресов и запускайте mbsacli с ключом /listfile, после которого указывается имя файла с перечнем компьютеров. В результате Вы получите сообщение примерно следующего содержания:

2. Computer Name, IP Address, Assessment, Report Name
3. ----------

HOME\MYNBOOK, 127.0.0.1, Severe Risk, HOME - MYNBOOK (06.12.2008 13-51)

Для того, чтобы увидеть подробные результаты проверки, надо повторно запустить mbsacli с ключом /ld, после которого указывается имя отчета. Вывод можно перенаправить в текстовый файл для дальнейшей обработки. Например:

mbsacli /ld "HOME - MYNBOOK (06.12.2008 13-51)" > c:\test\report1.txt

После выполнения задания проанализируйте результаты, кратко опишите их в отчете по лабораторной работе.

1. Опишите действующую на вашем компьютере политику паролей.
2. Измените ее в соответствии с рассмотренными в теоретической части курса рекомендациями по администрированию парольной системы.
3. Если в ходе проверки утилитой bsa были выявлены уязвимости связанные с управлением паролями пользователей, опишите пути их устранения или обоснуйте необходимость использования действующих настроек.

Контрольные вопросы

1. Что подразумевается под термином «Уязвимость операционной системы»?
2. В чем состоит основное отличие терминов «уязвимость» и «открытость»?
3. Приведите несколько примеров наиболее известных в мире последствий использования хакерами уязвимостей ОС?
4. Какие меры применяются для устранения уязвимостей ОС?
5. Что включает в себя локальная политика паролей?
6. Для чего необходимо владеть информацией о локальной политике паролей предприятия?

Практическое занятие № 8

Тема «Исследование надежности системы идентификации пользователя»

Цель занятия: изучение порядка выбора и хранения паролей, изучение порядка передачи паролей по сети, формирование навыков создания защищенных каталогов паролей.

Оборудование к занятию: компьютеры с операционной системой Windows, программное обеспечение - криптографическая программа PGP (Pretty Good Privacy).

Теоретическая часть

PGP – это криптографическая (шифровальная) программа с высокой степенью надежности, которая позволяет пользователям обмениваться информацией в электронном виде в режиме полной конфиденциальности[15].

Главное преимущество этой программы состоит в том, что для обмена зашифрованными сообщениями пользователям нет необходимости передавать друг другу тайные ключи т.к. эта программа построена на новом принципе работы – публичной криптографии или обмене открытыми (публичными) ключами, где пользователи могут открыто посылать друг другу свои публичные ключи с помощью сети Интернет и при этом не беспокоиться о возможности несанкционированного доступа каких-либо третьих лиц к их конфиденциальным сообщениям.

В PGP применяется принцип использования двух взаимосвязанных ключей: открытого и закрытого. К закрытому ключу имеете доступ только вы, а свой открытый ключ вы распространяете среди своих корреспондентов.

Великолепное преимущество этой программы состоит также в том, что она бесплатная и любой пользователь, имеющий доступ к Интернету, может ее «скачать» на свой компьютер в течение получаса. PGP шифрует сообщение таким образом, что никто кроме получателя сообщения, не может ее расшифровать. Создатель PGP Филипп Циммерман открыто опубликовал код программы, который неоднократно был исследован специалистами крипто-аналитиками высочайшего класса и ни один из них не нашел в программе каких-либо слабых мест.

Электронные сообщения, в том виде и формате, который существует на сегодняшний день, легко могут быть прочитаны и архивированы любым человеком, имеющим доступ к серверу Интернет провайдера. В настоящий момент спецслужбам проще и дешевле подключиться к электронным адресам большого количества лиц, нежели к телефонным разговорам. Здесь вообще ничего делать не надо. Все сделает компьютер. Агенту спецслужбы или другому заинтересованному человеку остается только сесть за компьютер и просмотреть все ваши сообщения. Научно-технический прогресс облегчил задачу таким людям, однако, этот же самый прогресс предоставил возможность пользователям сети Интернет скрыть свои сообщения от третьих лиц таким образом, что даже суперкомпьютер стоимостью несколько десятков миллионов долларов не способен их расшифровать.

Принцип работы PGP

[15] Установка и применение программы PGP. URL: http://www.gloffs.com/pgp.htm. Дата обращения 10.06.2012 г.

Когда пользователь шифрует сообщение с помощью PGP, то программа сначала сжимает текст, что сокращает время на отправку сообщения через модем и увеличивает надежность шифрования. Большинство приемов криптоанализа (взлома зашифрованных сообщений) основаны на исследовании «рисунков», присущих текстовым файлам, что помогает взломать ключ. Сжатие ликвидирует эти «рисунки» и таким образом повышает надежность зашифрованного сообщения. Затем PGP генерирует сессионный ключ, который представляет собой случайное число, созданное за счет движений вашей мышки и нажатий на клавиши клавиатуры.

Как только данные будут зашифрованы, сессионный ключ зашифровывается с помощью публичного ключа получателя сообщения, который отправляется к получателю вместе с зашифрованным текстом.

Расшифровка происходит в обратной последовательности. Программа PGP получателя сообщения использует закрытый ключ получателя для извлечения временного сессионного ключа, с помощью которого программа затем дешифрует зашифрованный текст.

Существует ряд требований к выбору паролей в зависимости от степени важности информации, которую защищает пароль. Указанные требования представлены в таблице 1.5. Для оценки стойкости парольных систем имеется набор определенных параметров (см. таблицу 1.6).

Таблица 1.5. Требования к выбору и использованию паролей

Требования к выбору пароля	**Получаемый эффект**
Установление максимальной длины пароля	Усложняет задачу злоумышленнику при попытке подсмотреть пароль или подобрать пароль методом «тотального опробования»
Использование в пароле различных групп символов	Усложняет задачу злоумышленнику при попытке подобрать пароль методом «тотального опробования»
Проверка и отбраковка пароля по словарю	Усложняет задачу злоумышленнику при попытке подобрать пароль по словарю
Установление максимального срока действия пароля	Усложняет задачу злоумышленнику при попытке подобрать пароль методом «тотального опробования», в том числе без непосредственного обращения к системе зашиты (режим off-line)
Установление минимального срока действия пароля	Препятствует попыткам пользователя заменить пароль на старый после его смены по предыдущему требованию
Введение журнала истории паролей	Обеспечивает дополнительную степень защиты по предыдущему требованию
Применение эвристического алгоритма,	Усложняет задачу злоумышленнику при

бракующего пароли на основании данных журнала истории	попытке подобрать пароль по словарю или с использованием эвристического алгоритма
Ограничение числа попыток ввода пароля	Препятствует интерактивному подбору паролей злоумышленником
Поддержка режима принудительной смены пароля пользователя	Обеспечивает эффективность требования, ограничивающего максимальный срок действия пароля
Использование задержки при вводе неправильного пароля	Препятствует интерактивному подбору паролей злоумышленником
Запрет на выбор пароля самим пользователем и автоматическая генерация паролей	Исключает возможность подобрать пароль по словарю. Если алгоритм генерации известен злоумышленнику, последний может подбирать пароли только методом «тотального опробования»
Принудительная смена пароля при первой регистрации пользователя в системе	Защищает от неправомерных действий системного администратора, имеющего доступ к паролю в момент создания учетной записи

Таблица 1.6. – Количественная оценка стойкости парольных систем

Параметр	Способ определения
Мощность алфавита паролей A Длина пароля L	Могут варьироваться для обеспечения заданного значения S(S=AL)
Мощность пространства паролей S	Вычисляется на основе заданных значений P, T или V
Скорость подбора паролей V: 1.Для интерактивного режима определяется как скорость обработки одной попытки регистрации проверяющей стороной. 2.Для режима off-line (на основе свертки пароля) определяется как скорость вычисления значения свертки для одного пробного пароля	Может быть искусственно увеличена для защиты от данной угрозы. Задается используемым алгоритмом вычисления свертки. Алгоритм, имеющий медленные реализации, повышает стойкость по отношению к данной угрозе.
Срок действия пароля (задает промежуток времени, по истечении которого пароль должен быть обязательно сменен) T	Определяется исходя из заданной вероятности P, или полагается заданным для дальнейшего определения S.
Вероятность подбора пароля в течение срока его действия (подбор продолжается непрерывно в течение всего срока действия пароля) P	Выбирается заранее для дальнейшего определения S или T

В качестве иллюстрации к таблицам 1.4. и 1.5. рассмотрим задачу на определение минимальной мощности пространства паролей (зависящей от параметров *A* и *L)* в соответствии с заданной вероятностью подбора пароля в течение его срока действия.

Пример. Задана вероятность $P=10^{-6}$. Необходимо найти минимальную длину пароля, которая обеспечит его стойкость в течение одной недели непрерывных попыток подобрать пароль.

Пусть скорость интерактивного подбора паролей V=10 паролей/мин. Тогда в течение недели можно перебрать 10*60*24*7= 100800 паролей. Далее, учитывая, что параметры S, *V, T* и P связаны соотношением P $P=V*T/S$, получаем: $S=100*800/10^{-6} = 1{,}008 * 10^{11}=10^{11}$. Полученному значению S соответствуют пары: $A=26$, L= 8 и $A=36$, L= 6.

Задание на практическую работу:

1) На основании рассмотренного примера решить задачу с другими условиями, определенными преподавателем.

2) Создать защищенный каталог из 10 и более паролей (выбирается произвольно) с использованием программы PGP и представить его преподавателю для проверки.

3) **Творческое задание**: описать возможные способы применения созданного защищенного каталога.

Контрольные вопросы:

1) Каким образом найти минимальную длину пароля, зная вероятность подбора пароля и срок действия?
2) Каков принцип работы программы Pretty Good Privacy?
3) Принцип использования, каких двух ключей применяется в PGP?
4) Каким образом происходит расшифровка сообщения в программе PGP?
5) К какому эффекту приведет установление минимального срока действия пароля?
6) От какой действия возникает эффект защиты от неправомерных действий системного администратора, имеющего доступ к паролю в момент создания учетной записи?
7) Перечислите количественные оценка стойкости парольных систем.

Практическое занятие № 9

Тема «Средства защиты и удостоверения подлинности электронных документов»

Цель занятия: изучить и практически освоить стандартные средства, обеспечивающие защиту и контроль подлинности офисных документов и их фрагментов.

Оборудование к занятию: компьютеры с операционной системой Windows, офисными пакетами MS Word и MS Excel.

Форма проведения занятия: индивидуальное выполнение.

Теоретическая часть

Зачастую при решении повседневных дел приходится сталкиваться с большим количеством электронных документов. Различные анкеты, договора, бланки, запросы оформляются средствами известных офисных пакетов. Вопрос получения вами или вашим адресатом нужного документа в неизменном виде всегда очень важен. Компания Microsft, предусмотрела в линейке своих офисных пакетов несколько вариантов защиты от

несанкционированного доступа к тесту документа. Версии MS Office от 2003 и выше содержат следующие возможности по защите электронных документов:

- Опечатывание документа с помощью цифрового сертификата;
- Запрос пароля при открытии или изменении документа;
- Рекомендация доступа только для чтения;
- Защита полей электронной формы от случайного изменения;
- Разрешить только добавление примечаний и записей исправления;
- Защита форматирования.

Задание к практической работе

ЗАДАНИЕ 1

1. Ознакомиться более подробно со способами защиты документа (представленными в теоретической части) от несанкционированных изменений на сайте компании Microsoft [16];

2. Создайте новый документ Word и сохраните его в личной папке.

3. Используя команды ***Сервис → Параметры страниц*** →…, задайте поля документа Word: книжная ориентация; левое и правое поле – 2 см, верхнее и нижнее поле – 2, 5 см; установите флажок ***Различать колонтитулы первой страницы***.

4. В поле верхнего колонтитула первой страницы, используя команды ***Вид → Колонтитулы*** и кнопки появившейся панели ***Колонтитулы***, введите: слева – свою фамилию и инициалы, справа – текущую дату. В поле нижнего колонтитула по центру вставьте номер страницы.

5. Стилем Заголовок 1 наберите в документе заголовок:

Защита текстового документа и его фрагментов

6. Стилем Заголовок 2 наберите текст:

Опечатывание документа с помощью цифрового сертификата

7. Стилем Обычный наберите текст из справки с сайта компании Microsoft посвященный тематике заголовка.

8. Перейдите к новому абзацу и вставьте в документ Word новый раздел, выполнив команды: **Вставка → Разрыв…→ Переключатель Новый раздел со следующей страницы** → ОК

8. Аналогично выполните действия п. 4-6 для всех шести видов защиты электронного документа в Word.

---

[16] Защита документа от несанкционированных изменений [Электронный ресурс]. Режим доступа: http://office.microsoft.com/ru-ru/word-help/HP001044674.aspx (Дата обращения 18.06.2012 г.)

9. Используя справочную систему Word (Помощника), найдите пояснения терминов Цифровые подписи и Сертификаты, а также другую связанную с этими терминами информацию[17]

10. Скопируйте из найденных справочных сведений в документ Word определения цифровой подписи и цифрового сертификата и выполните их форматирование.

Пример скопированного из справки текста:

Цифровая подпись - шифрованная электронная подпись, подтверждающая подлинность макроса или документа. Наличие цифровой подписи подтверждает, что макрос или документ был получен от владельца подписи и не был изменен.

Цифровой сертификат - вложение в файл, проект макроса или сообщение электронной почты, подтверждающее его подлинность, обеспечивающее шифрование или предоставляющее поддающуюся проверке подпись.

Цифровую подпись можно создать с помощью программы **Selfcert.exe**.

11. Для создания цифрового сертификата, используя поисковую систему Windows, найдите файл **Selfcert.exe** и выполните его, сделав по нему два щелчка левой кнопкой мыши.

12. В появившемся окне программы **Selfcert.exe** (см. рис. 1.35) введите имя создаваемого Вами сертификата (на рис. 1.35 введено имя Юристы) и нажмите кнопку ОК.

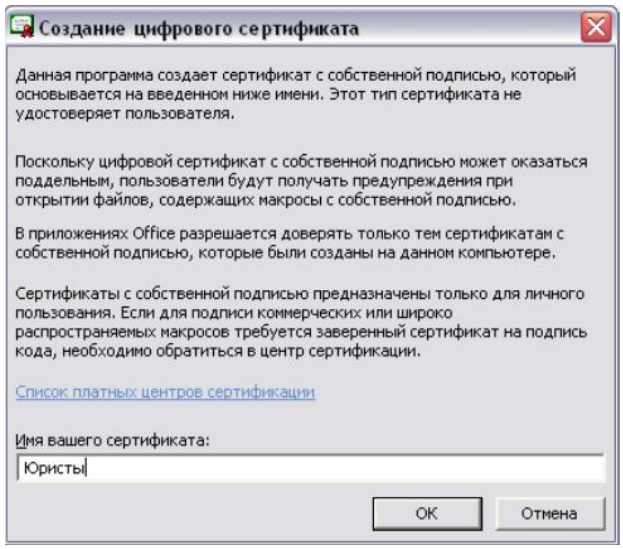


Рис. 1.35. Пример создания цифрового сертификата

13. Выполните защиту первого раздела документа, введя команды:

Команда Сервис → Установить защиту…→

[17] ЛКМ по Помощнику → Ввести текст Цифровые подписи → Кнопка Найти → Раскрыть гиперссылку О цифровых подписях → В тексте справки раскрыть гиперссылку Показать все

Переключатель Запретить любые изменения, кроме: Ввода данных в поля формы → Кнопка Разделы…→ Снять флажки незащищаемых разделов → ОК → Ввести пароль → Подтвердить пароль → ОК

14. Для задания пароля на открытие файла выполнить команды:

Сервис → Параметры… → Вкладка Безопасность →Задать пароль на открытие файла →

Кнопка ОК → Подтвердить пароль → ОК

15. Для добавления цифровой подписи к документу выполнить команды:

Сервис → Параметры… → Вкладка Безопасность → Кнопка Цифровые подписи → Кнопка Добавить… → Сохранить документ Word → Выбрать сертификат → Посмотреть параметры сертификата → ОК→ ОК→ ОК→ ОК

16. Закройте документ Word (уже без сохранения, так как при сохранении цифровая подпись удаляется!).

ЗАДАНИЕ 2

1. Создайте новый документ Excel и подготовьте электронную ведомость по указанному образцу (рис. 1.34).

	A	B	C	D	E	F	G
1	Электронная ведомость						
2	№№ п.п.	ФИО	Баллы			Сумма баллов	Отметка о зачете
3			Аттестация	Работа в семестре	Зачет		
4	1	2	3	4	5	6	7
5	1	Антонова И.	12	15	60	87	Зачтено
6	2	Борисов В.	18	16	12	46	Не зачтено
7	3	Васильев А.	16	17	24	57	Зачтено
8	4	Григорьева М.	8	18	23	49	Не зачтено
9	5	Яковлева Н.	2	10	40	52	Зачтено
10							

Рис. 1.34. Пример создания фрагмента электронной таблицы

Введите данные в ячейки «шапки» таблицы, выполните необходимое форматирование и объединение ячеек.

В графу 2 (ФИО) введите 5-7 произвольных фамилий.

В графы 3 (Аттестация) и 4 (Работа в семестре) введите произвольные баллы от 0 до 20.

В графу 6 (Сумма баллов) введите формулу, вычисляющую сумму баллов в графах 3, 4 и 5.

В графу 7 введите с помощью встроенной функции ЕСЛИ формулу, формирующую текст «Зачтено», если значение соответствующего поля графы 6 превышает 50, и текст «Не зачтено» в противном случае.

2. Для диапазона данных графы 5 (в примере E5:E9) выполните операции:

Выделить ячейки диапазона данных → Команда Формат → Ячейки… → Вкладка Защита → Снять флажок Защищаемая ячейка → ОК

3. Выполните защиту документа (листа электронной таблицы):

Команда Сервис → Защита → Защитить лист… → Установить флажок Защитить листы в отношении содержимого (Защитить лист и содержимое защищаемых ячеек) → Ввести пароль для отключения защиты листа → Подтвердить пароль → ОК

4. Введите данные зачета – баллы от 0 до 60. Проверьте, как меняются значения граф 6 и 7.

5. В случае ошибок (некорректных результатов, неправильного форматирования таблицы), снимите защиту:

Команда Сервис → Защита → Снять защиту → Ввести пароль → ОК

6. Устраните ошибки, а затем снова установите защиту.

7. Сохраните документ Excel в своей личной папке.

8. Подпишите документ Excel цифровой подписью с использованием ранее созданного Вами цифрового сертификата и закройте его окно.

9. Откройте подписанные документы Word и Excel. Посмотрите возможности работы с данными документами (открытие файла Word, ввода и изменения данных в его разделы; открытие файла Excel и ввода данных в ячейки документа).

Контрольные вопросы

1. Что такое цифровая подпись электронного документа?
2. Что такое цифровой сертификат?
3. Какую опасность, и при каких условиях, могут содержать документы Excel?
4. Какие способы защиты документа вы знаете?
5. Каким образом можно защитить документ при помощи пароля?
6. Каким образом можно создать анкету для опроса сотрудников, чтобы они могли вносить данные в строго определенные поля и никуда больше?

Практическое занятие № 10

Тема «Использование технологий виртуализации для обеспечения безопасности»

Цель занятия: изучить и практически освоить стандартные средства, обеспечивающие защиту и контроль подлинности офисных документов и их фрагментов.

Оборудование к занятию: компьютеры с операционной системой Windows, офисными пакетами MS Word и MS Excel.

Форма проведения занятия: индивидуальное выполнение.

Теоретическая часть

Антивирусная защита и защита сетевых портов позволяют значительно повысить безопасность компьютера. Однако существуют угрозы, которые могут обойти эти меры безопасности. Например, работа с Интернет сайтами, содержащими JavaScript код, может привести к заражению компьютера посредством уязвимости используемого браузера, тестовая установка нового программного обеспечения на рабочей системе может привести к установке троянских программ вместе с интересующим ПО.

Приведенные ситуации это лишь несколько примеров действий, которые не желательно проводить на своей рабочей машине. Для того чтобы выполнить потенциально не безопасные действия существуют специальные механизмы.

Для запуска не протестированного кода или непроверенного кода из неизвестных источников, а также обнаружения вирусов используются так называемые песочницы (англ. sandbox). Песочница обычно предоставляет собой жёстко контролируемый набор ресурсов для исполнения гостевой программы - например, место на диске или в памяти. Доступ к сети, возможность сообщаться с главной операционной системой или считывать информацию с устройств ввода обычно либо частично эмулируют, либо сильно ограничивают. Песочницы представляют собой пример виртуализации. Повышенная безопасность исполнения кода в песочнице зачастую связана с большой нагрузкой на систему - именно поэтому некоторые виды песочниц используют только для неотлаженного или подозрительного кода.

Один из видов песочниц это виртуальные машины, программы полностью эмулирующие «стандартный» компьютер.

Виртуальная машина (англ. virtual machine) - программная или аппаратная среда, исполняющая некоторый код (например, байт-код, p-код или машинный код реального процессора). Зачастую виртуальная машина эмулирует работу реального компьютера. На виртуальную машину, также как и на реальный компьютер, можно устанавливать операционную систему, у виртуальной машины также есть BIOS, оперативная память, жёсткий диск (выделенное место на жёстком диске реального компьютера), могут эмулироваться периферийные устройства. На одном компьютере может функционировать несколько виртуальных машин. В настоящей работе виртуальная машина рассматривается в качестве песочницы. Следует отметить, что на этом применении возможности виртуальных машин не исчерпываются. Они могут быть использованы

- ✓ для исследования производительности ПО или новой компьютерной архитектуры;
- ✓ с целью оптимизации использования ресурсов мейнфреймов и прочих мощных компьютеров, в частности для организации виртуальных выделенных хостингов;

- ✓ для моделирования информационных систем с клиент-серверной архитектурой на одной ЭВМ (эмуляция компьютерной сети с помощью нескольких виртуальных машин).

На сегодня много решений для виртуализации, наиболее известные это бесплатные решения от компаний SUN – VirtualBOX и Microsoft – VirtualPC, промышленным стандартом еще несколько лет назад было решение от компании VMWare. Следует отметить, что виртуальная машина достаточно требовательна к системным ресурсам, для комфортного использования данной технологии желательно иметь многоядерный процессор (например, Intel Core2 Duo) и не менее 1ГБ оперативной памяти.

Виртуальная машина это эмуляция аппаратного обеспечения компьютера, на которое должна быть установлена операционная система. Операционная система, установленная в виртуальном аппаратном окружении называется гостевой операционной системой, тогда как основная операционная называется операционной системой хост-машины. Различные виртуальные машины работают на различных ОС и позволяют устанавливать различные гостевые ОС. Часто бывает, что гостевая ОС должна совпадать с основной ОС. Рассматриваемая нами среда VirtualBox может быть установлена на основных видах ОС – Windows, Linux/BSD и MacOS X и позволяет установить в качестве гостевой следующие ОС - DOS, OS/2, MS Windows, GNU/Linux, OpenBSD, FreeBSD, NetBSD, Netware. 5.2 Установка SUN Virtual Box +OpenSuse Linux

В настоящей работе рассмотрим установку виртуальной машины SUN VirtualBox. Сначала необходимо скачать и установить VirtualBox с официального сайта http://www.virtualbox.org/wiki/Downloads.

После установки запускаем VirtualBox, отказываемся от регистрации в Sun. При запуске откроется главное окно программы (рис. 1.35). Приступить к созданию образа гостевой ОС можно нажав кнопку «Создать». Созданный образ для дальнейшей работы будет доступен для запуска, настройки или удаления. При создании образа мы указываем основные параметры образа. Большинство из них доступны для дальнейшей корректировки после создания образа. В следующем окне необходимо выбрать тип ОС – в нашей работе мы рассмотрим установку Linux OpenSUSE 11.

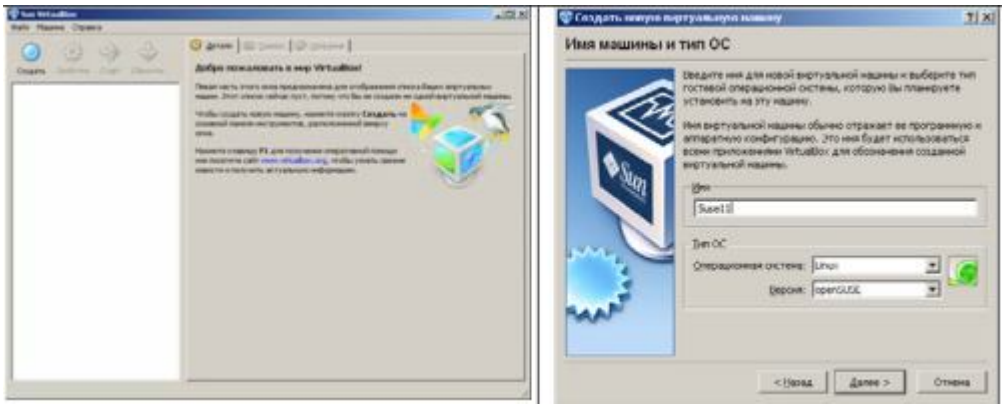


Рис. 1.35. Создание гостевой операционной системы.

Далее мы должны настроить объем ресурсов выделяемых под гостевую ОС. На рис. 1.36 показано выделение 300Мб ОЗУ под нужды виртуальной ОС.

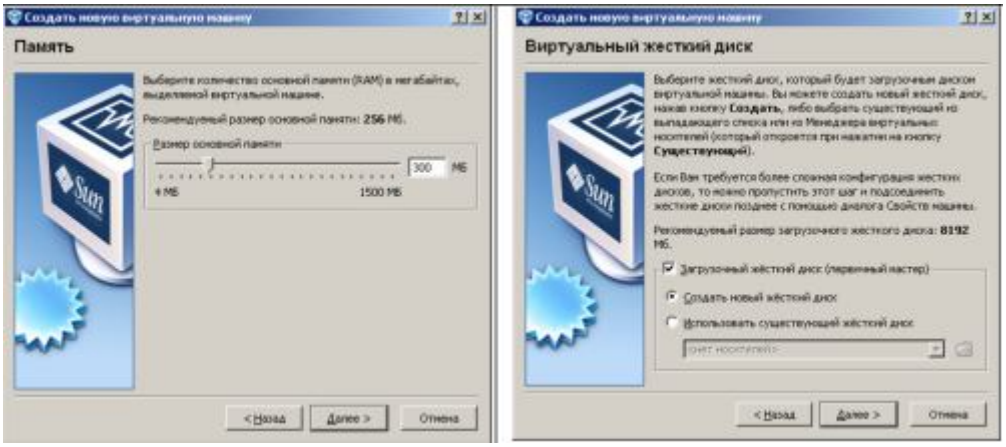


Рис. 1.36. Выделение ресурсов для гостевой операционной системы

Далее будет предложено создать виртуальный жесткий диск (располагающийся в файле-контейнере). Файл контейнер будет создан и размещен на жестком диске. Лучше выбрать динамически расширяемый образ – его размер на диске будет расти по мере необходимости.

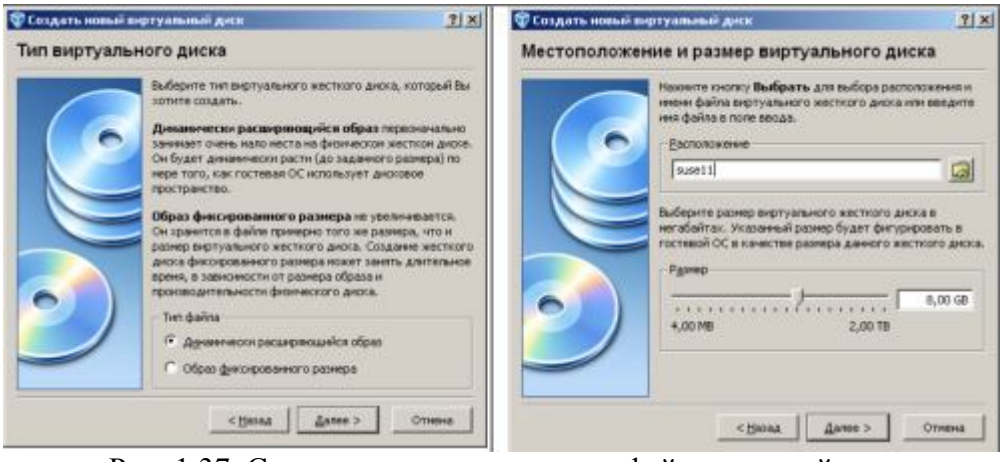


Рис. 1.37. Создание жесткого диска в файле – контейнере

После создания контейнера и виртуального жесткого диска, запустится мастер установки гостевой ОС. Будет предложено выбрать установочный носитель (рис. 1.38),

необходимо указать ISO образ предварительно полученный с сайта http://www.opensuse.org.

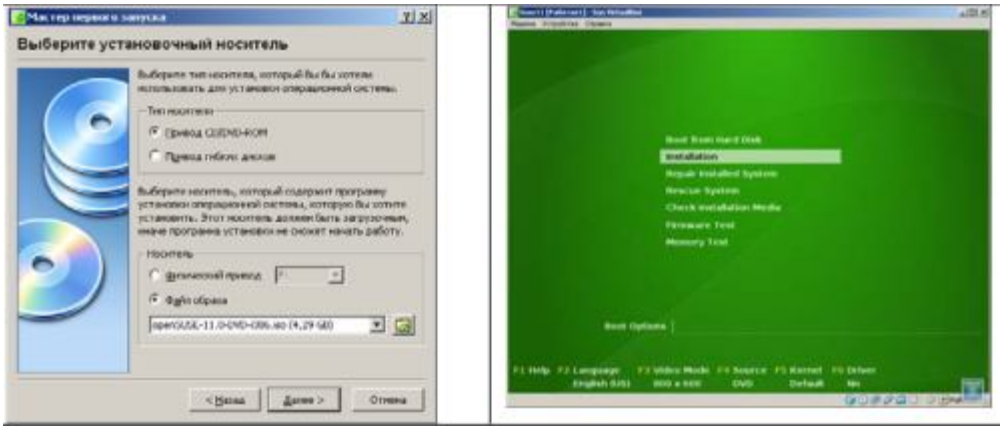


Рис. 1.38. Начало установки гостевой операционной системы

Далее произойдет процедура запуска виртуальной машины. Загрузка виртуальной машины будет проведена с установочного носителя, который был указан при старте.

Будет выдано приглашение инсталляции операционной системы OpenSuse 11. На экране начальной загрузки надо указать пункт Installation (рис. 1.38). В дальнейшем, при установке необходимо русский язык (Language), вместо английского (English), согласиться с лицензионным соглашением. Далее все сообщения установки будут на русском языке.

На экране выбора часового пояса необходимо указать ваше местонахождение. Далее на окне «Выбор рабочего стола» выбрать рабочий стол. Для настоящей работы мы остановимся на KDE 3.5. На этапе разметки диска нужно согласиться с предложенной разметкой. Далее мастер установки предложит создать пользователей и настроить порядок входа в систему. ***ВАЖНОЕ ЗАМЕЧАНИЕ***: *галочка, установленная напротив пункта «Использовать этот пароль для системного администратора» должна быть снята. Далее будет предложено задать пароль пользователя root, это важнейший пользователь в системе, он обладает всеми возможностями настройки системы, поэтому его пароль желательно хорошенько запомнить.* Далее произойдет перезагрузка и настройка первой системной конфигурации. При начале работы с виртуальной машиной появится информационное сообщение, предупреждающее о захвате указателя мыши виртуальной машиной (рис. 19). Захват происходит при щелчке мышью в области окна виртуальной машины. При таком захвате мышь двигается только внутри экрана гостевой ОС и взаимодействует с объектами гостевой ОС.

Для освобождения от захвата необходимо нажать хост клавишу. По умолчанию это правая клавиша ctrl. Другую хост-клавишу можно задать в настройках виртуальной машины.

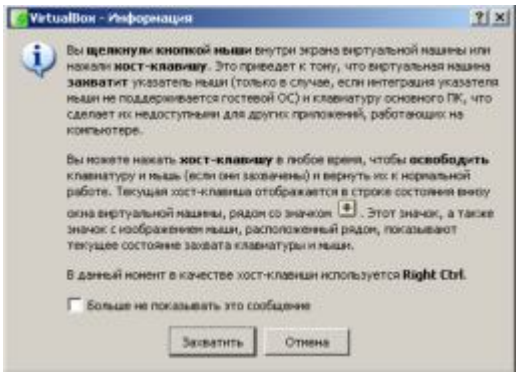


Рис. 1.39. Окно - предупреждение о захвате фокуса ввода

После завершения установки OpenSuse эта виртуальная система готова для использования. Использование виртуальной машины позволяет выполнять свободное пользование Интернет без угрозы для основной операционной системы. Эта система удобна для использования Linux в качестве второй ОС и постепенного перехода с Windows на Linux.

Установка Windows на виртуальную машину также возможно. Несмотря на то, что эта процедура в данной работе не рассматривается, она также может быть полезна. Перечислим лишь некоторые преимущества от использования Windows на виртуальной машине:

- ✓ возможность отката гостевой ОС к рабочему состоянию после любого сбоя;
- ✓ возможность использования любого ПО без риска заражения основной системы;
- ✓ проверка любых настроек ОС без риска потерять работоспособность системы.

Задания для практической работы

7. Установить на виртуальную машину VirtualBox OpenSuse Linux. Настроить, с использованием документации, обмен файлами между гостевой и основной ОС. Воспользоваться средствами гостевой ОС для выхода в Интернет и редактирования документов.
8. Отправить письмо на электронную почту соседям слева или справа, запустив браузер на виртуальной машине.

Контрольные вопросы

1. Что такое песочница и в чем преимущества ее использования?
2. Приводит ли использование виртуальной машины к потере производительности?
3. Какие операционные системы могут быть установлены в качестве гостевых?

4. Как использование виртуальной машины может повысить безопасность компьютера?
5. **Творческое задание**: описать возможности использования виртуальных машин в произвольной форме.

Практическое занятие № 11

Тема «Брандмауры и методы защиты компьютера от несанкционированного доступа»

Цель занятия: изучить принцип действия брандмауэра и обозревателя Internet Explorer как средств защиты от несанкционированного доступа и получить навык проведения анализа защищенности информационных ресурсов.

Оборудование для проведения занятия: компьютер с операционной системой Windows, наличие обозревателя Internet Explorer, возможность регулировать включение брандмаура Windows.

Теоретическая часть

Брандмауэр – сочетание программного и аппаратного обеспечения, образующее систему защиты от несанкционированного доступа из внешней глобальной сети во внутреннюю сеть (интрасеть). Брандмауэр предотвращает прямую связь между внутренней сетью и внешними компьютерами, пропуская сетевой трафик через прокси-сервер, находящийся снаружи сети. Прокси-сервер определяет, следует ли разрешить файлу попасть во внутреннюю сеть. Брандмауэр называется также шлюзом безопасности[18].

Можно считать брандмауэр пограничным постом, на котором проверяется информация (часто называемая трафик), приходящая из Интернета или локальной сети. В ходе этой проверки брандмауэр отклоняет или пропускает информацию на компьютер в соответствии с установленными параметрами.

Когда к компьютеру пытается подключиться кто-то из Интернета или локальной сети, такие попытки называют «непредусмотренными запросами». Когда на компьютер поступает непредусмотренный запрос, брандмауэр Windows блокирует подключение. Если на компьютере используются такие программы, как программа передачи мгновенных сообщений или сетевые игры, которым требуется принимать информацию из Интернета или локальной сети, брандмауэр запрашивает пользователя о блокировании или разрешении подключения. Если пользователь разрешает подключение, брандмауэр

[18] *Системы автоматизированного расчёта в управлении качеством и при защите информации: лабораторные работы / сост.: П.В. Балабанов, С.В. Пономарёв. – Тамбов : Изд-во Тамб. гос. техн. ун-та, 2009. – 32 с. URL: http://www.234555.ru/publ/12-1-0-408 (Режим доступа свободный).*

Windows создает исключение, чтобы в будущем не тревожить пользователя запросами по поводу поступления информации для этой программы [19].

Если идёт обмен мгновенными сообщениями с собеседником, который собирается прислать файл (например, фотографию), брандмауэр Windows запросит подтверждение о снятии блокировки подключения и разрешении передачи фотографии на компьютер. А при желании участвовать в сетевой игре через Интернет с друзьями пользователь может добавить эту игру как исключение, чтобы брандмауэр пропускал игровую информацию на компьютер. Хотя имеется возможность отключать брандмауэр Windows для отдельных подключений к Интернету или локальной сети, это повышает вероятность нарушения безопасности компьютера.

Чтобы открыть компонент «Брандмауэр Windows», нажмите кнопку Пуск, выберите пункты Настройка, Панель управления, Сеть и подключения к Интернету и Брандмауэр Windows.

В обозревателе Internet Explorer имеется несколько возможностей, позволяющих обеспечить защиту конфиденциальности, а также повысить безопасность личных данных пользователя. Параметры конфиденциальности позволяют защитить личные данные пользователя — с помощью этих параметров можно понять, как просматриваемые веб-узлы используют эти данные, а также задать значения параметров конфиденциальности, которые будут определять, разрешено ли веб-узлам сохранять файлы «cookie» на компьютере.

В число параметров конфиденциальности Internet Explorer входят следующие:

- ✓ Параметры конфиденциальности, определяющие обработку на компьютере файлов «cookie».
- ✓ Файлы «cookie» — это созданные веб-узлом объекты, которые сохраняют на компьютере определенные сведения, например о предпочтениях пользователя при посещении данного узла. Кроме того, эти файлы могут также сохранять личные данные пользователя, такие как имя и адрес электронной почты.
- ✓ Оповещение безопасности, выдаваемые пользователю при попытке получить доступ к веб-узлу,не соответствующему заданным параметрам конфиденциальности.
- ✓ Возможность просмотра политики конфиденциальности P3P для веб-узла.

Средства безопасности позволяют предотвратить доступ других пользователей к таким сведениям, на доступ к которым у них нет разрешения. Это, например, сведения о кредитной карточке, вводимые при покупках в Интернете. Эти средства безопасности могут также защитить компьютер от небезопасного программного обеспечения.

[19] *Межсетевой экран. URL: http://ru.wikipedia.org/wiki (Режим доступа: свободный)*

В число параметров безопасности Internet Explorer входят следующие.

- ✓ Возможность блокирования большинства всплывающих окон.
- ✓ Возможность обновления, отключения или повторного включения надстроек для веб-обозревателя.
- ✓ Средства повышения безопасности, предупреждающие пользователя о попытке веб-узла загрузить файлы или программы на компьютер.
- ✓ Цифровые подписи, которые подтверждают, что файл поступил действительно от указанного лица или издателя и с момента включения цифровой подписи в этот файл никем не внесены изменения.
- ✓ Безопасное подключение с использованием 128-разрядного ключа, которое применяется для связи с безопасными веб-узлами.

Поиск уязвимостей в системе защиты

Противостояние атакам – важное свойство защиты. Казалось бы, если в сети установлен межсетевой экран (firewall), то безопасность гарантирована, но это распространенное заблуждение может привести к серьёзным последствиям.

Например, межсетевой экран (МЭ) не способен защитить от пользователей, прошедших аутентификацию. А квалифицированному хакеру не составляет труда украсть идентификатор и пароль авторизованного пользователя. Кроме того, межсетевой экран не только не защищает от проникновения в сеть через модем или иные удалённые точки доступа, но и не может обнаружить такого злоумышленника.

При этом система защиты, созданная на основе модели адаптивного управления безопасностью сети (Adaptive Network Security, ANS), способна решить все или почти все перечисленные проблемы. Она позволяет обнаруживать атаки и реагировать на них в режиме реального времени, используя правильно спроектированные, хорошо управляемые процессы и средства защиты.

Компания Yankee Group опубликовала в июне 1998 г. отчёт, содержащий описание процесса обеспечения адаптивной безопасности сети. Этот процесс должен включать в себя анализ защищённости, т.е. поиск уязвимостей, обнаружение атак, а также использовать адаптивный (настраиваемый) компонент, расширяющий возможности двух первых функций, и управляющий компонент.

Анализ защищённости осуществляется на основе поиска уязвимых мест во всей сети, состоящей из соединений, узлов (например, коммуникационного оборудования), хостов, рабочих станций, приложений и баз данных. Эти элементы нуждаются как в оценке эффективности их защиты, так и в поиске в них неизвестных уязвимостей. Процесс анализа защищённости предполагает исследование сети для выявления в ней слабых мест

и обобщение полученных сведений, в том числе в виде отчёта. Если система, реализующая данную технологию, содержит адаптивный компонент, то устранение найденной уязвимости будет осуществляться автоматически. При анализе защищённости обычно идентифицируются:

- ✓ люки в системах (back door) и программы типа «троянский конь»;
- ✓ слабые пароли;
- ✓ восприимчивость к проникновению из внешних систем и к атакам типа «отказ в обслуживании»;
- ✓ отсутствие необходимых обновлений (parch, hotfix) операционных систем;
- ✓ неправильная настройка межсетевых экранов, WEB-серверов *и баз данных.*

Обнаружение атак – это процесс оценки подозрительных действий в корпоративной сети, реализуемый посредством анализа журналов регистрации операционной системы и приложения (log-файлов)либо сетевого трафика. Компоненты ПО обнаружения атак размещаются на узлах или в сегментах сети и оценивают различные операции, в том числе с учётом известных уязвимостей. Адаптивный компонент ANS позволяет модифицировать процесс анализа защищенности, предоставляя самую последнюю информацию о новых уязвимостях. Он также модифицирует компонент обнаружения атак, дополняя его последней информацией о подозрительных действиях и атаках. Примером адаптивного компонента может служить механизм обновления баз данных антивирусных программ, которые являются частным случаем систем обнаружения атак.

Управляющий компонент предназначен для анализа тенденций, связанных с формированием системы защиты организации и генерацией отчётов. К сожалению, эффективно реализовать все описанные технологии в одной системе пока не удаётся, поэтому пользователям приходится применять совокупность систем защиты, объединённых единой концепцией безопасности. Пример таких систем – семейство продуктов SAFEsuite, разработанных американской компанией Internet Security Systems (ISS). В настоящее время комплект ПО SAFEsuite поставляется в новой версии SAFEsuite Enterprise, в которую входит также ПО SAFEsuite Decisions, обеспечивающее принятие решений по проблемам безопасности.

Система анализа защищённости Internet Scanner предназначена для проведения регулярных всесторонних или выборочных тестов сетевых служб, операционных систем, используемого прикладного ПО, маршрутизаторов, межсетевых экранов, WEB-серверов и т.п.

Другим примером системы анализа защищенности является программа SuperScan, позволяющая сканировать открытые порты узлов с известными IP-адресами. Для начала

сканирования достаточно в поле Start указать IP-адрес сканируемого узла. Для более глубокого сканирования необходимо указать минимальную скорость сканирования, передвинув движок на отметку Min.

Задание к практической работе

Работа состоит из трех заданий. Кроме того имеется дополнительное задание, которое не является обязательным для выполнения. Полное выполнение дополнительного задания позволяет не защищать отчет по практической работе.

Задание 1. Настройка брандмауэра Windows

1. Запустите брандмауэр Windows на своем компьютере. Посмотрите, включен ли он. Если не брандмауэр включен, то включите.
2. Посмотрите, какие программы добавлены в исключение на вашем компьютере и выпишете их в тетрадь.
3. Добавьте 1-2 программы в исключение брэндамауэра Windows.
4. Найдите в настройках брэндмауэра Windows настройку «Разрешать превышение исходящего времени. К параметрам, какого протокола относится эта настройка?
5. Проверьте, как настроен на вашем компьютере журнал безопасности, и изучите, какие настройки можно устанавливать.

Задание 2. Настройка обозревателя Internet Explorer

1. Запустите обозреватель Internet Explorer на своем компьютере
2. В меню сервис найдите настройку «Запрет всплывающих окон» и включите его.
3. Установите в настройках обозревателя время для хранения списка посещенных веб-узлов 5 дней.
4. Найдите настройку «Проверять, не отозван ли сертификат сервера» и посмотрите, при каких условиях она активируется.

Задание 3. Проверка межсетевого взаимодействия

Данная работа выполняется в паре (на двух соседних компьютерах). Ее целью является демонстрация работы брандмауэра при межсетевом взаимодействии.

1. Определите IP-адреса двух соседних компьютеров.
2. Включите брандмауэр Windows на первом компьютере. Запустите командную строку на втором компьютере (Пуск ->Выполнить->cmd). Наберите в командной строке команду ping и IP-адрес первого компьютера. Каков результат? Запишите в тетрадь, сколько пакетов было отправлено, сколько потеряно и сколько получено. Объясните почему.

3. Теперь выключите брандмауэр на первом компьютере и повторите все действия из пункта 2. Что показала команда ping на этот раз? Почему?

Примечание: Многие антивирусные программы имеют встроенный брандмауэр, поэтому если результат такой же, как и в пункте 2, попробуйте отключить антивирус на некоторое время (или отключить только режим анти-хакер).

4. Попробуйте поменять компьютеры местами. Изменился ли результат?

Дополнительное задание

Брандмауэры Windows являются встроенными и не позволяют обеспечить универсальную защиту компьютера. При помощи сети Интернет найдите информацию о коммерческих и свободно распространяемых брандмауэрах. Каковы предлагаемые защитные функции у этих программных продуктов. Какова стоимость коммерческого ПО и насколько она оправдана?

Контрольные вопросы

1) Может ли брандмауэр блокировать компьютерным вирусам и «червям» доступ на компьютер?
2) Может ли брандмауэр запретить пользователю открывать сообщения электронной почты с опасными вложениями?
3) Может ли брандмауэр блокировать спам или несанкционированные почтовые рассылки?
4) Может ли брандмауэр запросить пользователя о выборе блокировки или разрешения для определённых запросов на подключение?
5) Перечислите параметры, определяющие работу брандмауэра.
6) Какой параметр брандмауэра обеспечивает наивысшую защиту компьютера?
7) Что такое брандмауэр, его назначение.
8) Какими возможностями обладает Интернет обозреватель для защиты личных данных пользователей?
9) Перечислите параметры безопасности Internet Explorer.
10) Для чего нужно проводить анализ защищенности сети?

Практическое занятие № 12

Тема «Типы компьютерных вирусов и методы борьбы с ними»

Цель занятия: получить навыки подбора антивирусного ПО для домашнего и офисного пользования.

Оборудование для занятия: компьютер с операционной системой Windows, текстовый редактор Microsoft Word, редактор электронных таблиц MS Excel, наличие доступа к ресурсам глобальной сети Internet.

Форма проведение занятия: индивидуальная работа с публичным представлением отчета.

Теоретическая часть

Компьютерный вирус – это небольшая саморазмножающаяся программа, мешающая нормальной работе компьютера [20].

Процесс внедрения вирусом своей копии в другую программу, файлы или системную область диска называется **заражением,** а программа или иной объект, содержащий вирус — **зараженным.**

Основные источники вирусов и последствия их действия

Основными источники вирусов являются:

- ✓ съемный диск или DVD-диск, на котором находятся зараженные вирусом файлы;
- ✓ компьютерная сеть, в том числе система электронной почты и Internet;
- ✓ жесткий диск, на который попал вирус в результате работы с зараженными программами;
- ✓ вирус, оставшийся в оперативной памяти после предшествующего пользователя.

При заражении безвредными вирусами происходит уменьшение объема свободной оперативной памяти или памяти на дисках. Заражение неопасными вирусами приводит также к уменьшению объема свободной оперативной памяти или памяти на дисках или непонятным системным сообщениям, музыкальным и визуальным эффектам и т.д.

Опасные вирусы производят замедление загрузки и работы компьютера, непонятные (без причин) изменения в файлах, а также изменения размеров и даты последней модификации файлов, ошибки при загрузке операционной системы, невозможность сохранять файлы в нужных каталогах. Очень опасные вирусы являются причиной исчезновения файлов, форматирования жесткого диска, невозможности загрузки файлов или операционной системы.

Классификация вирусов

Вирусы классифицируются по нескольким признакам:

1. ***По способу заражения***: резидентные и нерезидентные;
2. ***По среде обитания***: файловые, сетевые, бутовые (загрузочные);
3. ***По деструктивным возможностям***: опасные и неопасные;

[20] *Энциклопедия безопасности Касперского. URL: http://www.securelist.com/ru/threats/detect/ (Режим доступа: свободный).*

По «среде обитания» вирусы можно разделить на несколько типов.

Резидентные вирусы – это вирусы, которые оставляют себя или часть себя в оперативной памяти и перехватывают любые операции ввода/вывода. При выключении компьютера уничтожаются вместе с очищением памяти.

Нерезидентные вирусы – характеризуются тем, что активны только при запуске зараженного файла, как только файл закрывается, вирус сворачивается.

Опасные – характеризуются, как правило, спонтанными аудиоэффектами, притормаживают работу ОС, привязаны к датам, как правило, одноразовые.

Загрузочные вирусы

Рассмотрим схему функционирования простого загрузочного вируса, заражающего диски.

Вспомним, что происходит при включении компьютера. В первую очередь начинает работу программа BIOS, которая тестирует компьютерную систему. После того как выясняется, что все компоненты компьютера функционируют нормально, управление передается небольшой программе-загрузчику операционной системы (ЗОС), которая должна загрузить операционную систему с диска и передать ей управление.

Таким образом, нормальная схема начальной загрузки следующая:

BIOS(ПЗУ) → ЗОС(диск) → Операционная система (диск) (1)

Теперь рассмотрим вирус. В загрузочных вирусах выделяют две части — так называемую голову и так называемый хвост. Хвост, вообще говоря, может быть пустым.

Пусть имеется не зараженный компьютер и дискета с активным резидентным вирусом. Как только этот вирус обнаружит, что в дисководе появилась подходящая жертва — в нашем случае еще не зараженный винчестер — он приступает к заражению. Заражая диск, вирус производит следующие действия:

- выделяет некоторую область диска и помечает ее как недоступную операционной системе; это можно сделать по-разному, в простейшем и традиционном случае занятые вирусом секторы помечаются как сбойные ***(bad),*** иногда вирусы даже форматируют на диске дополнительную дорожку;
- копирует в выделенную область диска свой хвост и оригинальный (здоровый) загрузочный сектор;
- замещает программу начальной загрузки в загрузочном секторе (настоящем) своей головой;
- организует цепочку передачи управления согласно схеме:

Голова вируса → Хвост вируса → Оригинальный загрузочный сектор. (2)

Таким образом, голова вируса теперь первой получает управление, вирус устанавливается в память и передает управление оригинальному загрузочному сектору. В цепочке (1) появляется новое звено:

BIOS(ПЗУ) Вирус → ЗОС(диск) → Операционная система.

Файловые вирусы

Простые файловые вирусы

В отличие от загрузочных вирусов, которые практически всегда резидентные, файловые вирусы совсем не обязательно резидентные. Файловые вирусы поражают исполняемые файлы.

Шифрованные и **полиморфные вирусы**

К данному типу вирусов относятся те, у которых часть кода зашифрована. При запуске вирус расшифровывается (разворачивается) в памяти и только потом выполняется.

Полиморфные вирусы имеют один и тот же зашифрованный код вируса, который можно расшифровать разными расшифровщиками. Кроме того имеется алгоритм для их автоматической генерации.

Стелс-вирусы

Некоторые загрузочные и файловые вирусы предпринимают специальные действия для «маскировки» — скрытия своего присутствия в зараженных объектах. Такие вирусы получили название «стеле-вирусов». Наиболее просто стелс-механизм реализуется в операционной системе MS-DOS. Способов маскировки (стелсирования) имеется довольно много, но все они реализуют одну идею — «сделать вид, что с зараженным объектом все нормально».

Макро-вирусы

Данные вирусы являются макросами, хранящимися во внешних файлах программного обеспечения (документах Microsoft Office, Autocad, CorelDRAW и пр.) и при открытии документа исполняются внутренними интерпретаторами данных программ. Широкое распространение они получили благодаря огромным возможностям интерпретатора языка Visual Basic, интегрированного в Microsoft Office. Излюбленным местом обитания этих вирусов являются офисы с большим документооборотом.

Макрос, написанный на языке VBA и интегрированный в документ, например, Word или Excel, обладает всеми теми же возможностями, что и обычное приложение. Он может отформатировать ваш винчестер или просто удалить информацию, украсть какие-то файлы или пароли и отправить их по электронной почте. Фактически вирусы этого класса способны парализовать работу целого офиса, а то даже и не одного

Троянские программы и **утилиты скрытого администрирования**

Одними из наиболее распространенных вирусов данного типа являются **Trojan и Backdoor программы.** Отличие этих двух типов программ заключается в том, что троянская программа выполняет активные действия (уничтожение данных, сбор данных и отправка через Internet, выполнение каких-либо действий в определенное время), в то время как Backdoor-программы открывают удаленный доступ к компьютеру и ожидают команды злоумышленника. Для простоты будем называть оба этих класса троянскими программами.

Главное отличие «троянов» от всех перечисленных выше творений человеческого разума — это то, что троянские программы не размножаются сами. Они единожды устанавливаются на компьютер и долгое время (как правило, либо до момента обнаружения, либо до переустановки операционной системы по какой-либо причине) выполняют свои функции.

Компьютерный антивирус – программа для поиска и уничтожения компьютерных вирусов.

Различают следующие типы компьютерных антивирусов:

1. Детекторы (полифаги)

Программы-детекторы позволяют обнаруживать файлы, зараженные одним из нескольких известных вирусов. Для этого они используют так называемые «маски». Маской вируса называют некоторую постоянную последовательность программного кода, специфичную для этого вируса. Если антивирусная программа обнаружит такую последовательность в каком-либо файле, то файл считается зараженным и подлежит лечению. Некоторые программы-детекторы также выполняют эвристический анализ файлов и системных областей дисков, что часто (но отнюдь не всегда) позволяет обнаруживать новые, не известные программе-детектору вирусы.

2. Ревизоры

Программы-ревизоры запоминают сведения о состоянии файлов и системных областей дисков, т.е. принцип работы ревизора основан на подсчете контрольных сумм файлов и некоторой другой: длины файлов, даты их последней модификации и т.д. Эти сведения сохраняются в базе данных антивируса. При последующих запусках ревизоры сравнивают состояния данных, содержащихся в базе данных с реально подсчитанными. При выявлении несоответствий об этом сообщается пользователю. Недостаток ревизоров состоит в том, что они не могут обнаружить вирус в новых файлах (на съемных дисках, при распаковке файлов из архива, в электронной почте), поскольку в их базе данных отсутствует информация об этих файлах.

3. Сторожа

Программы-сторожа (или блокировщики) располагаются резидентно в оперативной памяти компьютера и проверяют на наличие вирусов запускаемые файлы и вставляемые в дисковод съемные диски. При наличии вируса об этом сообщается пользователю. Кроме того, многие программы-сторожа перехватывают те действия, которые используются вирусами для размножения и нанесения вреда (скажем, попытку записи в загрузочный сектор или форматирование жесткого диска), и сообщают о них пользователю. Пользователь может разрешить или запретить выполнение соответствующей операции. Программы-сторожа позволяют обнаружить многие вирусы на самой ранней стадии, когда вирус еще не успел размножиться и что-либо испортить. Тем самым можно свести убытки от вируса к минимуму.

Практическая часть

1) Посетить сайты наиболее известных разработчиков антивирусных программ:

а) Антивирус Касперского (http://www.kaspersky.ru/),

б) Доктор Web (http://www.drweb.com/),

в) NOD32 (http://www.esetnod32.ru/),

д) Avast! (http://www.avast-russia.com/).

2) Исходя из информации, представленной на сайтах разработчиков анитивирусного ПО, проанализировать виды угроз, от которых гарантированно предоставляется защита. Анализ проводить по параметрам защиты от: 1) мошеннического ПО; 2) хакерских атак; 3) фишинга; 4) спама.

3) Результаты представить в виде статистической гистограммы, используя средства программного продукта MS Excel.

4) На основе полученных результатов выбрать антивирусное ПО для реализации политики безопасности компании. Привести обоснование выбора в виде сравнительного отчета выбранного продукта с остальными продуктами, по следующим показателям: а) стоимость; б) надежность; в) устойчивость; г) простота использования; д) наличие спецпредложений.

5) Защитить отчет устно перед остальными студентами. На выступление дается 5 мин.

Контрольные вопросы

1) Что такое компьютерный вирус и компьютерный антивирус?
2) Повысится ли устойчивость компьютера к воздействию вируса, если установить два антивирусных продукта одновременно?
3) Какие существуют классификации вирусов?

4) Какие существуют разновидности файловых вирусов?
5) Каков принцип функционирования загрузочных вирусов?
6) Каковы внешние проявления наличия вируса в компьютере?
7) Перечислить типы антивирусного ПО?

Практическое занятие № 13

Тема «Итоговое тестирование за семестр»
Цель занятия: контрольный срез знаний за семестр.

Итоговое занятие посвящено контролю полученных знаний за семестр. Студентам необходимо ответить на вопросы теста. На ответы дается 40 мин. Затем преподаватель проверяет тесты и подводит итоги. При успешном выполнении теста и наличии необходимого числа баллов (в соответствии с балльно-рейтинговой раскладкой за семестр) студент получает зачет.

Для успешного выполнения тестирования необходимо повторить все конспекты лекций и теоретический материал к практическим занятиям. Все вопросы в тестах составлены только на основе этого материала.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ И ИНФОРМАЦИОННЫЕ СИСТЕМЫ

1. Учебно-методическое обеспечение

Основная литература

1. Инженерно-техническая защита информации : учебное пособие [Электронный ресурс] / Титов А. А. – 2010. 195 с. Режим доступа: http://edu.tusur.ru/training/publications/654. (Дата обращения 20.06.2012 г.)
2. Информатика. Базовый курс : учебное пособие для вузов / С. В. Симонович [и др.] ; ред. С. В. Симонович. - СПб.: Питер, 2008. - 639с. (6 экз. в библ. ТУСУР).

Дополнительная литература

1. Мельников В.П. Информационная безопасность и защита информации : учебное пособие для вузов / В.П. Мельников, С.А. Клейменов, А.М. Петраков – М.: Академия, 2009. – 336 с. (1 экз. в библ. ТУСУР);
2. Акулов О.А. Информатика. Базовый курс : учебник для вузов / О.А. Акулов, Н.В., Медведев. – М.: Омега-Л, 2009. – 576 с. (1 экз. в библ. ТУСУР);

3. Куприянов А.И. Основы защиты информации. – М.: Academia, 2006. – 253 с. (50 экз. в библ. ТУСУР);

4. Основы защиты информации: учеб. пособие в 3 ч. Сост. А.А. Шелупанов [и др.]. – Томск: В-Спектр, 2007. – 150 с. (81 экземпляр в библиотеке ТУСУР);

5. Галатенко, Владимир Антонович. Основы информационной безопасности : учебное пособие для вузов / В. А. Галатенко ; ред. В. Б. Бетелин. - М. : Интернет-Университет Информационных Технологий, 2008 ; М. : БИНОМ. Лаборатория знаний, 2008. (1 экз. в библ. ТУСУР).

2. Справочные и информационные системы

1. Информационный портал по компьютерной безопасности [Электронный ресурс]. URL: http://www.securitylab.ru. (дата обращения 11.06.2012 г.)

3. OpenPGP в России. [Электронный ресурс] - URL: http://www.pgpru.com. (Дата обращения 18.06.2012 г.)

4. Официальный сайт компании Doctor Web. [Электронный ресурс] - URL: http://www.drweb.com. (Дата обращения 18.06.2012 г.)

5. Официальный сайт антивирусной лаборатории Касперского. [Электронный ресурс] - URL: http://www.kaspersky.ru (Дата обращения 18.06.2012 г.)

6. Поисковая система Google. [Электронный ресурс] - URL: http://google.com (Дата обращения 18.06.2012 г.)

7. Википедния свободная энциклопедия. [Электронный ресурс] – URL: http://ru.wikipedia.org/wiki. (Дата обращения 18.06.2012 г.)

8. Стандарты информационной безопасности. [Электронный ресурс] – URL: http://www.leta.ru/library/standards/ (Дата обращения 18.06.2012 г.)