МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
ДЕПАРТАМЕНТ НАУЧНО-ТЕХНОЛОГИЧЕСКОЙ ПОЛИТИКИ И ОБРАЗОВАНИЯ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
"КРАСНОЯРСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ"

Титовская Н.В., Титовский С.Н.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Учебное пособие

Красноярск 2023

Рецензенты:

И.Н. Коюпченко, канд. физ.-мат. наук, доц. каф. математического моделирования и информационных технологий ТЭИ ФГАОУ ВО СФУ

Постников А.И., канд.техн.наук., доцент каф. Вычислительной техники ИКИТ СФУ

Титовская Н.В., Титоский С.Н.

Информационная безопасность: учеб. пособие/ Н.В. Титовская, С.Н. Титовский; Краснояр. гос. аграр. ун-т. – Красноярск, 2023. – 182 с.

Охватывает теоретический и практический курс учебной дисциплины «Информационная безопасность». Проблема обеспечения информационной безопасности рассмотрена на различных уровнях. Значительное внимание уделено основным угрозам информационной безопасности и их источникам.

Наряду с теоретическими сведениями обеспечения информационной безопасности в учебном пособии рассмотрены практические механизмы защиты информации и поддерживающей ее инфраструктуры, в том числе и применительно к вычислительным сетям. В пособии содержится руководство по выполнению десяти лабораторных работ, имеются тесты по контролю знаний студентов. В конце каждой рассматриваемой темы приводится список контрольных вопросов. В приложении приводится справочник основных терминов и понятий в сфере информационной безопасности, а также варианты тестовых контрольных заданий.

Учебное пособие предназначено для студентов направления подготовки 09.03.03 «Прикладная информатика», 09.02.07 «Информационные системы и программирование».

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Развитие современного общества напрямую связано с ростом производства, потребления и накопления информации во всех отраслях человеческой деятельности. Информационные потоки в обществе увеличиваются с каждым днем, и этот процесс носит лавинообразный характер.

По своему значению для развития общества информация приравнивается к важнейшим ресурсам наряду с сырьем и энергией. В развитых странах большинство работающих заняты не в сфере производства, а в той или иной степени занимаются обработкой информации.

Вместе с тем можно отметить и новую тенденцию, заключающуюся во все большей информационной зависимости общества в целом и отдельного человека в частности. Именно поэтому в последнее время появились такие категории, как «информационная политика», «информационная безопасность», «информационная война» и целый ряд других новых понятий, в той или иной мере связанных с информацией.

Столь же ярко демонстрирует повышение роли информации в производственных процессах появление в XX веке такого понятия, как промышленный шпионаж. Не материальные ценности, а чистая информация становится объектом хищения. Это обстоятельство подчеркивает, насколько важной является информация для современного общества.

Информационная безопасность является одной из главных проблем, с которой сталкивается современное общество. Причиной обострения этой проблемы является широкомасштабное использование автоматизированных средств накопления, хранения, обработки и передачи информации.

В первом разделе учебного пособия изложены общие подходы к обеспечению информационной безопасности, дано понятие политики безопасности и ее содержание, проанализированы основные угрозы информационной безопасности.

Во втором разделе рассмотрена проблема защиты автоматизированных систем от программных вирусов. В соответствии с приведенной классификацией компьютерных вирусов и вирусоподобных программ в разделе изложены основные способы противодействия проникновения вирусов и вирусоподобных программ в компьютеры пользователей.

В третьем разделе рассмотрены вопросы обеспечения информационной безопасности в компьютерных сетях. С развитием локальных и глобальных сетей именно удаленные атаки становятся лидирующими как по количеству попыток, так и по успешности их применения, и, соответственно, обеспечение безопасности вычислительных сетей с точки зрения противостояния удаленным атакам приобретает первостепенное значение.

В четвертом разделе описаны наиболее значимые механизмы защиты вычислительных систем от несанкционированных действий как преднамеренного, так и непреднамеренного характера, такие как аутентификация, аудит, шифрование, межсетевое экранирование и др.

Пятый раздел включает десять практических занятий по профилактике компьютерных вирусов, а также настройке политики безопасности. Все практические занятия содержат подробные алгоритмы, сопровождаемые соответствующими пояснениями и иллюстрациями. По каждому из занятий предусмотрено задание для самостоятельной работы.

Для повышения качества контроля знаний в пособии предусмотрены две формы контроля. Во-первых, в конце каждого раздела приводится перечень наиболее важных вопросов. Во-вторых, приведены три варианта тестовых контрольных заданий, охватывающих весь курс.

В приложении приводятся основных термины и понятия в сфере информационной безопасности.

Пособие соответствует Федеральному государственному образовательному стандарту по подготовке студентов высших специальных учебных заведений.

1. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И УРОВНИ ЕЕ ОБЕСПЕЧЕНИЯ

1.1. Понятие «информационная безопасность»

Информационная безопасность – это защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб владельцам или пользователям информации [10].

Рассматривая информацию как товар, можно сказать, что нанесение ущерба информации в целом приводит к материальным затратам. Например, раскрытие технологии изготовления оригинального продукта приведет к появлению аналогичного продукта, но от другого производителя, и, как следствие, владелец технологии, а может быть, и автор, потеряют часть рынка и т. д.

С другой стороны, рассматривая информацию как субъект управления (технология производства, расписание движения транспорта и т. д.), можно утверждать, что изменение ее может привести к катастрофическим последствиям в объекте управления – производстве, транспорте и др.

Именно поэтому при определении понятия «информационная безопасность» на первое место ставится защита информации от различных воздействий.

Поэтому под ***защитой информации*** понимается комплекс мероприятий, направленных на обеспечение информационной безопасности.

Согласно ГОСТ 350922-96 ***защита информации*** – это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Решение проблемы информационной безопасности, как правило, начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем. Это обусловлено тем, что для разных категорий субъектов характер решаемых задач может существенно различаться. Например, задачи, решаемые администратором локальной сети по обеспечению информационной безопасности, в значительной

степени отличаются от задач, решаемых пользователем на домашнем компьютере, не связанном сетью.

Исходя из этого, отметим следующие важные выводы:

- задачи по обеспечению информационной безопасности для разных категорий субъектов могут существенно различаться;
- информационная безопасность не сводится исключительно к защите от несанкционированного доступа к информации это принципиально более широкое понятие.

В ряде случаев понятие «информационная безопасность» подменяется термином «компьютерная безопасность». В этом случае информационная безопасность рассматривается очень узко, поскольку компьютеры только одна из составляющих информационных систем. Несмотря на это, в рамках изучаемого курса основное внимание будет уделяться изучению вопросов, связанных с обеспечением режима информационной безопасности применительно к вычислительным системам, в которых информация хранится, обрабатывается и передается с помощью компьютеров.

Согласно определению, компьютерная безопасность зависит не только от компьютеров, но и от поддерживающей инфраструктуры, к которой можно отнести системы электроснабжения, жизнеобеспечения, вентиляции, средства коммуникаций, а также обслуживающий персонал.

1.2. Составляющие информационной безопасности

Обеспечение информационной безопасности в большинстве случаев связано с комплексным решением трех задач:

1) обеспечением доступности информации;
2) обеспечением целостности информации;
3) обеспечением конфиденциальности информации.

Именно доступность, целостность и конфиденциальность являются равнозначными составляющими информационной безопасности.

Доступность – это гарантия получения требуемой информации или информационной услуги пользователем за определенное время.

Фактор времени в определении доступности информации в ряде случаев является очень важным, поскольку некоторые виды информации и информационных услуг имеют смысл только в определенный промежуток времени.

Целостность информации условно подразделяется на статическую и динамическую. ***Статическая*** целостность информации предполагает неизменность информационных объектов от их исходного состояния, определяемого автором или источником информации. ***Динамическая*** целостность информации включает вопросы корректного выполнения сложных действий с информационными потоками, например, анализ потока сообщений для выявления некорректных сообщений, контроль правильности передачи сообщений, подтверждение отдельных сообщений и др.

Целостность является важнейшим аспектом информационной безопасности в тех случаях, когда информация используется для управления различными процессами, например техническими, социальными и т. д.

Целостность – гарантия того, что информация сейчас существует в ее исходном виде, то есть при ее хранении или передаче не было произведено несанкционированных изменений.

Конфиденциальность – гарантия доступности конкретной информации только тому кругу лиц, для кого она предназначена.

Конфиденциальная информация есть практически во всех организациях. Это может быть технология производства, программный продукт, анкетные данные сотрудников и др. Применительно к вычислительным системам в обязательном порядке конфиденциальными данными являются пароли для доступа к системе.

Нарушение каждой из трех категорий приводит к нарушению информационной безопасности в целом. Так, нарушение доступности приводит к отказу в доступе к информации, нарушение целостности приводит к фальсификации информации и, наконец, нарушение конфиденциальности приводит к раскрытию информации.

1.3. Классификация угроз информационной безопасности

Угроза информационной безопасности – это потенциальная возможность нарушения режима информационной безопасности. Преднамеренная реализация угрозы называется ***атакой*** на информационную систему. Лица, преднамеренно реализующие угрозы, являются ***злоумышленниками***.

Чаще всего угроза является следствием наличия уязвимых мест в защите информационных систем, например, неконтролируемый доступ к персональным компьютерам или нелицензионное программное обеспечение.

Угрозы информационной безопасности классифицируются по нескольким признакам:

- ***по составляющим информационной безопасности*** (доступность, целостность, конфиденциальность), против которых в первую очередь направлены угрозы;
- ***по компонентам информационных систем***, на которые угрозы нацелены (данные, программы, аппаратура, персонал);
- ***по характеру воздействия*** (случайные или преднамеренные, действия природного или техногенного характера);
- ***по расположению источника угроз*** (внутри или вне рассматриваемой информационной системы).

Рассмотрим угрозы по характеру воздействия. Опыт проектирования, изготовления и эксплуатации информационных систем показывает, что информация подвергается различным случайным воздействиям на всех этапах цикла жизни системы.

Причинами ***случайных воздействий*** при эксплуатации могут быть:

- аварийные ситуации из-за стихийных бедствий и отключений электропитания (природные и техногенные воздействия);
- отказы и сбои аппаратуры;
- ошибки в программном обеспечении;
- ошибки в работе персонала;
- помехи в линиях связи из-за воздействий внешней среды.

Преднамеренные воздействия – это целенаправленные действия злоумышленника. В качестве злоумышленника может выступить служащий, посетитель, конкурент, наемник. Действия нарушителя могут быть обусловлены разными мотивами, например:

недовольством служащего служебным положением; любопытством; конкурентной борьбой; уязвленным самолюбием и т. д.

Угрозы, классифицируемые ***по расположению источника угроз,*** бывают внутренние и внешние. Внешние угрозы обусловлены применением вычислительных сетей и созданием на их основе информационных систем.

Основная особенность любой вычислительной сети состоит в том, что ее компоненты распределены в пространстве. Связь между узлами сети осуществляется физически с помощью сетевых линий и программно с помощью механизма сообщений. При этом управляющие сообщения и данные, пересылаемые между узлами сети, передаются в виде пакетов обмена. Особенность данного вида угроз заключается в том, что местоположение злоумышленника изначально неизвестно.

1.4. Каналы несанкционированного доступа к информации

Одним из наиболее распространенных и многообразных способов воздействия на информационную систему, позволяющих нанести ущерб любой из составляющих информационной безопасности, является ***несанкционированный доступ***. Несанкционированный доступ возможен из-за ошибок в системе защиты, нерационального выбора средств защиты, их некорректной установки и настройки.

Каналы НСД классифицируются по компонентам автоматизированных информационных систем.

Через человека:

- хищение носителей информации;
- чтение информации с экрана или клавиатуры;
- чтение информации из распечатки.

Через программу:

- перехват паролей;
- расшифровка зашифрованной информации;
- копирование информации с носителя.

Через аппаратуру:

- подключение специально разработанных аппаратных средств, обеспечивающих доступ к информации;

- перехват побочных электромагнитных излучений от аппаратуры, линий связи, сетей электропитания и т. д.

Технические каналы утечки информации

Под техническим каналом утечки информации (ТКУИ) понимают совокупность объекта разведки, технического средства разведки (ТСР), с помощью которого добывается информация об этом объекте, и физической среды, в которой распространяется информационный сигнал. По сути, под ТКУИ понимают способ получения с помощью ТСР разведывательной информации об объекте. Причем под разведывательной информацией обычно понимаются сведения или совокупность данных об объектах разведки независимо от формы их представления.

Физические процессы, происходящие в технических средствах при их функционировании, создают в окружающем пространстве побочные излучения, которые в той или иной степени связаны с обрабатываемой информацией. Физические явления, лежащие в основе появления этих излучений, имеют различный характер, тем не менее, они могут рассматриваться как непреднамеренная передача конфиденциальной информации по некоторым побочным каналам, образованным источником излучения, средой распространения и, возможно, приемной стороной (злоумышленником). Такие побочные каналы принято называть техническим каналом утечки информации.

Основными источниками образования технических каналов утечки любой, в том числе конфиденциальной, информации являются:

- преобразователи физических величин;
- излучатели электромагнитных колебаний;
- паразитные связи и наводки на провода и элементы электронных устройств.

Примером реализации системы преобразователей является звукоусилительная система, в которой микрофон превращает звук в электрический сигнал. Последний передается и усиливается усилителем низкой (звуковой) частоты, а затем поступает на громкоговоритель, воспроизводящий звук существенно более громкий, нежели тот, который воспринимается микрофоном.

Образованию каналов утечки информации способствуют определенные обстоятельства и причины технического характера, такие как несовершенство схемных решений (конструктивных и

технологических), принятых для данной категории технических средств, эксплуатационный износ элементов изделия (изменение параметров элементов, аварийный выход/вывод из строя) и др.

При выявлении технических каналов утечки информации применительно к средствам вычислительной техники необходимо рассматривать все оборудование как систему, включающую основное (стационарное) оборудование, например, компьютеры, соединительные линии (совокупность проводов и кабелей, прокладываемых между отдельными компьютерами и элементами вычислительной сети), распределительные и коммутационные устройства, системы электропитания, системы заземления.

В этой системе следует различать устройства, непосредственно участвующие в обработке, хранении, передаче конфиденциальной информации, и устройства, непосредственно не участвующие в обработке конфиденциальной информации, но использующиеся с основным оборудованием, обеспечивая его работу (система электропитания, заземление и т. д.) или условия для работы пользователей (система кондиционирования и т.д.).

В качестве потенциальных каналов утечки информации следует рассматривать элементы вспомогательного оборудования, имеющие выход за пределы контролируемой зоны, то есть зоны, в пределах которой исключено несанкционированное пребывание посторонних лиц, например, в пределах аудитории или отдельного здания и т. д.

Кроме соединительных линий основного и вспомогательного оборудования за пределы контролируемой зоны могут выходить провода и кабели, к ним не относящиеся, но проходящие через помещения, где установлены технические средства, а также металлические трубы систем отопления, водоснабжения и другие токопроводящие металлоконструкции. Такие провода, кабели и токопроводящие элементы называются посторонними проводниками и тоже являются потенциальными каналами утечки информации.

В зависимости от физической природы возникновения информационных сигналов, а также среды их распространения и способов перехвата технические каналы утечки информации бывают электромагнитные, электрические и параметрические.

Электромагнитные каналы утечки информации.

К электромагнитным относятся каналы утечки информации, возникающие за счет:

- различного вида побочных электромагнитных излучений (ЭМИ) основного и вспомогательного оборудования;
- излучений элементов основного и вспомогательного оборудования;
- излучений на частотах работы высокочастотных (ВЧ) генераторов основного и вспомогательного оборудования;
- излучений на частотах самовозбуждения усилителей низкой частоты (УНЧ) основного оборудования.

Электромагнитные излучения элементов основного и вспомогательного оборудования. Носителем информации в технических средствах является электрический ток, параметры которого (сила тока, напряжение, частота и фаза) изменяются по закону информационного сигнала. При прохождении электрического тока по токоведущим элементам основного и вспомогательного оборудования вокруг них возникает электрическое и магнитное поле. В силу этого элементы основного и вспомогательного оборудования можно рассматривать как излучатели электромагнитного поля, модулированного по закону изменения информационного сигнала.

Электромагнитные излучения на частотах работы высокочастотных генераторов(ВЧ-генераторов) основного и вспомогательного оборудования. В состав основного и вспомогательного оборудования входят различного рода высокочастотные генераторы. К таким устройствам можно отнести: задающие генераторы, генераторы тактовой частоты, генераторы стирания и подмагничивания магнитофонов, гетеродины радиоприемных и телевизионных устройств, генераторы измерительных приборов и т. д.

В результате внешних воздействий информационного сигнала (например, электромагнитных колебаний) на элементах ВЧ-генераторов наводятся электрические сигналы. Приемником магнитного поля могут быть катушки индуктивности колебательных контуров, дроссели в цепях электропитания и т. д. Приемником электрического поля являются провода высокочастотных цепей и другие элементы. Наведенные электрические сигналы могут вызвать непреднамеренную модуляцию собственных ВЧ-колебаний генераторов. Эти промодулированные ВЧ-колебания излучаются в окружающее пространство.

Электромагнитные излучения на частотах самовозбуждения УНЧ основного и вспомогательного оборудования. Самовозбуждение УНЧ основного и вспомогательного оборудования (например, усилителей систем звукоусиления и звукового сопровождения) возможно за счет случайных преобразований отрицательных обратных связей (индуктивных или емкостных) в паразитные положительные, что приводит к переводу усилителя из режима усиления в режим автогенерации сигналов. Частота самовозбуждения лежит в пределах рабочих частот нелинейных элементов УНЧ (например, полупроводниковых приборов). Сигнал на частотах самовозбуждения, как правило, оказывается модулированным информационным сигналом. Самовозбуждение наблюдается, в основном, при переводе УНЧ в нелинейный режим работы, то есть в режим перегрузки.

Перехват побочных электромагнитных излучений ТСПИ осуществляется средствами радио-, радиотехнической разведки, размещенными вне контролируемой зоны.

Электрические каналы утечки информации.

Причинами возникновения электрических каналов утечки информации являются:

- наводки электромагнитных излучений основного оборудования на соединительные линии вспомогательного оборудования и посторонние проводники, выходящие за пределы контролируемой зоны;
- прохождение информационных сигналов в цепи электропитания основного и вспомогательного оборудования;
- прохождение информационных сигналов в цепи заземления основного и вспомогательного оборудования.

Наводки электромагнитных излучений возникают при излучении элементами основного и вспомогательного оборудования (в том числе и их соединительными линиями) информационных сигналов, а также при наличии гальванической связи соединительных линий основного оборудования и посторонних проводников или линий вспомогательного оборудования. Уровень наводимых сигналов в значительной степени зависит от мощности излучаемых сигналов, расстояния до проводников, а также длины совместного пробега соединительных линий основного оборудования и посторонних проводников.

Пространство вокруг основного оборудования, в пределах которого на случайных антеннах наводится информационный сигнал выше допустимого (нормированного) уровня, называется (опасной) зоной 1.

Случайной антенной в данном случае может стать цепь вспомогательного оборудования или посторонние проводники, способные принимать побочные электромагнитные излучения.

Случайные антенны могут быть сосредоточенными и распределенными. Сосредоточенная случайная антенна представляет собой компактное техническое средство, например, телефонный аппарат, громкоговоритель радиотрансляционной сети и т. д. К распределенным случайным антеннам относятся случайные антенны с распределенными параметрами: кабели, провода, металлические трубы и другие токопроводящие коммуникации.

Прохождение информационных сигналов в цепи электропитания возможно при наличии магнитной связи между выходным трансформатором усилителя (например, УНЧ) и трансформатором выпрямительного устройства. Кроме того, токи усиливаемых информационных сигналов замыкаются через источник электропитания, создавая на его внутреннем сопротивлении падение напряжения, которое при недостаточном затухании в фильтре выпрямительного устройства может быть обнаружено в линии электропитания. Информационный сигнал может проникнуть в цепи электропитания также в результате того, что среднее значение потребляемого тока в оконечных каскадах усилителей в большей или меньшей степени зависит от амплитуды информационного сигнала, что создает неравномерную нагрузку на выпрямитель и приводит к изменению потребляемого тока по закону изменения информационного сигнала.

Прохождение информационных сигналов в цепи заземления. Кроме заземляющих проводников, служащих для непосредственного соединения основного оборудования с контуром заземления, гальваническую связь с землей могут иметь различные проводники, выходящие за пределы контролируемой зоны. К ним относятся нулевой провод сети электропитания, экраны подключения к соединительным линиям вспомогательного оборудования и посторонним проводникам, проходящим через помещения, где установлено основное оборудование, а также к его системе электропитания и заземления. Для этих целей используются

специальные средства радио- и радиотехнической разведки, а также специальная измерительная аппаратура.

Электронные устройства перехвата информации, устанавливаемые в основное оборудование, иногда называют аппаратными закладками. Они представляют собой мини-передатчики, излучение которых модулируется информационным сигналом. Наиболее часто закладки устанавливаются в основное оборудование иностранного производства.

Перехваченная с помощью закладных устройств информация или непосредственно передается по радиоканалу, или сначала записывается на специальное запоминающее устройство, а уже затем по команде передается на запросивший ее объект.

Параметрический канал утечки информации.

Перехват обрабатываемой в технических средствах информации возможен также путем их «высокочастотного облучения». При взаимодействии облучающего электромагнитного поля с элементами основного оборудования происходит переизлучение электромагнитного поля. В ряде случаев это вторичное излучение модулируется информационным сигналом. При съеме информации для исключения взаимного влияния облучающего и переизлученного сигналов может использоваться их временная или частотная развязка. Например, для облучения основного оборудования могут использовать импульсные сигналы. При переизлучении параметры сигналов изменяются. Поэтому данный канал утечки информации часто называют параметрическим.

Для перехвата информации по данному каналу необходимы специальные высокочастотные генераторы с антеннами, имеющими узкие диаграммы направленности и специальные радиоприемные устройства.

1.5. Анализ угроз информационной безопасности

Наиболее распространенные угрозы нарушения доступности информации

Самыми частыми и самыми опасными (с точки зрения размера ущерба) являются непреднамеренные ошибки штатных пользователей, операторов, системных администраторов и других лиц, обслуживающих информационные системы.

Иногда такие ошибки и являются собственно угрозами (неправильно введенные данные или ошибка в программе), иногда они создают уязвимые места, которыми могут воспользоваться злоумышленники (обычные ошибки администрирования).

Самый эффективный способ борьбы с непреднамеренными случайными ошибками – максимальная автоматизация и строгий контроль.

Другие угрозы доступности классифицируем по компонентам автоматизированной информационной системы, на которые нацелены угрозы:

- отказ пользователей;
- внутренний отказ информационной системы;
- отказ поддерживающей инфраструктуры.

Применительно к пользователям рассматриваются следующие угрозы:

- нежелание работать с информационной системой (чаще всего проявляется при необходимости осваивать новые возможности);
- невозможность работать с системой в силу отсутствия соответствующей подготовки (недостаток общей компьютерной грамотности, неумение интерпретировать диагностические сообщения, неумение работать с документацией и т. п.);
- невозможность работать с системой в силу отсутствия технической поддержки (неполнота документации, недостаток справочной информации и т. п.).

Основными источниками внутренних отказов являются:

- отступление (случайное или умышленное) от установленных правил эксплуатации;
- выход системы из штатного режима эксплуатации в силу случайных или преднамеренных действий пользователей или

обслуживающего персонала (превышение расчетного числа запросов, чрезмерный объем обрабатываемой информации и т. п.);

- ошибки при конфигурировании системы;
- отказы программного и аппаратного обеспечения;
- разрушение данных;
- разрушение или повреждение аппаратуры.

По отношению к поддерживающей инфраструктуре рассматриваются следующие угрозы:

- нарушение работы (случайное или умышленное) систем связи, электропитания, водо – и/или теплоснабжения, кондиционирования;
- разрушение или повреждение помещений;
- невозможность или нежелание обслуживающего персонала и/или пользователей выполнять свои обязанности.

Опасными являются и ***стихийные бедствия*** – пожары, наводнения, землетрясения, ураганы. По статистике на долю этих источников угроз с учетом перебоев электропитания приходится 13% потерь, нанесенных информационным системам.

Угрозы доступности могут выглядеть грубо – как ***повреждение*** или даже ***разрушение*** оборудования (в том числе носителей данных). Такое повреждение может вызываться естественными причинами (чаще всего – грозами). К сожалению, находящиеся в массовом использовании источники бесперебойного питания не защищают от мощных кратковременных импульсов.

Одним из способов нарушения доступности является загрузка информационной системы (загрузка полосы пропускания сетей, вычислительных возможностей процессоров или оперативной памяти). По расположению источника такие угрозы подразделяется на ***внутренние*** и ***внешние***. При просчетах в конфигурации системы локальная программа способна практически монополизировать процессор и/или физическую память, сведя скорость выполнения других программ к нулю.

Известны случаи вывода из строя сервисов глобальной сети Интернет, когда на сервер с множества разных адресов с максимальной скоростью направляются вполне легальные запросы на соединение и/или обслуживание.

Одним из опаснейших способов нарушения доступности и в целом информационной безопасности является внедрение в атакуемые системы ***вредоносного программного обеспечения***.

Целями такого программного обеспечения является:

- внедрение другого вредоносного программного обеспечения;
- получение контроля над атакуемой системой;
- агрессивное потребление ресурсов;
- изменение или разрушение программ и/или данных.

К сожалению, количество «вредного» программного обеспечения постоянно увеличивается. Вирусы и троянские программы считают уже на десятки тысяч, а базы данных антивирусных программ обновляются практически ежедневно, несмотря на постоянно внедряемые методы «универсального» детектирования (то есть детектирования не конкретных вариантов отдельно взятого вируса, а всего «семейства» или даже целого класса вредоносных программ).

Причины роста данного вида угроз связаны с тем, что к компьютерам получают доступ все большее и большее количество кибер-хулиганов (по мере расширения глобальных информационных сетей). Какое-то число из них начинает самоутверждаться описанным выше способом.

Подробный анализ данного класса угроз рассмотрим в следующих темах.

Основные угрозы нарушения целостности информации

На втором месте по размерам ущерба (после непреднамеренных ошибок и упущений) стоят кражи и подлоги. По данным газеты USA Today, еще в 1992 году в результате подобных противоправных действий с использованием персональных компьютеров американским организациям был нанесен общий ущерб в размере 882 миллионов долларов.

В большинстве случаев виновниками оказывались штатные сотрудники организаций, отлично знакомые с режимом работы и мерами защиты. Это еще раз подтверждает опасность внутренних угроз.

С целью нарушения статической целостности злоумышленник (как правило, штатный сотрудник) может:

- ввести неверные данные;

- изменить данные, например, время создания или получения документа.

Угрозой целостности является не только фальсификация или изменение данных, но и отказ от совершенных действий. С этой угрозой связано понятие «аутентичность», то есть возможность подтверждения (доказательства) авторства того или иного документа или действия.

Потенциально уязвимы с точки зрения нарушения ***целостности*** не только ***данные***, но и ***программы***. Внедрение рассмотренного выше вредоносного программного обеспечения – пример подобного нарушения.

Угрозами динамической целостности являются дублирование данных или внесение дополнительных сообщений (сетевых пакетов и т. п.). Соответствующие действия в сетевой среде называются активным прослушиванием.

Основные угрозы нарушения конфиденциальности информации

Конфиденциальную информацию условно можно разделить на предметную и служебную. Служебная информация (например, пароли пользователей) не относится к определенной предметной области, в информационной системе она играет техническую роль, но ее раскрытие особенно опасно, поскольку оно чревато получением несанкционированного доступа ко всей информации, в том числе предметной.

Даже если информация хранится в компьютере или предназначена для компьютерного использования, угрозы ее конфиденциальности могут носить некомпьютерный и вообще нетехнический характер, например, при работе с несколькими информационными системами возникает необходимость запоминания нескольких паролей. В таких случаях чаще всего пользуются записными книжками, листками, которые зачастую находятся рядом с компьютером и т. д. Описанный класс уязвимых мест можно назвать размещением конфиденциальных данных в среде, где им не обеспечена необходимая защита. Помимо паролей, хранящихся в записных книжках пользователей, в этот класс попадает передача конфиденциальных данных в открытом виде (в разговоре, в письме, по сети), которая делает возможным перехват данных. Для атаки могут использоваться разные технические средства (подслушивание

или прослушивание разговоров, пассивное прослушивание сети и т. п.), но идея одна – осуществить доступ к данным в тот момент, когда они наименее защищены.

Перехват данных – очень серьезная угроза, и если конфиденциальность действительно является критичной, а данные передаются по многим каналам, их защита может оказаться весьма сложной и дорогостоящей. Технические средства перехвата хорошо проработаны, доступны, просты в эксплуатации, а установить их, например, на кабельную сеть, может кто угодно, так что эту угрозу нужно принимать во внимание по отношению не только к внешним, но и к внутренним коммуникациям.

Кражи оборудования являются угрозой не только для резервных носителей, но и для компьютеров, особенно портативных.

К неприятным угрозам, от которых трудно защищаться, можно отнести злоупотребление полномочиями. На многих типах систем привилегированный пользователь (например, системный администратор) способен прочитать любой (незашифрованный) файл, получить доступ к почте любого пользователя и т. д. Другой пример – нанесение ущерба при сервисном обслуживании. Обычно сервисный инженер получает неограниченный доступ к оборудованию и имеет возможность действовать в обход программных защитных механизмов.

Контрольные вопросы по разделу №1

1. В чем заключается проблема «информационной безопасности»?
2. Дайте определение «информационной безопасности».
3. Перечислите составляющие информационной безопасности и их определение.
4. Каким образом взаимосвязаны между собой составляющие информационной безопасности? Приведите собственные примеры.
5. Перечислите уровни формирования режима информационной безопасности.
6. Перечислите основополагающие документы по «информационной безопасности».
7. Дайте характеристику составляющих «информационной безопасности» применительно к вычислительным сетям.
8. Перечислите основные механизмы безопасности.

9. Что понимается под администрированием средств безопасности?
10. Классы защищенности межсетевых экранов.
11. Содержание административного уровня обеспечения «информационной безопасности».
12. Дайте определение политики безопасности.
13. Направления разработки политики безопасности.
14. Перечислите классы угроз информационной безопасности. Назовите причины и источники случайных воздействий на информационные системы.
15. Дайте характеристику преднамеренным угрозам.
16. Перечислите каналы несанкционированного доступа.
17. Что понимается под техническим каналом утечки информации?
18. Каковы причины возникновения электромагнитных каналов утечки информации?
19. Как образуется параметрический канал утечки информации?
20. Основные угрозы целостности информации.
21. Охарактеризуйте угрозы доступности информации.

2. КОМПЬЮТЕРНЫЕ ВИРУСЫ И ЗАЩИТА ОТ НИХ

Компьютерные вирусы – одна из главных угроз информационной безопасности. Это связано с масштабностью распространения этого явления и, как следствие, огромного ущерба, наносимого информационным системам [10].

Компьютерные вирусы были и остаются одной из наиболее распространенных причин потери информации, вирусные эпидемии способны блокировать работу организаций и предприятий.

Основная особенность компьютерных вирусов заключается в возможности их самопроизвольного внедрения в различные объекты операционной системы. К более полной характеристике современного компьютерного вируса следует добавить способность создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети или файлы, системные области компьютера и прочие выполняемые объекты.

Одно из общепринятых определений вируса, содержащееся в ГОСТе Р 51275-99 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»:

«Программный вирус» – это исполняемый или интерпретируемый программный код, обладающий свойством несанкционированного распространения и самовоспроизведения в автоматизированных системах или телекоммуникационных сетях с целью изменить или уничтожить программное обеспечение и/или данные, хранящиеся в автоматизированных системах.

Невозможность четкой формулировки определения компьютерного вируса сама по себе не является проблемой. Главная проблема, которая следует из этого, заключается в том, что нет четких (однозначных) признаков, по которым можно отличить различные файлы от «вирусов», что не позволяет в полной мере устранить их влияние.

Несмотря на все усилия разработчиков антивирусного программного обеспечения, до сегодняшнего дня нет достаточно надежных антивирусных средств и скорее всего противостояние «вирусописателей» и их оппонентов будет постоянным.

2.1. Классификация компьютерных вирусов

Классификация компьютерных вирусов по среде обитания

По среде «обитания» вирусы делятся на:

- файловые;
- загрузочные;
- макровирусы;
- сетевые.

Файловые вирусы внедряются в выполняемые файлы (наиболее распространенный тип вирусов), либо создают файлы-двойники (компаньон – вирусы), либо используют особенности организации файловой системы (link-вирусы).

Загрузочные вирусы записывают себя либо в загрузочный сектор диска (boot-сектор), либо в сектор, содержащий системный загрузчик жесткого диска (Master Boot Record), либо меняют указатель на активный boot-сектор.

Макровирусы заражают файлы – документы и электронные таблицы популярных офисных приложений.

Сетевые вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты.

Существует большое количество сочетаний, например, файлово-загрузочные вирусы, заражающие как файлы, так и загрузочные сектора дисков. Такие вирусы, как правило, имеют довольно сложный алгоритм работы, часто применяют оригинальные методы проникновения в систему, используют стелс- и полиморфик-технологии. Другой пример такого сочетания – сетевой макровирус, который не только заражает редактируемые документы, но и рассылает свои копии по электронной почте.

Заражаемая операционная система является вторым уровнем деления вирусов на классы. Каждый файловый или сетевой вирус заражает файлы какой-либо одной или нескольких опрерационных систем. Макровирусы заражают файлы форматов Word, Excel, пакета Office. Загрузочные вирусы также ориентированы на конкретные форматы расположения системных данных в загрузочных секторах дисков.

Классификация компьютерных вирусов по особенностям алгоритма работы

По особенностям алгоритма работы вирусы делятся на:

- резидентные;
- стелс-вирусы;
- полиморфик-вирусы;
- вирусы, использующие нестандартные приемы.

Резидентный вирус при инфицировании компьютера оставляет в оперативной памяти свою резидентную часть, которая затем перехватывает обращения операционной системы к объектам заражения и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения компьютера или перезагрузки операционной системы. Нерезидентные вирусы не заражают память компьютера и сохраняют активность ограниченное время. К резидентным относятся макровирусы, поскольку они постоянно присутствуют в памяти компьютера на все время работы зараженного редактора. При этом роль операционной системы берет на себя редактор, а понятие «перезагрузка операционной системы» трактуется как выход из редактора.

Использование ***стелс-алгоритмов*** позволяет вирусам полностью или частично скрыть себя в системе. Наиболее распространенным стелс-алгоритмом является перехват запросов операционной системы на чтение/запись зараженных объектов. Стелс-вирусы при этом либо временно лечат их, либо «подставляют» вместо себя незараженные участки информации. В случае макровирусов наиболее популярный способ – запрет вызовов меню просмотра макросов.

Самошифрование и полиморфичность используются практически всеми типами вирусов для того, чтобы максимально усложнить процедуру детектирования (обнаружения) вируса. ***Полиморфик-вирусы*** (polymorphic) – это достаточно труднообнаруживаемые вирусы, не имеющие сигнатур, то есть не содержащие ни одного постоянного участка кода. В большинстве случаев два образца одного и того же полиморфик-вируса не будут иметь ни одного совпадения. Это достигается шифрованием основного тела вируса и модификациями программы-расшифровщика.

Различные нестандартные приемы часто используются в вирусах для того, чтобы как можно глубже спрятать себя в ядре операционной системы, защитить от обнаружения свою резидентную копию, затруднить лечение от вируса (например, поместив свою копию в Flash-BIOS) и т. д.

Классификация компьютерных вирусов по деструктивным возможностям

По деструктивным возможностям вирусы можно разделить на:

- ***безвредные,*** то есть никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения);
- ***неопасные,*** влияние которых ограничивается уменьшением свободной памяти на диске;
- ***опасные вирусы,*** которые могут привести к серьезным сбоям в работе компьютера;
- ***очень опасные,*** в алгоритм работы которых заведомо заложены процедуры, которые могут привести к потере программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти, и далее повредить аппаратные средства компьютера.

2.2. Характеристика «вирусоподобных» программ

К «вредным программам», помимо вирусов, относятся:

- «троянские программы» (логические бомбы);
- утилиты скрытого администрирования удаленных компьютеров;
- «intended»-вирусы;
- конструкторы вирусов;
- полиморфик-генераторы.

«Троянские» программы (логические бомбы). К «троянским» программам относятся программы, наносящие какие-либо разрушительные действия в зависимости от каких-либо условий. Например, уничтожение информации на дисках при каждом запуске или по определенному графику и т. д. Большинство известных «троянских» программ являются программами, которые маскируются под какие-либо полезные программы, новые версии популярных утилит или дополнения к ним. Очень часто они рассылаются по электронным конференциям. По сравнению с вирусами «троянские» программы не получают широкого распространения по достаточно простым причинам – они либо уничтожают себя вместе с остальными данными на диске, либо демаскируют свое присутствие и уничтожаются

пострадавшим пользователем. К «троянским» программам также относятся так называемые «дропперы» вирусов – зараженные файлы, код которых подправлен таким образом, что известные версии антивирусов не определяют присутствие вируса в файле. Например, файл шифруется или упаковывается неизвестным архиватором, что не позволяет антивирусу «увидеть» заражение.

Отметим еще один тип программ (программы – «злые шутки»), которые используются для устрашения пользователя, свидетельствуя о заражении вирусом или о каких-либо предстоящих действиях с этим связанных, то есть сообщают о несуществующих опасностях, вынуждая пользователя к активным действиям. Например, к «злым шуткам» относятся программы, которые «пугают» пользователя сообщениями о форматировании диска (хотя никакого форматирования на самом деле не происходит), детектируют вирусы в незараженных файлах, выводят странные вирусоподобные сообщения и т. д. К категории «злых шуток» можно отнести также заведомо ложные сообщения о новых «супер-вирусах». Такие сообщения периодически появляются в сети Интернет и обычно вызывают панику среди пользователей.

Утилиты скрытого администрирования. Утилиты скрытого администрирования являются разновидностью «логических бомб» («троянских программ»), которые используются злоумышленниками для удаленного администрирования компьютеров в сети. По своей функциональности они во многом напоминают различные системы администрирования, разрабатываемые и распространяемые различными фирмами-производителями программных продуктов. Единственная особенность этих программ заставляет классифицировать их как вредные «троянские» программы: отсутствие предупреждения об инсталляции и запуске. При запуске такая программа устанавливает себя в систему и затем следит за ней, при этом пользователю не выдается никаких сообщений о действиях программы в системе. Чаще всего ссылка на такую программу отсутствует в списке активных приложений. В результате пользователь может и не знать о ее присутствии в системе, в то время как его компьютер открыт для удаленного управления.

Внедренные в операционную систему утилиты скрытого управления позволяют делать с компьютером все что в них заложил их автор: принимать/отсылать файлы, запускать и уничтожать их, выводить сообщения, стирать информацию, перезагружать компьютер и

т.д. в результате эти программы могут быть использованы для обнаружения и передачи конфиденциальной информации, для запуска вирусов, уничтожения данных и т.п.

«Intended»-вирусы. К таким вирусам относятся программы, которые, на первый взгляд, являются стопроцентными вирусами, но не способны размножаться по причине ошибок. Например, вирус, который при заражении не помещает в начало файла команду передачи управления на код вируса, либо записывает в нее неверный адрес своего кода, либо неправильно устанавливает адрес перехватываемого прерывания (в большинстве приводит к «зависанию» компьютера) и т. д. К категории «intended» также относятся вирусы, которые по приведенным выше причинам размножаются только один раз – из «авторской» копии. Заразив какой-либо файл, они теряют способность к дальнейшему размножению. Появляются «intended»-вирусы чаще всего из-за неумелой перекомпиляции какого-либо уже существующего вируса, либо по причине недостаточного знания языка программирования, либо по причине незнания технических тонкостей операционной системы.

Конструкторы вирусов. К данному виду «вредных» программ относятся утилиты, предназначенные для изготовления новых компьютерных вирусов. Известны конструкторы вирусов для DOS, Windows и макровирусов. Они позволяют генерировать исходные тексты вирусов, объектные модули, и/или непосредственно зараженные файлы. Некоторые конструкторы снабжены стандартным оконным интерфейсом, где при помощи системы меню можно выбрать тип вируса, поражаемые объекты (COM и/или EXE), наличие или отсутствие самошифровки, противодействие отладчику, внутренние текстовые строки, выбрать эффекты, сопровождающие работу вируса, и т. п.

Полиморфные генераторы. Полиморфик-генераторы, как и конструкторы вирусов, не являются вирусами в прямом смысле этого слова, поскольку в их алгоритм не закладываются функции размножения, т. е. открытия, закрытия и записи в файлы, чтения и записи секторов и т. д. Главной функцией подобного рода программ является шифрование тела вируса и генерация соответствующего расшифровщика. Обычно полиморфные генераторы распространяются в виде файла-архива. Основным файлом в архиве любого генератора является объектный модуль, содержащий этот генератор.

2.3. Антивирусные программы

Одним из наиболее эффективных способов борьбы с вирусами является использование антивирусного программного обеспечения. ***Антивирусная программа*** – программа, предназначенная для поиска, обнаружения, классификации и удаления компьютерного вируса и вирусоподобных программ.

Вместе с тем, необходимо признать, что не существует антивирусов, гарантирующих стопроцентную защиту от вирусов, поскольку на любой алгоритм антивируса всегда можно предложить новый алгоритм вируса, невидимого для этого антивируса.

При работе с антивирусными программами необходимо знать некоторые понятия:

- «Ложное срабатывание» – детектирование вируса в незараженном объекте (файле, секторе или системной памяти).
- «Пропуск вируса» – недетектирование вируса в зараженном объекте.
- «Сканирование по запросу» – поиск вирусов по запросу пользователя. В этом режиме антивирусная программа неактивна до тех пор, пока не будет вызвана пользователем из командной строки, командного файла или программы-расписания.
- «Сканирование на лету» – постоянная проверка на вирусы объектов, к которым происходит обращение (запуск, открытие, создание и т. п.). В этом режиме антивирус постоянно активен, он присутствует в памяти «резидентно» и проверяет объекты без запроса пользователя.

Классификация антивирусных программ

Самыми популярными и эффективными антивирусными программами являются антивирусные сканеры, CRC-сканеры (ревизоры). Существуют также антивирусы блокировщики и иммунизаторы.

Сканеры. Принцип работы антивирусных сканеров основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых (неизвестных сканеру) вирусов. Для поиска известных вирусов используются так называемые «маски». Маской вируса является некоторая постоянная последовательность кода, специфичная для этого конкретного вируса. Если вирус не содержит постоянной маски или длина этой маски недостаточно велика, то

используются другие методы. Примером такого метода является алгоритмический язык, описывающий все возможные варианты кода, которые могут встретиться при заражении подобного типа вирусом. Такой подход используется некоторыми антивирусами для детектирования полиморфик-вирусов.

Во многих сканерах используются также алгоритмы «эвристического сканирования», т. е. анализ последовательности команд в проверяемом объекте, набор некоторой статистики и принятие решения для каждого проверяемого объекта. Поскольку эвристическое сканирование является во многом вероятностным методом поиска вирусов, то на него распространяются многие законы теории вероятностей. Например, чем выше процент обнаруживаемых вирусов, тем больше количество ложных срабатываний.

Сканеры также можно разделить на две категории – «универсальные» и «специализированные». Универсальные сканеры рассчитаны на поиск и обезвреживание всех типов вирусов вне зависимости от операционной системы, на работу в которой рассчитан сканер. Специализированные сканеры предназначены для обезвреживания ограниченного числа вирусов или только одного их класса, например макровирусов.

Сканеры также делятся на «резидентные» (мониторы), производящие сканирование «на лету», и «нерезидентные», обеспечивающие проверку системы только по запросу. Как правило, «резидентные» сканеры обеспечивают более надежную защиту системы, поскольку они немедленно реагируют на появление вируса, в то время как «нерезидентный» сканер способен опознать вирус только во время своего очередного запуска.

К достоинствам сканеров всех типов относится их универсальность, к недостаткам – размеры антивирусных баз, которые сканерам приходится хранить и пополнять, и относительно небольшая скорость поиска вирусов.

CRC-сканеры. Принцип работы CRC-сканеров основан на подсчете CRC-сумм (контрольных сумм) для присутствующих на диске файлов/системных секторов. Эти CRC-суммы затем сохраняются в базе данных антивируса, как, впрочем, и некоторая другая информация: длины файлов, даты их последней модификации и т. д. При последующем запуске CRC-сканеры сверяют данные, содержащиеся в базе данных, с реально подсчитанными значениями. Если информация о файле, записанная в базе данных, не совпадает с

реальными значениями, то CRC-сканеры сигнализируют о том, что файл был изменен или заражен вирусом.

CRC-сканеры, использующие «анти-стелс» алгоритмы, реагируют практически на 100 % вирусов сразу после появления изменений на компьютере. Характерный недостаток этих антивирусов заключается в невозможности обнаружения вируса с момента его появления и до тех пор, пока не будут произведены изменения на компьютере. CRC-сканеры не могут определить вирус в новых файлах (в электронной почте, на дискетах, в восстанавливаемых файлах или при распаковке файлов из архива), поскольку в их базах данных отсутствует информация об этих файлах.

Блокировщики. Антивирусные блокировщики – это резидентные программы, перехватывающие «вирусоопасные» ситуации и сообщающие об этом пользователю. К «вирусоопасным» относятся вызовы на открытие для записи в выполняемые файлы, запись в загрузочный сектор диска и др., которые характерны для вирусов в моменты их размножения.

К достоинствам блокировщиков относится их способность обнаруживать и блокировать вирус на самой ранней стадии его размножения, что, кстати, бывает очень полезно в случаях, когда давно известный вирус постоянно активизируется.

Иммунизаторы. Иммунизаторы делятся на два типа: иммунизаторы, сообщающие о заражении, и иммунизаторы, блокирующие заражение каким-либо типом вируса.

Факторы, определяющие качество антивирусных программ

Качество антивирусной программы определяется несколькими факторами, перечислим их по степени важности:

- Надежность и удобство работы – отсутствие «зависаний» антивируса и прочих технических проблем, требующих от пользователя специальной подготовки.
- Качество обнаружения вирусов всех распространенных типов, сканирование внутри файлов-документов/таблиц, упакованных и архивированных файлов. Отсутствие «ложных срабатываний». Возможность лечения зараженных объектов.
- Существование версий антивируса под все популярные платформы (DOS, Windows, Linux и т. д.).
- Возможность сканирования «на лету».

- Существование серверных версий с возможностью и администрирования сети.
- Скорость работы.

2.4. Профилактика компьютерных вирусов

Одним из методов борьбы с вирусами является, как и в медицине, своевременная профилактика. Компьютерная профилактика предполагает соблюдение правил («компьютерной гигиены»), позволяющих значительно снизить вероятность заражения вирусом и потери каких-либо данных. Профилактика компьютерных вирусов начинается с выявления путей проникновения вируса в компьютер и компьютерные сети.

Характеристика путей проникновения вирусов в компьютеры

Рассмотрим основные пути проникновения вирусов в компьютеры пользователей:

1. Глобальные сети – электронная почта.
2. Электронные конференции, файл-серверы ftp.
3. Пиратское программное обеспечение.
4. Локальные сети.
5. Персональные компьютеры «общего пользования».
6. Сервисные службы.

Глобальные сети – электронная почта. Основным источником вирусов на сегодняшний день является глобальная сеть Интернет. Наибольшее число заражений вирусом происходит при обмене электронными письмами через почтовые серверы E-mail. Пользователь получает электронное письмо с вирусом, который активизируется (причем, как правило, незаметно для пользователя) после просмотра файла-вложения электронного письма. После этого вирус (стелс) выполняет свои функции. В первую очередь, вирус «заботится» о своем размножении, для этого формируются электронные письма от имени пользователя по всем адресам адресной книги. Далее идет цепная реакция.

Локальные сети. Другой путь «быстрого заражения» – локальные сети. Если не принимать необходимых мер защиты, то зараженная рабочая станция при входе в сеть заражает один или нескольких служебных файлов на сервере. Далее пользователи при очередном

подключении к сети запускают зараженные файлы с сервера, и вирус таким образом получает доступ на компьютеры пользователей.

Персональные компьютеры «общего пользования». Опасность представляют также компьютеры, установленные в учебных заведениях. Если один из студентов принес на своих дискетах вирус и заразил какой-либо учебный компьютер, то очередной вирус будет гулять по всему учебному заведению, включая домашние компьютеры студентов и сотрудников.

Пиратское программное обеспечение. Нелегальные копии программного обеспечения, как это было всегда, являются одной из основных «зон риска». Часто пиратские копии содержат файлы, зараженные самыми разнообразными типами вирусов. Необходимо помнить, что низкая стоимость программы может дорого обойтись при потере данных.

Сервисные службы. Достаточно редко, но до сих пор вполне реально заражение компьютера вирусом при его ремонте или профилактическом осмотре в сервисных центрах.

Правила защиты от компьютерных вирусов

Учитывая возможные пути проникновения вирусов, приведем основные правила защиты от вирусов.

Внимательно относитесь к программам и документам, которые получаете из глобальных сетей. Перед тем, как запустить файл на выполнение или открыть документ/таблицу, обязательно проверьте его на наличие вирусов.

Используйте специализированные антивирусы для проверки «на лету» (например, SpIDer Guard из пакета Dr. Web и др.) всех файлов, приходящих по электронной почте (и из Интернета в целом).

Для уменьшения риска «заразить» файл на сервере администраторам сетей следует активно использовать стандартные возможности защиты сети, такие как: ограничение прав пользователей; установку атрибутов «только на чтение» или «только на запуск» для всех выполняемых файлов (к сожалению, это не всегда оказывается возможным) и т. д.

Регулярно проверяйте сервер обычными антивирусными программами, для удобства и системности используйте планировщики заданий.

Целесообразно запустить новое программное обеспечение на тестовом компьютере, не подключенном к общей сети.

Используйте лицензионное программное обеспечение, приобретенное у официальных продавцов.

Дистрибутивы копий программного обеспечения (в том числе копий операционной системы) необходимо хранить на защищенных от записи дисках.

Пользуйтесь только хорошо зарекомендовавшими себя источниками программ и прочих файлов.

Постоянно обновляйте вирусные базы используемого антивируса.

Старайтесь не запускать непроверенные файлы, в том числе полученные из компьютерной сети. Перед запуском новых программ обязательно проверьте их одним или несколькими антивирусами.

Ограничьте (по возможности) круг лиц, допущенных к работе на конкретном компьютере.

Пользуйтесь утилитами проверки целостности информации. Такие утилиты сохраняют в специальных базах данных информацию о системных областях дисков (или целиком системные области) и информацию о файлах (контрольные суммы, размеры, атрибуты, даты последней модификации файлов и т. д.).

Периодически сохраняйте на внешнем носителе файлы, с которыми ведется работа.

При работе с Word/Excel включите защиту от макросов, которая сообщает о присутствии макроса в открываемом документе и предоставляет возможность запретить этот макрос. В результате макрос не только не выполняется, но и не виден средствами Word/Excel.

Обнаружение макровируса

Характерными проявлениями макровирусов являются:

- Word: невозможность конвертирования зараженного документа Word в другой формат;
- Word: зараженные файлы имеют формат Template (шаблон), поскольку при заражении Word-вирусы конвертируют файлы из формата Word Document в Template;
- Excel/Word: в STARTUP (Автозагрузка)-каталоге присутствуют «посторонние» файлы;
- Excel: наличие в Книге (Book) лишних и скрытых Листов (Sheets).

Для проверки системы на предмет наличия вируса можно использовать пункт меню Сервис/макрос. Если обнаружены «чужие макросы», то они могут принадлежать вирусу. Однако этот метод не

работает в случае стелс-вирусов, которые запрещают работу этого пункта меню, что, в свою очередь, является достаточным основанием считать систему зараженной.

Многие вирусы имеют ошибки или некорректно работают в различных версиях Word/Excel, в результате чего Word/Excel выдают сообщения об ошибке.

Если такое сообщение появляется при редактировании нового документа или таблицы и при этом заведомо не используются какие-либо пользовательские макросы, то это также может служить признаком заражения системы.

Сигналом о вирусе являются и изменения в файлах и системной конфигурации Word, Excel и Windows. Многие вирусы тем или иным образом меняют пункты меню, разрешают или запрещают некоторые функции, устанавливают на файлы пароль при их заражении. Большое количество вирусов создает новые секции и/ или опции в файле конфигурации Windows (WIN. INI).

Естественно, что к проявлениям вируса относятся такие очевидные факты, как появление сообщений или диалогов с достаточно странным содержанием или на языке, не совпадающем с языком установленной версии Word/Excel.

Контрольные вопросы по разделу №2

1. Каковы характерные черты компьютерных вирусов?
2. Дайте определение программного вируса.
3. Какой вид вирусов наиболее распространяемый в распределенных вычислительных сетях? Почему?
4. Перечислите классификационные признаки компьютерных вирусов.
5. В чем особенности резидентных вирусов?
6. Перечислите деструктивные возможности компьютерных вирусов.
7. Поясните самошифрование и полиморфичность как свойства компьютерных вирусов.
8. Перечислите виды «вирусоподобных» программ.
9. Поясните механизм функционирования «троянской программы» (логической бомбы).
10. Поясните понятия «сканирование на лету» и «сканирование по запросу».

11. Перечислите виды антивирусных программ.
12. Охарактеризуйте антивирусные сканеры.
13. В чем особенности эвристических сканеров?
14. Какие факторы определяют качество антивирусной программы?
15. Перечислите наиболее распространенные пути заражения компьютеров вирусами.
16. Перечислите основные правила защиты от компьютерных вирусов, получаемых не из вычислительных сетей.
17. Характерные черты макровируса.
18. Как проверить систему на наличие макровируса?
19. Является ли наличие скрытых листов в Excel признаком заражения макровирусом?

3. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В КОМПЬЮТЕРНЫХ СЕТЯХ

3.1. Общие сведения о безопасности в компьютерных сетях

Основной особенностью любой сетевой системы является то, что ее компоненты распределены в пространстве и связь между ними физически осуществляется при помощи сетевых соединений (коаксиальный кабель, витая пара, оптоволокно и т. п.) и программно при помощи механизма сообщений. При этом все управляющие сообщения и данные, пересылаемые между объектами распределенной вычислительной системы, передаются по сетевым соединениям в виде пакетов обмена [10].

Сетевые системы характерны тем, что наряду с локальными угрозами, осуществляемыми в пределах одной компьютерной системы, к ним применим специфический вид угроз, обусловленный распределенностью ресурсов и информации в пространстве. Это так называемые сетевые или удаленные угрозы. Они характерны, во-первых, тем, что злоумышленник может находиться за тысячи километров от атакуемого объекта, и, во-вторых, тем, что нападению может подвергаться не конкретный компьютер, а информация, передающаяся по сетевым соединениям. С развитием локальных и глобальных сетей именно удаленные атаки становятся лидирующими как по количеству попыток, так и по успешности их применения и, соответственно, обеспечение безопасности вычислительных сетей с точки зрения противостояния удаленным атакам приобретает первостепенное значение. Специфика распределенных вычислительных систем состоит в том, что если в локальных вычислительных сетях наиболее частыми являются угрозы раскрытия и целостности, то в сетевых системах на первое место выходит угроза отказа в обслуживании.

Удаленная угроза – потенциально возможное информационное разрушающее воздействие на распределенную вычислительную сеть, осуществляемая программно по каналам связи. Это определение охватывает обе особенности сетевых систем – распределенность компьютеров и распределенность информации. Поэтому при рассмотрении вопросов информационной безопасности вычислительных сетей рассматриваются два подвида удаленных угроз – это ***удаленные угрозы на инфраструктуру и протоколы сети и***

удаленные угрозы на телекоммуникационные службы. Первые используют уязвимости в сетевых протоколах и инфраструктуре сети, а вторые – уязвимости в телекоммуникационных службах.

Цели сетевой безопасности могут меняться в зависимости от ситуации, но основные цели обычно связаны с обеспечением составляющих «информационной безопасности»:

1) целостности данных;
2) конфиденциальности данных;
3) доступности данных.

Целостность данных – одна из основных целей информационной безопасности сетей - предполагает, что данные не были изменены, подменены или уничтожены в процессе их передачи по линиям связи, между узлами вычислительной сети. Целостность данных должна гарантировать их сохранность как в случае злонамеренных действий, так и случайностей. Обеспечение целостности данных является обычно одной из самых сложных задач сетевой безопасности.

Конфиденциальность данных – вторая главная цель сетевой безопасности. При информационном обмене в вычислительных сетях большое количество информации относится к конфиденциальной, например, личная информация пользователей, учетные записи (имена и пароли), данные о кредитных картах и др.

Доступность данных – третья цель безопасности данных в вычислительных сетях. Функциями вычислительных сетей являются совместный доступ к аппаратным и программным средствам сети и совместный доступ к данным. Нарушение информационной безопасности как раз и связана с невозможностью реализации этих функций.

В локальной сети должны быть доступны: принтеры, серверы, рабочие станции, данные пользователей и др.

В глобальных вычислительных сетях должны быть доступны информационные ресурсы и различные сервисы, например, почтовый сервер, сервер доменных имен, web-сервер и др.

При рассмотрении вопросов, связанных с информационной безопасностью, в современных вычислительных сетях необходимо учитывать следующие факторы:

- глобальную связанность;
- разнородность корпоративных информационных систем;
- распространение технологии «клиент/сервер».

Применительно к системам связи глобальная связанность означает, что речь идет о защите сетей, пользующихся внешними сервисами, основанными на протоколах TCP/IP, и предоставляющих аналогичные сервисы вовне. Весьма вероятно, что внешние сервисы находятся в других странах, поэтому от средств защиты в данном случае требуется следование стандартам, признанным на международном уровне. Национальные границы, законы, стандарты не должны препятствовать защите потоков данных между клиентами и серверами.

Из факта глобальной связанности вытекает также меньшая эффективность мер физической защиты, общее усложнение проблем, связанных с защитой от несанкционированного доступа, необходимость привлечения для их решения новых программно-технических средств, например, межсетевых экранов.

Разнородность аппаратных и программных платформ требует от изготовителей средств защиты соблюдения определенной технологической дисциплины. Важны не только чисто защитные характеристики, но и возможность встраивания этих систем в современные корпоративные информационные структуры. Если, например, продукт, предназначенный для криптографической защиты, способен функционировать исключительно на платформе Wintel (Windows+Intel), то его практическая применимость вызывает серьезные сомнения.

Корпоративные информационные системы оказываются разнородными еще в одном важном отношении – в разных частях этих систем хранятся и обрабатываются данные разной степени важности и секретности.

Использования технологии «клиент/сервер» с точки зрения информационной безопасности имеет следующие особенности:

- каждый сервис имеет свою трактовку главных аспектов информационной безопасности (доступности, целостности, конфиденциальности);
- каждый сервис имеет свою трактовку понятий субъекта и объекта;
- каждый сервис имеет специфические угрозы;
- в каждый сервис нужно по-своему администрировать;
- средства безопасности в каждый сервис нужно встраивать по-особому.

Специфика средств защиты в компьютерных сетях

Особенности вычислительных сетей и, в первую очередь, глобальных, предопределяют необходимость использования специфических методов и средств защиты, например:

- защита подключений к внешним сетям;
- защита корпоративных потоков данных, передаваемых по открытым сетям;
- защита потоков данных между клиентами и серверами;
- обеспечение безопасности распределенной программной среды;
- защита важнейших сервисов (в первую очередь Web-сервиса);

В последнее время все четче просматривается незащищенность вычислительных сетей от глобальных атак.

3.2. Сетевые модели передачи данных

Понятие протокола передачи данных

Обмен информацией между ЭВМ на больших расстояниях всегда казался более важной задачей, чем локальный обмен. Поэтому ему уделялось больше внимания и, соответственно, велось большее финансирование во многих странах. Один из немногих открытых проектов по исследованию вычислительных сетей, финансировавшийся военным ведомством США, известен под названием сеть ARPA - Advanced Research Projects Agency. С самого начала в рамках этого проекта велись работы по объединению ресурсов многих вычислительных машин различного типа. В 1960 – 1970-е годы многие результаты, полученные при эксплуатации сети ARPA, были опубликованы в открытой печати. Это обстоятельство, а также тот факт, что почти все страны занялись практически слепым копированием не только аппаратной архитектуры американских машин, но и базового программного обеспечения, обусловили сильное влияние сети ARPA на многие другие сети, именно поэтому принято считать, что сеть ARPA является предшественницей знаменитой всемирной компьютерной сети Интернет.

Основной задачей сетевой общественности явилась разработка протоколов обмена информацией. Эта задача совершенно справедливо представлялась важнейшей, поскольку настоятельно требовалось заставить понимать друг друга компьютеры, обладавшие различной

архитектурой и программным обеспечением. Первоначально разработчики многочисленных корпоративных сетей договаривались о внутренних протоколах информационного обмена в своих сетях. Никакой стандартизации не было. Но уже в 70-е годы специалистам стало совершенно ясно, что стандартизация необходима и неизбежна. В эти годы шел бурный процесс создания многочисленных национальных и международных комитетов и комиссий по стандартизации программных и аппаратных средств в области вычислительной техники и информационного обмена.

В общем случае ***протокол сетевого обмена информацией*** можно определить как перечень форматов передаваемых блоков данных, а также правил их обработки и соответствующих действий. Другими словами, протокол обмена данными – это подробная инструкция о том, какого типа информация передается по сети, в каком порядке обрабатываются данные, а также набор правил обработки этих данных.

Человек – оператор компьютера, включенного в сеть, тем или иным способом, например, с помощью программ-приложений, формирует и передает по сети сообщения, предназначенные для других людей или компьютеров. В ответ он также ожидает поступления сообщения. В этом смысле сообщение представляет собой логически законченную порцию информации, предназначенную для потребления конечными пользователями – человеком или прикладной программой. Например, это может быть набор алфавитно-цифровой и графической информации на экране или файл целиком. Сейчас сообщения неразрывно связывают с прикладным уровнем или, как его еще называют, уровнем приложений сетевых протоколов.

Сообщения могут проходить довольно сложный путь по сетям, стоять в очередях на передачу или обработку, в том числе не доходить до адресата, о чем отправитель также должен быть уведомлен специальным сообщением.

Первоначально вычислительные сети были сетями коммутации сообщений. Это было оправдано, пока сообщения были сравнительно короткими. Но параллельно с этим всегда существовали задачи передачи на расстояние больших массивов информации. Решение этой задачи в сетях с коммутацией сообщений является неэффективным, поскольку длины сообщений имеют большой разброс – от очень коротких до очень длинных, что характерно для компьютерных сетей.

В связи с этим было предложено разбивать длинные сообщения на части (пакеты) и передавать сообщения не целиком, а пакетами, вставляя в промежутках пакеты других сообщений. На месте назначения сообщения собираются из пакетов. Короткие сообщения при этом были вырожденным случаем пакета, равного сообщению.

В настоящее время почти все сети в мире являются сетями коммутации пакетов.

Принципы организации обмена данными в вычислительных сетях

Существуют два принципа организации обмена данными:

- установление виртуального соединения с подтверждением приема каждого пакета;
- передача датаграмм.

Установление виртуального соединения или создание виртуального канала является более надежным способом обмена информацией. Поэтому он более предпочтителен при передаче данных на большие расстояния и по физическим каналам, в которых возможны помехи. При виртуальном соединении пункт приема информации уведомляет отправителя о правильном или неправильном приеме каждого пакета. Если какой-то пакет принят неправильно, отправитель повторяет его передачу. Так длится до тех пор, пока все сообщение не будет успешно передано. На время передачи информации между двумя пунктами коммутируется канал, подобный каналу при телефонном разговоре. Виртуальным его называют потому, что в отличие от телефонного коммутированного канала обмен информацией может идти по различным физическим путям даже в процессе передачи одного сообщения.

Термин ***датаграмма*** образован по аналогии с термином телеграмма. Аналогия заключается том, что короткие пакеты - собственно датаграммы – пересылаются адресату без подтверждения получения каждого из них. О получении всего сообщения целиком должна уведомить целевая программа.

Транспортный протокол TCP и модель TCP/IP

За время развития вычислительных сетей было предложено и реализовано много протоколов обмена данными, самыми удачными из которых явились семейство протоколов TCP/IP (Transmission

Control Protocol/ Internet Protocol – протокол управления передачей/ межсетевой протокол).

TCP/IP – это набор протоколов, состоящий из следующих компонентов:

- ***межсетевой протокол (Internet Protocol)***, обеспечивающий адресацию в сетях (IP-адресацию);
- ***межсетевой протокол управления сообщениями*** (***Internet Control Message Protocol*** – ***ICMP***), который обеспечивает низкоуровневую поддержку протокола IP, включая такие функции, как сообщения об ошибках, квитанции, содействие в маршрутизации и т. п.;
- ***протокол разрешения адресов*** (***Address Resolution Protocol*** – ARP), выполняющий преобразование логических сетевых адресов в аппаратные, а также обратный ему RARP (Reverse ARP);
- ***протокол пользовательских датаграмм*** (***User Datagram Protocol*** – ***UPD***);
- ***протокол управления передачей*** (***Transmission Control Protocol*** – ***TCP***).

Протокол UDP обеспечивает передачу пакетов без проверки доставки, в то время как протокол TCP требует установления виртуального канала и соответственно подтверждения доставки пакета с повтором в случае ошибки.

Этот набор протоколов образует самую распространенную модель сетевого обмена данными, получившую название TCP/IP. Модель TCP/IP иерархическая и включает четыре уровня:

Уровень	Название	Функция
4	Прикладной	Приложения пользователей, создание сообщений
3	Транспортный	Доставка данных между программами в сети
2	Сетевой	Адресация и маршрутизация
I	Канальный	Сетевые аппаратные средства и их драйверы

Прикладной уровень определяет способ общения пользовательских приложений. В системах «клиент-сервер» приложение-клиент должно знать, как посылать запрос, а приложение-сервер должно знать, как ответить на запрос. Этот уровень обеспечивает такие протоколы, как HTTP, FTP, Telnet.

Транспортный уровень позволяет сетевым приложениям получать сообщения по строго определенным каналам с конкретными параметрами.

На ***сетевом уровне*** определяются адреса включенных в сеть компьютеров, выделяются логические сети и подсети, реализуется маршрутизация между ними.

На ***канальном уровне*** определяется адресация физических интерфейсов сетевых устройств, например, сетевых плат. К этому уровню относятся программы управления физическими сетевыми устройствами, так называемые драйверы.

Как уже отмечалось ранее, в сетях с коммутацией пакетов, а модель TCP/IP относится к таким, для передачи по сети сообщение (сформированное на прикладном уровне) разбивается на пакеты или датаграммы. Пакет или датаграмма – это часть сообщения с добавленным заголовком пакета или датаграммы.

На транспортном уровне к полезной информации добавляется заголовок – служебная информация. Для сетевого уровня полезной информацией является уже пакет или датаграмма транспортного уровня. К ним добавляется заголовок сетевого уровня.

Полученный блок данных называется IP-пакетом. Полезной нагрузкой для канального уровня является уже IP-пакет. Здесь перед передачей по каналу к нему добавляются собственный заголовок и еще завершитель. Получившийся блок называется кадром. Он и передается по сети.

Переданный по сети кадр в пункте назначения преобразуется в обратном порядке, проходя по уровням модели снизу вверх.

3.3. Модель взаимодействия открытых систем OS1/ISO

Сравнение сетевых моделей передачи данных TCP/IP и OSI/ISO

В конце 80-х годов наблюдался подлинный бум, вызванный разработкой Международной организации по стандартизации коммуникационных протоколов – (International Standard Organization). Разработанная ISO спецификация, названная моделью взаимодействия открытых систем (OSI – Open Systems Interconnection), заполонила научные публикации. Казалось, что эта модель займет первое место и оттеснит широко распространившийся TCP/IP. Но этого не произошло. Одной из причин явилась тщательная проработка протоколов TCP/IP, их функциональность и открытость к наращиванию функциональных возможностей, хотя к настоящему времени достаточно очевидно, что они имеют и множество недостатков. Приведем сравнительную схему уровневых моделей протоколов OSI и TCP/IP (рис. 1).

7	Прикладной уровень
6	Представительный уровень
5	Сеансовый уровень
4	Транспортный уровень
3	Сетевой уровень
2	Канальный уровень
1	Физический уровень

4	Прикладной уровень
3	Транспортный уровень
2	Межсетевой уровень
1	Сетевой уровень

Рис. 1. Модели OSI и TCP/IP

Многоуровневое представление средств сетевого взаимодействия имеет свою специфику, связанную с тем, что в процессе обмена сообщениями участвуют две стороны, то есть в данном случае необходимо организовать согласованную работу двух «иерархий», работающих на разных компьютерах. Оба участника сетевого обмена должны принять множество соглашений. Например, они должны согласовать уровни и форму электрических сигналов, способ определения длины сообщений, договориться о методах контроля достоверности и т. п. Другими словами, соглашения должны быть приняты для всех уровней, начиная от самого низкого

– уровня передачи битов – до самого высокого, реализующего сервис для пользователей сети.

Распределение функций безопасности по уровням модели OSI/ISO

Модель взаимодействия открытых систем (Open System Interconnection, OSI) определяет различные уровни взаимодействия систем в сетях с коммутацией пакетов, дает им стандартные имена и указывает, какие функции должен выполнять каждый уровень.

Модель OSI была разработана на основании большого опыта, полученного при создании компьютерных сетей, в основном глобальных, в 70-е годы. В модели OSI средства взаимодействия делятся на семь уровней: прикладной, представительный, сеансовый, транспортный, сетевой, канальный и физический. Каждый уровень имеет дело с определенным аспектом взаимодействия сетевых устройств.

Физический уровень имеет дело с передачей ***битов*** по физическим каналам связи, таким, как коаксиальный кабель, витая пара, оптоволоконный кабель или цифровой территориальный канал. К этому уровню имеют отношение характеристики физических сред передачи данных, такие как полоса пропускания, помехозащищенность, волновое сопротивление и другие.

Одной из задач ***канального уровня*** является проверка доступности среды передачи. Другая задача канального уровня – реализация механизмов обнаружения и коррекции ошибок. Для этого на канальном уровне биты группируются в наборы, называемые кадрами (frames). Канальный уровень обеспечивает корректность передачи каждого кадра.

Сетевой уровень служит для образования единой транспортной системы, объединяющей несколько сетей, причем эти сети могут использовать различные принципы передачи сообщений между конечными узлами и обладать произвольной структурой связей. Внутри одной сети доставка данных обеспечивается канальным уровнем, а вот доставкой данных между различными сетями занимается сетевой уровень, который и поддерживает возможность правильного выбора ***маршрута*** передачи сообщения даже в том случае, когда структура связей между составляющими сетями имеет характер, отличный от принятого в протоколах канального уровня.

Сети соединяются между собой специальными устройствами, называемыми маршрутизаторами. ***Маршрутизатор*** – это устройство, которое собирает информацию о топологии межсетевых соединений и пересылает пакеты сетевого уровня в сеть назначения. Чтобы передать сообщение от отправителя, находящегося в одной сети, получателю, находящемуся в другой сети, нужно совершить некоторое количество транзитных передач между сетями.

Транспортный уровень обеспечивает приложениям или верхним уровням стека – прикладному и сеансовому - передачу данных с той степенью надежности, которая им требуется. Модель OSI определяет пять классов сервиса, предоставляемых транспортным уровнем. Эти виды сервиса отличаются качеством предоставляемых услуг: срочностью, возможностью восстановления прерванной связи, наличием средств мультиплексирования нескольких соединений между различными прикладными протоколами через общий транспортный протокол, а главное – способностью к обнаружению и исправлению ошибок передачи, таких как искажение, потеря и дублирование пакетов.

Сеансовый уровень обеспечивает управление диалогом: фиксирует, какая из сторон является активной в настоящий момент, предоставляет средства синхронизации. Последние позволяют вставлять контрольные точки в длинные передачи, чтобы в случае отказа можно было вернуться назад к последней контрольной точке, а не начинать все сначала. На практике немногие приложения используют сеансовый уровень, и он редко реализуется в виде отдельных протоколов, хотя функции этого уровня часто объединяют с функциями прикладного уровня и реализуют в одном протоколе.

Представительный уровень имеет дело с формой представления передаваемой по сети информации, не меняя при этом ее содержания. За счет уровня представления информация, передаваемая прикладным уровнем одной системы, всегда понятна прикладному уровню другой системы. С помощью средств данного уровня протоколы прикладных уровней могут преодолеть синтаксические различия в представлении данных или же различия в кодах символов, например, в кодах ASCII и EBCDIC. На этом уровне может выполняться шифрование и дешифрование данных, благодаря которому секретность обмена данными обеспечивается сразу для всех прикладных служб. Примером такого протокола является протокол

Secure Socket Layer (SSL), который обеспечивает секретный обмен сообщениями для протоколов прикладного уровня стека TCP/IP.

Прикладной уровень – это набор разнообразных протоколов, с помощью которых пользователи сети получают доступ к разделяемым ресурсам, таким как файлы, принтеры или гипертекстовые Web-страницы, а также организуют совместную работу, например, с помощью протокола электронной почты. Единица данных, которой оперирует прикладной уровень, обычно называется сообщением.

Функции всех уровней модели OSI могут быть отнесены к одной из двух групп: либо к функциям, зависящим от конкретной технической реализации сети, либо к функциям, ориентированным на работу с приложениями.

Три нижних уровня – физический, канальный и сетевой – являются сетезависимыми, то есть протоколы этих уровней тесно связаны с технической реализацией сети и используемым коммуникационным оборудованием.

Три верхних уровня – прикладной, представительный и сеансовый – ориентированы на приложения и мало зависят от технических особенностей построения сети. На протоколы этих уровней не влияют какие бы то ни было изменения в топологии сети, замена оборудования или переход на другую сетевую технологию.

Транспортный уровень является промежуточным, он скрывает все детали функционирования нижних уровней от верхних. Это позволяет разрабатывать приложения, не зависящие от технических средств непосредственной транспортировки сообщений.

Столь подробное рассмотрение модели OSI/ISO связано с тем, что при разработке стандартов и спецификации по сетевой безопасности специалисты ориентируются на эту перспективную модель. Так, в «Общих критериях» приводится распределение функций безопасности по уровням эталонной семиуровневой модели OSI, показано в таблице 1.

Таблица 1

Распределение функций безопасности по уровням OSI/ISO

Функция безопасности	Уровень OSI						
	1	2	3	4	5	6	7
Аутентификация	-	-	+	+	-	-	+

Управление доступом	-	-	+	+	-	-	+
Конфиденциальность соединения	+	+	+	+	-	+	+
Конфиденциальность вне соединения	-	+	+	+	-	+	+
Избирательная конфиденциальность	-	-	-	-	-	+	+
Конфиденциальность трафика	+	-	+	-	-	-	+
Целостность с восстановлением	-	-	-	+	-	-	+
Целостность без восстановления	-	-	+	+	-	-	+
Избирательная целостность	-	-	-	-	-	-	+
Целостность вне соединения	-	-	+	+	-	-	+
Неотказуемость	-	-	-	-	-	-	+

"+" - данный уровень может предоставить функцию безопасности;

"-" - данный уровень не подходит для предоставления функции безопасности.

3.4. Адресация в глобальных сетях

Основы IP-протокола

Одной из главных проблем построения глобальных сетей является проблема адресации. С одной стороны, постоянное расширение глобальной сети Интернет привело к нехватке уникальных адресов для вновь подключаемых узлов. С другой стороны, система адресации в таких сетях должна быть защищена от возможного вмешательства злоумышленников, связанных с подменой адресов и реализацией обходных маршрутов передачи сообщений.

Адресация современного Интернета основана на протоколе IP (Internet Protocol), история которого неразрывно связана с транспортным протоколом TCP.

Концепция протокола IP представляет сеть как множество компьютеров (хостов), подключенных к некоторой интерсети. Интерсеть, в свою очередь, рассматривается как совокупность физических сетей, связанных маршрутизаторами. Физические объекты (хосты, маршрутизаторы, подсети) идентифицируются при помощи специальных IP-адресов. Каждый IP-адрес представляет собой

32-битовый идентификатор. Принято записывать IP-адреса в виде 4-х десятичных чисел, разделенных точками.

Для этого 32-х битовый IP-адрес разбивается на четыре группы по 8 бит (1 байт), после чего каждый байт двоичного слова преобразовывается в десятичное число по известным правилам. Например, IP-адрес:

10010011 10000111 00001110 11100101

преобразовывается указанным способом к следующему виду: 147.135.14.229.

Классы адресов вычислительных сетей

Каждый адрес является совокупностью двух идентификаторов: сети – NetID, и хоста – HostID. Все возможные адреса разделены на 5 классов, схема которых приведена на рисунке 2.

Из рисунка 2 видно, что классы сетей определяют как возможное количество этих сетей, так и число хостов в них. Практически используются только первые три класса:

Класс A определен для сетей с числом хостов до 16777216. Под поле NetID отведено 7 бит, под поле HostID – 24 бита.

Класс B используется для среднемасштабных сетей (NetID – 14 бит, HostID – 16 бит). В каждой такой сети может быть до 65536 хостов.

Класс C применяется для небольших сетей (NetID – 21 бит, HostID – 8 бит) с числом хостов до 255.

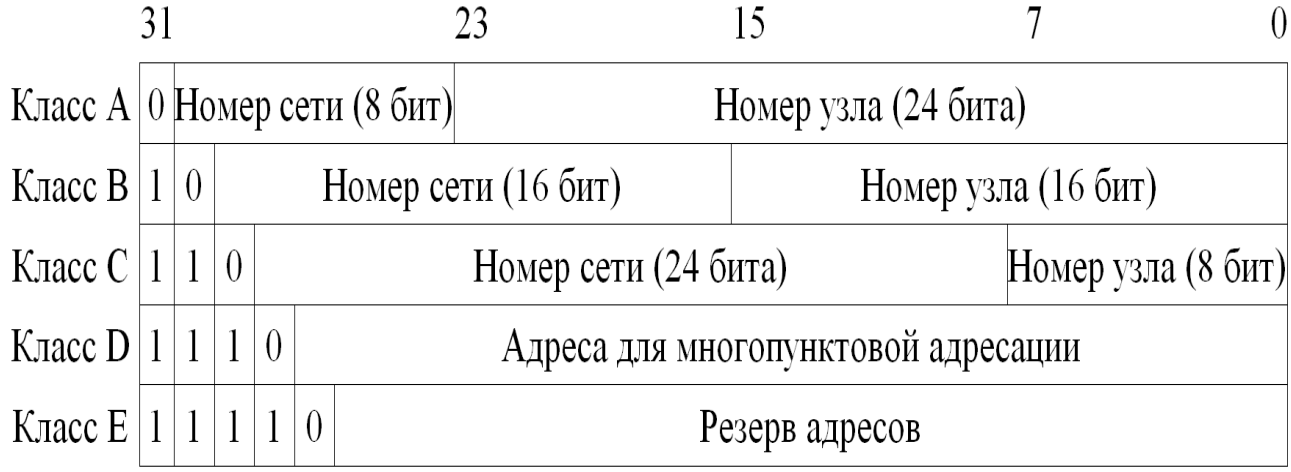

Рис. 2. Классы адресов

Система доменных имен

Постоянное расширение сети Internet привело к дефициту уникальных адресов для вновь подключаемых узлов. С другой стороны, система адресации в такой сети должна быть универсальной и удобной для пользователя. Последнее обстоятельство особенно было важно с началом использования ресурсов сети не только специалистами, но и неподготовленными пользователями, не владеющими тонкостями адресации в сети. Решающим аргументом для перехода к альтернативным способам адресации в сети, удобным для работы пользователей, было неудобство запоминания 32-х битового кода, идентифицирующего отдельный узел. Это неудобство проявилось сразу же, когда сеть использовалась узким кругом специалистов. Поэтому появилась альтернативные формы записи 32-х битового IP-адреса – десятичная (195.224.11.77) и шестнадцатеричная (0xffffff80) дот-нотации. Последняя форма записи особенно была удобной для программистов, часто применяющих шестнадцатеричный алфавит для записи кода программы.

Впоследствии с появлением в сети различных сервисов (электронная почта и другие службы), а также с увеличением числа узлов и такая форма записи оказалась неудобной, поскольку достаточно сложно запомнить несколько цифровых адресов, даже в десятичной дот-нотации. Это обусловило появление в сети ARPANET принципиально нового способа адресации, заключающегося в присвоении узлам сети доменного имени. В данном случае правильнее говорить о новом способе именования узлов сети, поскольку доменное имя не является логическим адресом, например, как IP-адрес или физическим адресом, как, например, шестибайтовый адрес сетевого интерфейса. Доменное имя – это только лишь удобная для пользователя форма идентификации узла вычислительной сети (сервис).

Домен – группа узлов сети (хостов), объединенных общим именем, которое для удобства несет определенную смысловую нагрузку. Например, домен «ru» объединяет узлы на территории России, а домен «sport» – узлы, относящиеся к спортивным организациям или содержащие информацию о спорте и т. д.

В более широком смысле под доменом понимается множество узлов вычислительной сети, которые администрируются и поддерживаются как одно целое.

Доменное имя – это уникальный алфавитно-цифровой идентификатор узла (состоит из символов ASCII-кода – букв от A до Z латинского алфавита и цифр от 0 до 9, также допускается дефис «-»).

Введение доменных имен поставило перед разработчиками задачу определения соответствия между доменным именем и логическим IP-адресом узла сети. Подобная задача разработчиками ARPANET была решена, когда для определения соответствия между логическим IP-адресом и физическим адресом сетевого интерфейса в пределах локальной сети были введены протоколы ARP и RARP. Однако для глобальной сети решение такой задачи является более сложным.

Первоначально, когда ARPANET состояла из небольшого числа узлов, соответствие между доменными именами и IP-адресами узлов перечислялось в одном файле (hosts.txt) в виде таблицы соответствия цифрового адреса имени машины.

Авторство создания этих таблиц принадлежит Джону Постелю. Именно он первым поддерживал файл hosts.txt, который можно было получить по FTP. Этот файл хранился в сетевом информационном центре Станфордского исследовательского института (SRI). Администраторы сетей передавали в SRI дополнения и изменения, происшедшие в конфигурации администрируемой ими сети. Периодически администраторы переписывали этот файл в свои системы.

В локальных сетях файлы hosts используются достаточно успешно до сих пор. Практически все операционные системы от различных версий Unix до Windows последних версий поддерживают эту систему соответствия IP-адресов именам хостов.

Пользователь для обращения к узлу мог использовать как IP-адрес узла, так и его имя. Процедура использования имени заключается в следующем: сначала по имени в файле hosts находят IP-адрес, а затем по IP-адресу устанавливают соединение с удаленным информационным ресурсом.

С ростом сети ARPANET это стало чрезвычайно затруднительно, поскольку файл увеличивался в размерах, а его пересылка по сети и хранение на каждом узле требовало значительных ресурсов. Однако главное неудобство заключалось в том, что такой способ не позволял оперативно учитывать все изменения в сети.

В 1984 году в сети ARPANET стала использоваться служба, получившая название системы доменных имен (Domain Name System – DNS). DNS была описана Полом Мокапетрисом в двух документах: RFC-882 и RFC-883 (позже эти документы были заменены на RFC-1034 и RFC-1035).

В соответствии с RFC-1034 и RFC-1035, описывающими DNS, роль доменного имени в процессе установки соединения осталась прежней. Это значит, что главное, для чего используется DNS служба, – это получение IP-адреса узла сети. Исходя из этого, любая реализация DNS является прикладным процессом, который работает над стеком протоколов межсетевого обмена TCP/IP. Таким образом, базовым элементом адресации в сетях TCP/IP с введением DNS остался IP-адрес, а доменное именование (система доменных имен) играет роль вспомогательного сервиса.

DNS состоит из трех основных частей:

- пространство (множество) доменных имен (domain name space);
- серверов доменных имен (domain name servers);
- клиентов DNS (Resolver).

Пространство доменных имен имеет вид дерева (иерархии) узлов, как показано на рисунке 3 и подчиняется следующим правилам (RFC-1034):

- имя корня – пустая строка, то есть полное имя обязательно завершается точкой[1];
- каждый узел дерева должен быть помечен простым именем, включающим допустимые символы;
- прописные и строчные буквы в доменных именах не различаются;
- допустимая длина простого имени не более 63 символов;
- доменные имена узлов в пределах одного домена должны быть уникальны;
- допускается применение одинаковых доменных имен в разных доменах, как показано на рисунке 3, где доменное имя «.mil» используется для обозначения домена первого уровня и домена второго уровня, являющегося поддоменом домена «.ru»;
- полное имя узла образуется из последовательности имени самого узла и всех имен доменов, которые с ним связаны (снизу вверх по соответствующей ветви дерева) до корня включительно, записываемых слева направо и разделяемых точками, например, как показано на рисунке 3, узлу «.Ekfacultet» соответствует следующее полное доменное имя «.Ekfacultet.urgi.krasnoyarsk.ru»;
- максимальная длина полного имени – 255 символов, включая точки;
- максимальное число уровней дерева – 127[2];

[1] В некоторых случаях, например, при записи почтовых адресов заключительная точка должна быть опущена.

- кроме полного (абсолютного) имени узла (FQDN, fully qualified domain name) допускается применение относительного (относительно некоторого опорного узла) имени, в этом случае завершающая точка отсутствует;
- поддерево доменных имен вместе со своим корневым узлом называется доменом (поддоменом), например, обозначенная на рисунке 3 ветвь относится к группе узлов («.Ekfacultet», «.Urfacultet», «.Phfacultet», «.Dizfacultet», «.Reefacultet») и под-Доменов («krasnoyarsk.» «.urgi»), входящих в домен «.ru», а все узлы, показанные на рисунке 6 на самом нижнем уровне, входят в домен (поддомен) третьего уровня «.urgi» и т. д.
- объединение узлов в домены является чисто логическим, то есть не зависящим ни от месторасположения, ни от IP-адреса, ни от способа маршрутизации.

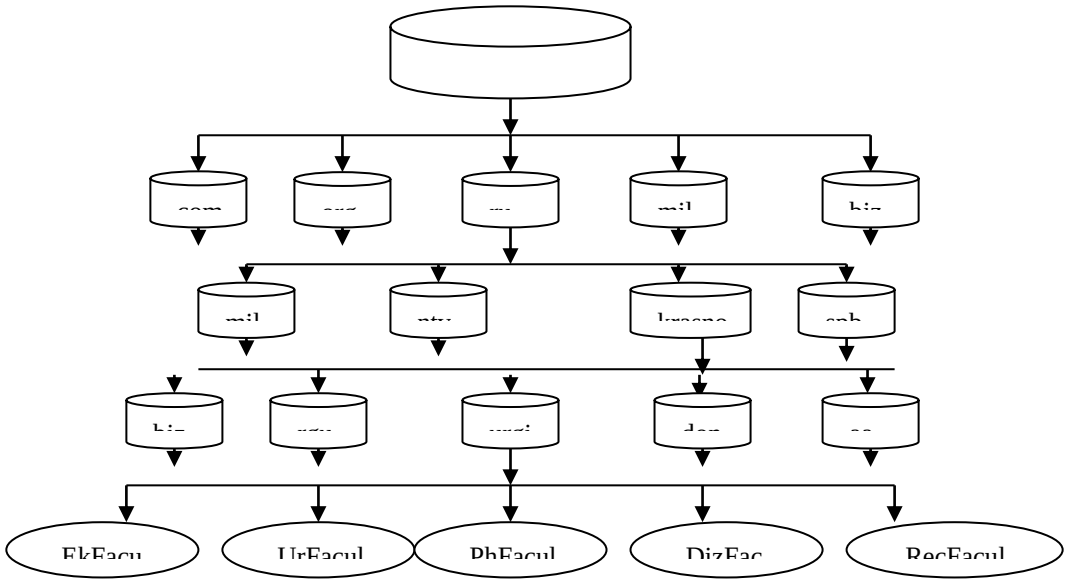

Рис. 3. Структура DNS

Полное доменное имя узла используется как ключевая информация для поиска IP-адреса узла в базе данных, содержащей таблицы соответствия доменных имен и логических адресов.

[2] На практике применение доменных имен с числом уровней более 3-х затруднительно для пользователя.

Корень – это множество все узлов Internet. Данное множество подразделяется на домены первого или верхнего уровня (top-level или TLD).

Корневой зоной Internet и системой корневых серверов управляет ICANN, в частности, ICANN делегирует (передает) права управления зонами первого уровня gTLD (generic top-level domains, домены верхнего организационного уровня) и ccTLD (country code top-level domains, национальные домены).

В соответствии с принятыми правилами право администрирования каждого домена первого уровня передается одной конкретной организации (оператору регистра; администратором доменной зоны «ru» является РосНИИРОС). Зарегистрировать домен второго уровня, например, в доменной зоне «ru» можно у одного из многочисленных регистраторов (коммерческие организации, имеющие доступ к общей базе данных оператора регистра для данной доменной зоны).

Первоначально в ARPANET было семь доменов верхнего организационного уровня:

1. **com** (коммерческие организации);
2. **edu** (образовательные организации, в основном изСША);
3. **gov** (правительственные организации США);
4. **int** (международные организации);
5. **mil** (военные организации США);
6. **net**(организации, обеспечивающие сетевую инфраструктуру);
7. **org** (некоммерческие организации).

В 90-х годах к ним были добавлены следующие домены:

8. **aero** (организации, связанные с авиацией);
9. **arpa** (используется для отображения адресов в имена);
10. **biz** (коммерческие организации);
11. **coop** (кооперативы);
12. **info** (разное);
13. **museum** (музеи);
14. **name** (персональные домены);
15. **pro** (лицензированные профессионалы).

Список доменов ccTLD базируется на стандарте двухбуквенных кодов государств и территорий (ISO 3166).

Примеры доменов верхнего уровня ccTLD, соответствующие отдельным государствам, приведены в таблице 2.

В Internet система доменных имен реализована в виде распределенной базы данных, включающей в себя серверы DNS, клиенты DNS (resolver), объединенные общим протоколом запросов к базе данных и обмена информацией между серверами.

Таблица 2

Примеры национальных доменов верхнего уровня

Страна	Код	Страна	Код
Аргентина	ar	Кипр	cy
Армения	am	Киргизстан	kg
Австрия	at	Казахстан	kz
Азербайджан	az	Канада	ca
Белорусь	by	Индия	id
Бельгия	be	Латвия	LV
Болгария	bg	Литва	lt
Чехия	cz	Молдова	md
Эстония	ee	Нидерланды	nl
Финляндия	fi	Польша	pl
Франция	fr	Португалия	pt
Германия	de	Россия	ru
Греция	gr	Словакия	sk
Грузия	ge	Словения	si
Дания	dk	Испания	es
Венгрия	hu	Швеция	se
Италия	it	Швейцария	ch
Япония	jp	Узбекистан	uz
Украина	ua	Туркменистан	tm
Великобритания	gb	Соединенные Штаты	us

Информация, соответствующая каждому доменному имени, хранится в записях ресурсов RR (resource records) DNS-сервера. Основным типом хранимой информации является IP-адрес. Одному доменному имени может соответствовать несколько IP-адресов (в случае использования нескольких сетевых интерфейсов на компьютере). Кроме этого, в записях ресурсов может храниться дополнительная информация, например, максимально допустимое время кэширования[3] полученной информации (TTL, time to live).

[3] Кэширование информации заключается в ее запоминании запросившим узлом или DNS-сервером более низкого уровня. По истечении указанного времени данная информация может быть удалена клиентом.

В системе доменных имен различают несколько типов DNS-серверов.

В зависимости от типа отклика на запрос серверы делятся на авторитетные (authoritative) и неавторитетные (non authoritative).

Авторитетный отклик (authoritative response) возвращают серверы, которые являются ответственными за зону, в которой описана информация, необходимая клиенту DNS.

Неавторитетный отклик (non authoritative response) возвращают серверы, которые не отвечают за зону, содержащую необходимую клиенту информацию.

В зависимости от способа поддержания базы данных авторитетные DNS-серверы делятся на первичные (primary) и дублирующие (secondary).

Первичный сервер доменных имен является ответственным за информацию о конкретной доменной зоне[4] и поэтому хранит эту информацию, загружает ее для ответов клиентам с локального диска узла, на котором он функционирует. Описание зоны этого сервера ведется непосредственно администратором зоны.

Дублирующий сервер доменных имен также является ответственным за эту доменную зону. В его функции входит дублирование первичного сервера на случай нарушения его работы. Кроме этого, дублирующий сервер, обрабатывая часть запросов, снимает нагрузку с первичного сервера.

Администратор дублирующего сервера не изменяет данные описания доменной зоны, а только обеспечивает синхронизацию базы данных дублирующего сервера с базой данных первичного сервера.

Примером такой организации является система корневых (root-servers) DNS-серверов Internet. Всего в сети Internet 13 корневых DNS-серверов.

Корневые серверы являются основой всей системы доменных имен, поскольку являются ***авторитетными серверами*** для корневой зоны и содержат ссылки на такие же серверы зон первого уровня или сами являются авторитетными серверами некоторых зон первого уровня (например, com. или net.).

На запрос о домене корневой сервер возвращает как минимум имя и адрес уполномоченного сервера домена первого уровня, в который входит указанный в запросе узел. Обратившись по

[4] Для каждой доменной зоны первичным может быть только один сервер, поскольку «первоисточник» может и должен быть только один.

полученному адресу, можно получить имя и адрес уполномоченного сервера домена второго уровня и т. д.

Из всего списка корневых серверов только один из них (A.ROOT-SERVERS.NET) является первичным, а все остальные дублирующие, хотя они содержат идентичную информацию.

Благодаря такой организации Internet выдержал несколько глобальных атак злоумышленников.

Защита DNS-серверов любого уровня, а особенно корневых, является одной из проблем современной сети Internet.

Обобщенная схема работы системы доменных имен следующая.

Пользователь инициирует запрос к web-серверу (например к "www.urgi.ru"). В соответствии с настройками сетевого подключения DNS-клиент формирует DNS-запрос к ближайшему DNS-серверу (как правило, по умолчанию DNS-сервер провайдера) об IP-адресе узла, на котором функционирует данный web-сервер.

Если DNS-сервер провайдера является авторитетным для доменной зоны «.ru», то он возвращает узлу пользователя (а вернее программе, инициировавшей запрос) DNS-отклик, в котором содержится требуемый IP-адрес (в предположении, что такой web-сервер вообще зарегистрирован).

В случае, если DNS-сервер провайдера не является авторитетным для доменной зоны «.ru», то он формирует аналогичный DNS-запрос к вышестоящему DNS-серверу (чаще всего, но не обязательно, корневому DNS-серверу). Корневой DNS-сервер в ответ на полученный запрос формирует DNS-отклик, в котором содержится IP-адрес авторитетного для данной доменной зоны DNS-сервера, получив который, DNS-сервер провайдера сформирует к нему запрос и полученный отклик вернет клиенту. При этом полученная информация будет занесена в кэш-память DNS-сервера провайдера. В случае повторного запроса от пользователя IP-адреса web-сервера (например к «www.urgi.ru»), DNS-сервер провайдера сформирует отклик, используя информацию из кэш-памяти, и не будет обращаться к вышестоящему DNS-серверу.

Запросы клиентов (или серверов) могут быть рекурсивными или итеративными. Рекурсивный запрос подразумевает, что запрашиваемый сервер должен самостоятельно пробежаться по всей системе серверов (вплоть до корневого) до получения конечного ответа (в том числе отрицательного) и вернуть его клиенту. При этом сам сервер может пользоваться итеративными или рекурсивными

запросами. Сервер может отказаться выполнять рекурсивные запросы «сторонних» клиентов. При итеративном запросе сервер делает только один шаг поиска и возвращает ссылку на авторитетный сервер (или конечный ответ, если он сам является авторитетным для данного домена). Дальнейший поиск производится самим клиентом.

Очевидно, что сервер доменных имен и клиентское программное обеспечение реализуют заложенную в DNS архитектуру «клиент-сервер», а программные средства, указанные в последнем пункте, позволяют упростить настройку сервера и управление им.

История развития сети Интернет показывает, что DNS-сервер является объектом атак со стороны злоумышленников, поскольку, выведя из строя этот сервер или изменив данные его базы, можно, нарушить работу сети.

3.5. Классификация удаленных угроз в вычислительных сетях

Удаленные угрозы можно классифицировать по следующим признакам[5].

По характеру воздействия:

- пассивные (класс 1.1);
- активные (класс 1.2).

Пассивным воздействием на распределенную вычислительную систему называется воздействие, которое не оказывает непосредственного влияния на работу системы, но может нарушать ее политику безопасности. Именно отсутствие непосредственного влияния на работу сети приводит к тому, что пассивное удаленное воздействие практически невозможно обнаружить. Примером пассивного типового удаленного воздействия в вычислительных сетях является прослушивание канала связи в сети. Под ***активным*** воздействием на вычислительную сеть понимается воздействие, оказывающее непосредственное влияние на работу сети (изменение конфигурации, нарушение работоспособности и т. д.) и нарушающее принятую в ней политику безопасности. Практически все типы удаленных угроз являются активными воздействиями.

По цели воздействия:

- нарушение конфиденциальности информации (класс 2.1);

[5] Медведовский И.Д., Семьянов П.В., Платонов В.В. Атака через Internet /Под ред. проф. П.Д.Зегжды/ НПО "Мир и семья-95", 1997.

- нарушение целостности информации (класс 2.2);
- нарушение доступности информации (работоспособности системы) (класс 2.3).

Этот классификационный признак является прямой проекцией трех основных типов угроз – раскрытия, целостности и отказа в обслуживании.

Одна из основных целей злоумышленников – получение несанкционированного доступа к информации. Существуют две принципиальные возможности доступа к информации: перехват и искажение. Возможность перехвата информации означает получение к ней доступа, но невозможность ее модификации. Следовательно, перехват информации ведет к нарушению ее конфиденциальности. Примером перехвата информации может служить прослушивание канала в сети. В этом случае имеется несанкционированный доступ к информации без возможности ее искажения. Очевидно также, что нарушение конфиденциальности информации является пассивным воздействием.

Возможность искажения информации означает либо полный контроль над информационным потоком между объектами системы, либо возможность передачи сообщений от имени другого объекта. Таким образом, очевидно, что искажение информации ведет к нарушению ее целостности. Данное информационное разрушающее воздействие представляет собой яркий пример активного воздействия. Примером удаленной угрозы, цель которой нарушение целостности информации, может служить типовая удаленная атака «ложный объект распределенной вычислительной сети».

Принципиально другая цель преследуется злоумышленником при реализации угрозы для нарушения работоспособности сети. В этом случае не предполагается получение несанкционированного доступа к информации. Его основная цель – добиться, чтобы узел сети или какой-то из сервисов, поддерживаемый им, вышел из строя и для всех остальных объектов сети доступ к ресурсам атакованного объекта был бы невозможен. Примером удаленной атаки, целью которой является нарушение работоспособности системы, может служить типовая удаленная атака «отказ в обслуживании».

По условию начала осуществления воздействия. Удаленное воздействие так же, как и любое другое, может начать осуществляться только при определенных условиях. В вычислительных сетях можно выделить три вида условий начала осуществления удаленной атаки:

- атака по запросу от атакуемого объекта (класс 3.1);
- атака по наступлению ожидаемого события на атакуемом объекте (класс 3.2);
- безусловная атака (класс 3.3).

В первом случае злоумышленник ожидает передачи от потенциальной цели атаки запроса определенного типа, который и будет условием начала осуществления воздействия. Примером подобных запросов в сети Internet служат DNS-запросы. Отметим, что данный тип удаленных атак наиболее характерен для распределенных вычислительных сетей.

Во втором случае злоумышленник осуществляет постоянное наблюдение за состоянием операционной системы удаленной цели атаки и при возникновении определенного события в этой системе начинает воздействие. Как и в предыдущем случае, инициатором осуществления начала атаки выступает сам атакуемый объект.

Реализация третьего вида атаки не связана ни с какими событиями и реализуется безусловно по отношению к цели атаки, то есть атака осуществляется немедленно.

По наличию обратной связи с атакуемым объектом:

- с обратной связью (класс 4.1);
- без обратной связи (однонаправленная атака) (класс 4.2).

Удаленная атака, осуществляемая при наличии обратной связи с атакуемым объектом, характеризуется тем, что на некоторые запросы, переданные на атакуемый объект, атакующему требуется получить ответ, а следовательно, между атакующим и целью атаки существует обратная связь, которая позволяет атакующему адекватно реагировать на все изменения, происходящие на атакуемом объекте.

В отличие от атак с обратной связью удаленным атакам без обратной связи не требуется реагировать на какие-либо изменения, происходящие на атакуемом объекте. Атаки данного вида обычно осуществляются передачей на атакуемый объект одиночных запросов, ответы на которые атакующему не нужны. Подобную удаленную атаку можно называть однонаправленной удаленной атакой. Примером однонаправленных атак является типовая удаленная атака «отказ в обслуживании».

По расположению субъекта атаки относительно атакуемого объекта:

- внутрисегментное (класс 5.1);

- межсегментное (класс 5.2).

Рассмотрим ряд определений.

Субъект атаки (или источник атаки) – это атакующая программа или злоумышленник, непосредственно осуществляющие воздействие.

Маршрутизатор (router) – устройство, обеспечивающее маршрутизацию пакетов обмена в глобальной сети.

Подсеть (subnetwork) (в терминологии Internet) совокупность хостов, являющихся частью глобальной сети, для которых маршрутизатором выделен одинаковый номер подсети. Хосты внутри одной подсети могут взаимодействовать между собой непосредственно, минуя маршрутизатор.

Сегмент сети – физическое объединение хостов. Например, сегмент сети образует совокупность хостов, подключенных к серверу по схеме «общая шина». При такой схеме подключения каждый хост имеет возможность подвергать анализу любой пакет в своем сегменте.

С точки зрения удаленной атаки чрезвычайно важно, как по отношению друг к другу располагаются субъект и объект атаки, то есть в одном или в разных сегментах они находятся. В случае внутрисегментной атаки, как следует из названия, субъект и объект атаки находятся в одном сегменте. При межсегментной атаке субъект и объект атаки находятся в разных сегментах. Данный классификационный признак позволяет судить о так называемой «степени удаленности» атаки.

Важно отметить, что межсегментная удаленная атака представляет гораздо большую опасность, чем внутрисегментная. Это связано с тем, что в случае межсегментной атаки объект её и непосредственно атакующий могут находиться на расстоянии многих тысяч километров друг от друга, что может существенно воспрепятствовать мерам по локализации субъекта атаки.

По уровню модели ISO/OSI, на котором осуществляется воздействие:

- физический (класс 6.1);
- канальный (класс 6.2);
- сетевой (класс 6.3);
- транспортный (класс 6.4);
- сеансовый (класс 6.5);
- представительный (класс 6.6);
- прикладной (класс 6.7).

3.6. Типовые удаленные атаки и их характеристика

Типовая удаленная атака – это удаленное информационное разрушающее воздействие, программно осуществляемое по каналам связи и характерное для любой распределенной вычислительной сети.

Основной особенностью распределенной вычислительной сети является распределенность ее объектов в пространстве и связь между ними по физическим линиям связи. При этом все управляющие сообщения и данные, пересылаемые между объектами вычислительной сети, передаются по сетевым соединениям в виде пакетов обмена. Эта особенность привела к появлению специфичного для распределенных вычислительных сетей типового удаленного воздействия, заключающегося в прослушивании канала связи, называемого ***анализом сетевого трафика***.

Анализ сетевого трафика позволяет:

- изучить логику работы распределенной вычислительной сети, это достигается путем перехвата и анализа пакетов обмена на канальном уровне (знание логики работы сети позволяет на практике моделировать и осуществлять другие типовые удаленные атаки);
- перехватить поток данных, которыми обмениваются объекты сети, то есть удаленная атака данного типа заключается в получении несанкционированного доступа к информации, которой обмениваются пользователи (примером перехваченной при помощи данной типовой удаленной атаки информации могут служить имя и пароль пользователя, пересылаемые в незашифрованном виде по сети).

Одной из проблем безопасности распределенной ВС является недостаточная идентификация и аутентификация (определение подлинности) удаленных друг от друга объектов. Основная трудность заключается в осуществлении однозначной идентификации сообщений, передаваемых между субъектами и объектами взаимодействия. Обычно в вычислительных сетях эта проблема решается использованием виртуального канала, по которому объекты обмениваются определенной информацией, уникально идентифицирующей данный канал. Для адресации сообщений в распределенных вычислительных сетях используется сетевой адрес, который уникален для каждого объекта системы (на канальном уровне модели OSI – это аппаратный адрес сетевого адаптера, на сетевом уровне – адрес определяется протоколом сетевого уровня

(например, IP-адрес). Сетевой адрес также может использоваться для идентификации объектов сети.

В том случае, когда в вычислительной сети используют нестойкие алгоритмы идентификации удаленных объектов, оказывается возможной типовая удаленная атака, заключающаяся в передаче по каналам связи сообщений от имени произвольного объекта или субъекта сети, то есть ***подмена объекта или субъекта сети.***

Недостаточно надежная идентификация сетевых управляющих устройств (например, маршрутизаторов) является причиной возможного внедрения в сеть ложного объекта путем изменения маршрутизации пакетов, передаваемых в сети.

Современные глобальные сети представляют собой совокупность сегментов сети, связанных между собой через сетевые узлы. При этом маршрутом называется последовательность узлов сети, по которой данные передаются от источника к приемнику. Каждый маршрутизатор имеет специальную таблицу, называемую ***таблицей маршрутизации***, в которой для каждого адресата указывается оптимальный маршрут. Таблицы маршрутизации существуют не только у маршрутизаторов, но и у любых хостов (узлов) в глобальной сети. Для обеспечения эффективной и оптимальной маршрутизации в распределенных ВС применяются специальные управляющие протоколы, позволяющие маршрутизаторам обмениваться информацией друг с другом (RIP (Routing Internet Protocol), OSPF (Open Shortest Path First)), уведомлять хосты о новом маршруте – ICMP (Internet Control Message Protocol), удаленно управлять маршрутизаторами (SNMP (Simple Network Management Protocol)). Эти протоколы позволяют удаленно изменять маршрутизацию в сети Интернет, то есть являются протоколами управления сетью.

Реализация данной типовой удаленной атаки заключается в несанкционированном использовании протоколов управления сетью для изменения исходных таблиц маршрутизации. В результате успешного изменения маршрута атакующий получит полный контроль над потоком информации, которой обмениваются объекты сети, и атака перейдет во вторую стадию, связанную с приемом, анализом и передачей сообщений, получаемых от дезинформированных объектов вычислительной сети.

Получив контроль над проходящим потоком информации между объектами, ложный объект вычислительной сети может применять

различные методы воздействия на перехваченную информацию, например:

1) селекция потока информации и сохранение ее на ложном объекте (нарушение конфиденциальности);

2) модификация информации:

- модификация данных (нарушение целостности);
- модификация исполняемого кода и внедрение разрушающих программных средств – программных вирусов (нарушение доступности, целостности);

3) подмена информации (нарушение целостности).

Одной из основных задач, возлагаемых на сетевую операционную систему, функционирующую на каждом из объектов распределенной вычислительной сети, является обеспечение надежного удаленного доступа с любого объекта сети к данному объекту. В общем случае в сети каждый субъект системы должен иметь возможность подключиться к любому объекту сети и получить в соответствии со своими правами удаленный доступ к его ресурсам. Обычно в вычислительных сетях возможность предоставления удаленного доступа реализуется следующим образом: на объекте в сетевой операционной системе запускаются на выполнение ряд программ-серверов (например, FTP-сервер, WWW-сервер и т. п.), предоставляющих удаленный доступ к ресурсам данного объекта. Данные программы-серверы входят в состав телекоммуникационных служб предоставления удаленного доступа. Задача сервера состоит в том, чтобы постоянно ожидать получения запроса на подключение от удаленного объекта и, получив такой запрос, передать на запросивший объект ответ на разрешение подключения либо на отказ. По аналогичной схеме происходит создание виртуального канала связи, по которому обычно взаимодействуют объекты сети. В этом случае непосредственно операционная система обрабатывает приходящие извне запросы на создание виртуального канала и передает их в соответствии с идентификатором запроса (номер порта) прикладному процессу, которым является соответствующий сервер. В зависимости от различных параметров объектов вычислительной сети, основными из которых являются быстродействие ЭВМ, объем оперативной памяти и пропускная способность канала связи, количество одновременно устанавливаемых виртуальных подключений ограничено, соответственно ограничено и число запросов, обрабатываемых в единицу времени. С этой особенностью работы

вычислительных сетей связана типовая удаленная атака «***отказ в обслуживании***».

Результат применения этой удаленной атаки – нарушение на атакованном объекте работоспособности соответствующей службы предоставления удаленного доступа, то есть невозможность получения удаленного доступа с других объектов вычислительной сети – отказ в обслуживании. Одна из разновидностей этой типовой удаленной атаки заключается в передаче с одного адреса такого количества запросов на атакуемый объект, которое позволяет трафик. В этом случае, если в системе не предусмотрены правила, ограничивающие число принимаемых запросов с одного объекта (адреса) в единицу времени, то результатом этой атаки может являться как переполнение очереди запросов и отказа одной из телекоммуникационных служб, так и полная остановка компьютера из-за невозможности системы заниматься ничем другим, кроме обработки запросов. И последней, третьей разновидностью атаки «отказ в обслуживании», является передача на атакуемый объект некорректного, специально подобранного запроса. В этом случае при наличии ошибок в удаленной системе возможно зацикливание процедуры обработки запроса, переполнение буфера с последующим зависанием системы. Основными причинами успеха удаленных угроз в вычислительных сетях являются:

1. Отсутствие выделенного канала связи между объектами сети.
2. Недостаточная идентификация объектов и субъектов сети.
3. Взаимодействие объектов без установления виртуального канала.
4. Отсутствие в распределенных вычислительных сетях полной информации о ее объектах.
5. Отсутствие в распределенных вычислительных сетях криптозащиты сообщений.

Контрольные вопросы по разделу №3

1. В чем заключаются особенности обеспечения «информационной безопасности» компьютерных сетей?
2. Дайте определение понятия «удаленная угроза».
3. В чем заключается специфика методов и средств защиты компьютерных сетей?

4. Поясните понятие «глобальная сетевая атака», приведите примеры.

5. Какие протоколы образуют модель TCP/IP?

6. Какой протокол обеспечивает преобразование логических сетевых адресов в аппаратные?

7. Проведите сравнительную характеристику моделей передачи данных TCP/IP и OSI/ISO.

8. На каком уровне модели OSI/ISO реализуется сервис безопасности «неотказуемость» (согласно «Общим критериям»)?

9. Для чего предназначен DNS-сервер?

10. Перечислите классы удаленных угроз.

11. Как классифицируются удаленные угрозы «по характеру воздействия»?

12. Охарактеризуйте удаленные угрозы «по цели воздействия».

13. Может ли пассивная угроза привести к нарушению целостности информации?

14. Дайте определение типовой удаленной атаки.

15. Что является целью злоумышленников при «анализе сетевого трафика»?

16. Назовите причины успеха удаленной атаки «ложный объект».

4. МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ ИФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1. Идентификация и аутентификация

Идентификация и аутентификации применяются для ограничения доступа случайных и незаконных субъектов (пользователи, процессы) информационных систем к ее объектам (аппаратные, программные и информационные ресурсы) [10].

Общий алгоритм работы таких систем заключается в том, чтобы получить от субъекта (например, пользователя) информацию, удостоверяющую его личность, проверить ее подлинность и затем предоставить (или не предоставить) этому пользователю возможность работы с системой.

Наличие процедур аутентификации и/или идентификации пользователей является обязательным условием любой защищенной системы, поскольку все механизмы защиты информации рассчитаны на работу с поименованными субъектами и объектами информационных систем.

Идентификация – присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным.

Аутентификация (установление подлинности) – проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности. Другими словами, аутентификация заключается в проверке: является ли подключающийся субъект тем, за кого он себя выдает.

При построении систем идентификации и аутентификации возникает проблема выбора идентификатора, на основе которого осуществляются процедуры идентификации и аутентификации пользователя. В качестве идентификаторов обычно используют:

- набор символов (пароль, секретный ключ, персональный идентификатор и т. п.), который пользователь запоминает или для их запоминания использует специальные средства хранения (электронные ключи);
- физиологические параметры человека (отпечатки пальцев, рисунок радужной оболочки глаза и т. п.) или особенности поведения (особенности работы на клавиатуре и т. п.).

Наиболее распространенными простыми и привычными являются методы аутентификации, основанные на паролях –

конфиденциальных идентификаторах субъектов. В этом случае при вводе субъектом своего пароля подсистема аутентификации сравнивает его с паролем, хранящимся в базе эталонных данных в зашифрованном виде. В случае совпадения паролей подсистема аутентификации разрешает доступ к ресурсам системы.

Парольные методы аутентификации по степени изменяемости паролей делятся на:

- методы, использующие постоянные (многократно используемые) пароли;
- методы, использующие одноразовые (динамично изменяющиеся) пароли.

Использование одноразовых или динамически меняющихся паролей является более надежным методом парольной защиты.

В последнее время получили распространение комбинированные методы идентификации и аутентификации, требующие, помимо знания пароля, наличие карточки (token) – специального устройства, подтверждающего подлинность субъекта.

Карточки разделяют на два типа:

- пассивные (карточки с памятью);
- активные (интеллектуальные карточки).

Самыми распространенными являются пассивные карточки с магнитной полосой, которые считываются специальным устройством, имеющим клавиатуру и процессор. При использовании указанной карточки пользователь вводит свой идентификационный номер. В случае его совпадения с электронным вариантом, закодированным в карточке, пользователь получает доступ в систему. Это позволяет достоверно установить лицо, получившее доступ к системе, и исключить несанкционированное использование карточки злоумышленником (например, при ее утере). Такой способ часто называют двухкомпонентной аутентификацией.

Интеллектуальные карточки кроме памяти имеют собственный микропроцессор. Это позволяет реализовать различные варианты парольных методов защиты, например, многоразовые пароли, динамически меняющиеся пароли.

Методы аутентификации, основанные на измерении биометрических параметров человека, обеспечивают почти 100 % идентификацию, решая проблемы утери или утраты паролей и личных идентификаторов. Однако эти методы нельзя использовать при идентификации процессов или данных (объектов данных), они только

начинают развиваться, требуют пока сложного и дорогостоящего оборудования. Это обусловливает их использование пока только на особо важных объектах.

Примерами внедрения указанных методов являются системы идентификации пользователя по рисунку радужной оболочки глаза, по почерку, по тембру голоса и др.

Новейшим направлением аутентификации является доказательство подлинности удаленного пользователя по его местонахождению. Данный защитный механизм основан на использовании системы космической навигации, типа GPS (Global Positioning System). Пользователь, имеющий аппаратуру GPS, многократно посылает координаты заданных спутников, находящихся в зоне прямой видимости. Подсистема аутентификации, зная орбиты спутников, может с точностью до метра определить месторасположение пользователя. Высокая надежность аутентификации определяется тем, что орбиты спутников подвержены колебаниям, предсказать которые достаточно трудно. Кроме того, координаты постоянно меняются, что исключает их перехват. Такой метод аутентификации может быть использован в случаях, когда авторизованный удаленный пользователь должен находиться в нужном месте.

Механизм идентификации и аутентификации пользователей

Общая процедура идентификации и аутентификации пользователя при его доступе в защищенную информационную систему заключается в следующем.

Пользователь предоставляет системе свой личный идентификатор (например, вводит пароль или предоставляет палец для сканирования отпечатка). Далее система сравнивает полученный идентификатор со всеми хранящимися в ее базе идентификаторами. Если результат сравнения успешный, то пользователь получает доступ к системе в рамках установленных полномочий. В случае отрицательного результата система сообщает об ошибке и предлагает повторно ввести идентификатор.

В тех случаях, когда пользователь превышает лимит возможных повторов ввода информации (ограничение на количество повторов является обязательным условием для защищенных систем) система временно блокируется и выдается сообщение о несанкционированных действиях (причем, может быть, и незаметно для пользователя).

Если в процессе аутентификации подлинность субъекта установлена, то система защиты информации должна определить его полномочия (совокупность прав). Это необходимо для последующего контроля и разграничения доступа к ресурсам.

В целом аутентификация по уровню информационной безопасности делится на три категории:

1) статическая аутентификация;
2) устойчивая аутентификация;
3) постоянная аутентификация.

Первая категория обеспечивает защиту только от несанкционированных действий в системах, где нарушитель не может во время сеанса работы прочитать аутентификационную информацию. Примером средства ***статической*** аутентификации являются традиционные постоянные пароли. Их эффективность преимущественно зависит от сложности угадывания паролей и, собственно, от того, насколько хорошо они защищены.

Устойчивая аутентификация использует динамические данные аутентификации, меняющиеся с каждым сеансом работы. Реализациями устойчивой аутентификации являются системы, использующие одноразовые пароли и электронные подписи. Устойчивая аутентификация обеспечивает защиту от атак, где злоумышленник может перехватить аутентификационную информацию и использовать ее в следующих сеансах работы.

Однако устойчивая аутентификация не обеспечивает защиту от активных атак, в ходе которых маскирующийся злоумышленник может оперативно (в течение сеанса аутентификации) перехватить, модифицировать и вставить информацию в поток передаваемых данных. ***Постоянная*** аутентификация обеспечивает идентификацию каждого блока передаваемых данных, что предохраняет их от несанкционированной модификации или вставки. Примером реализации указанной категории аутентификации является использование алгоритмов генерации электронных подписей для каждого бита пересылаемой информации.

4.2. Криптография и шифрование

Структура криптосистемы

Самый надежный технический метод защиты информации основан на использовании криптосистем. Криптосистема включает:

- алгоритм шифрования;
- набор ключей (последовательность двоичных чисел), используемых для шифрования;
- систему управления ключами.

Общая схема работы криптосистемы показана на рис. 4.

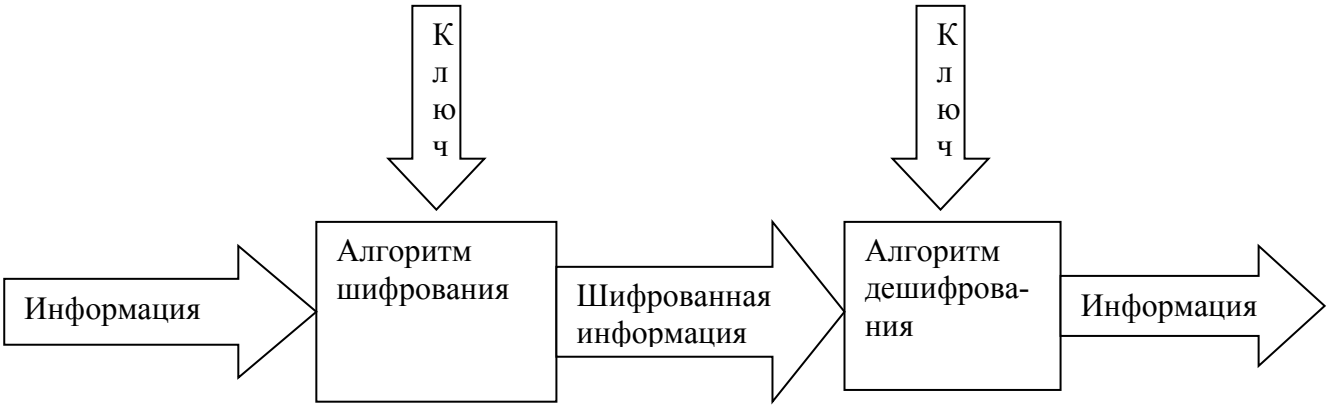

Рис. 4. Криптосистема

Криптосистемы решают такие проблемы информационной безопасности, как обеспечение конфиденциальности, целостности данных, а также аутентификацию данных и их источников.

Криптографические методы защиты являются обязательным элементом безопасных информационных систем. Особое значение криптографические методы получили с развитием распределенных открытых сетей, в которых нет возможности обеспечить физическую защиту каналов связи.

Классификация систем шифрования данных

Основным классификационным признаком систем шифрования данных является способ их функционирования. По способу функционирования системы шифрования данных делят на два класса:

- системы «прозрачного» шифрования;
- системы, специально вызываемые для осуществления шифрования.

В системах прозрачного шифрования (шифрование «на лету») криптографические преобразования осуществляются в режиме реального времени, незаметно для пользователя. Например, пользователь записывает подготовленный в текстовом редакторе документ на защищаемый диск, а система защиты в процессе записи

выполняет его шифрование. Системы второго класса обычно представляют собой утилиты (программы), которые необходимо специально вызывать для выполнения шифрования.

Как уже отмечалось, особое значение криптографические преобразования имеют при передаче данных по распределенным вычислительным сетям. Для защиты данных в распределенных сетях используются два подхода: канальное шифрование и оконечное (абонентское) шифрование.

В случае ***канального шифрования*** защищается вся информация, передаваемая по каналу связи, включая служебную. Этот способ шифрования обладает следующим достоинством: встраивание процедур шифрования на канальный уровень позволяет использовать аппаратные средства, что способствует повышению производительности системы.

Оконечное (абонентское) шифрование позволяет обеспечить конфиденциальность данных, передаваемых между двумя абонентами. В этом случае защищается только содержание сообщений, вся служебная информация остается открытой.

Симметричные и асимметричные методы шифрования

Классические криптографические методы делятся на два основных типа: ***симметричные*** (шифрование секретным ключом) и ***асимметричные*** (шифрование открытым ключом).

В ***симметричных*** методах для шифрования и расшифровывания используется один и тот же секретный ключ. Наиболее известным стандартом на симметричное шифрование с закрытым ключом является стандарт для обработки информации в государственных учреждениях США DES (Data Encryption Standard). Общая технология использования симметричного метода шифрования представлена на рис. 5.

Основной недостаток этого метода заключается в том, что ключ должен быть известен и отправителю, и получателю. Это существенно усложняет процедуру назначения и распределения ключей между пользователями. Указанный недостаток послужил причиной разработки методов шифрования с открытым ключом – асимметричных методов.

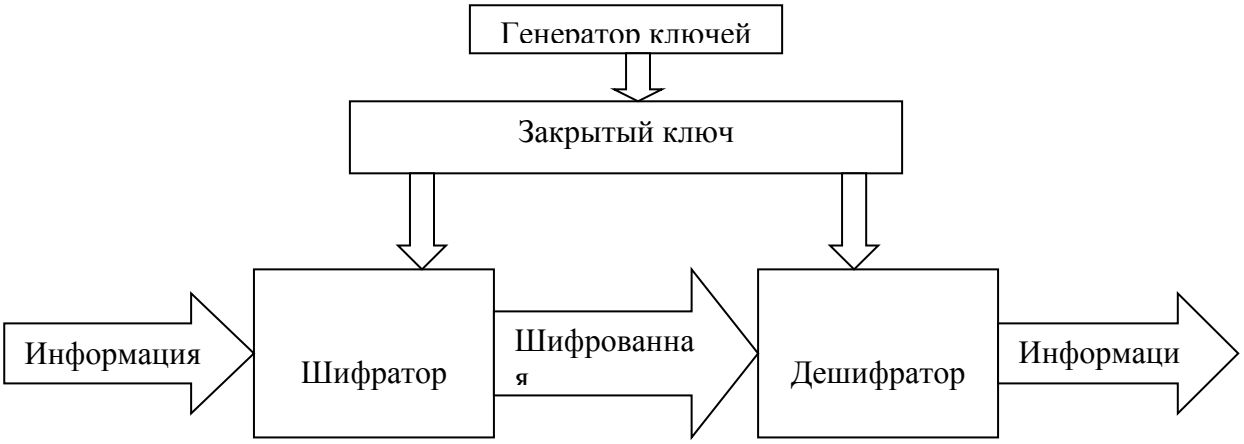

Рис. 5. Симметричное шифрование

Асимметричные методы используют два взаимосвязанных ключа: для шифрования и расшифрования. Один ключ является закрытым и известным только получателю. Его используют для расшифрования. Второй из ключей является открытым, то есть он может быть общедоступным по сети и опубликован вместе с адресом пользователя. Его используют для выполнения шифрования. Схема функционирования данного типа криптосистемы показана на рис. 6.

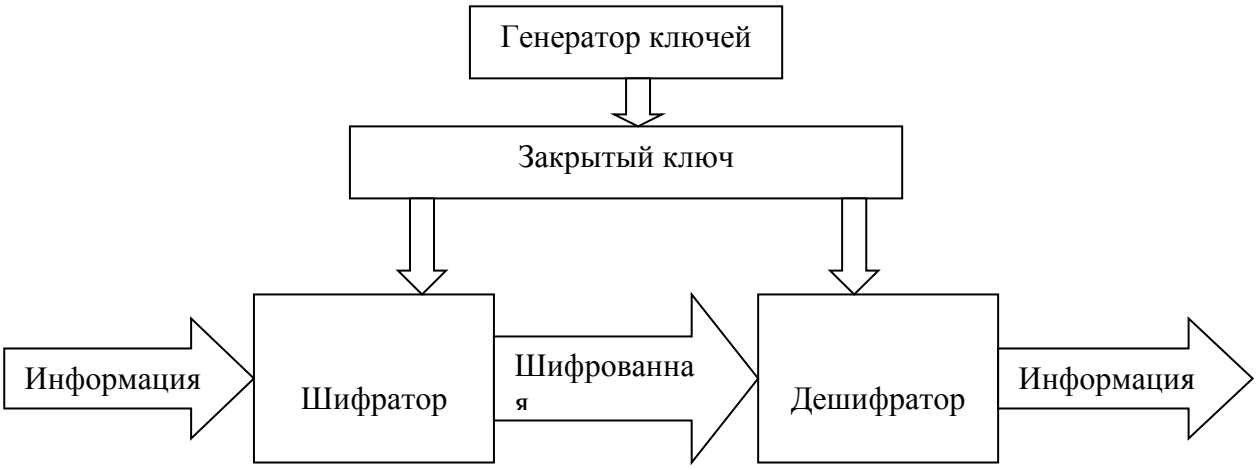

Рис. 6. Асимметричное шифрование

В настоящее время наиболее известным и надежным является асимметричный алгоритм RSA (Rivest, Shamir, Adleman).

Электронная цифровая подпись

Для контроля целостности передаваемых по сетям данных используется электронная цифровая подпись, которая реализуется по методу шифрования с открытым ключом.

Электронная цифровая подпись представляет собой относительно небольшое количество дополнительной аутентифицирующей информации, передаваемой вместе с подписываемым текстом. Отправитель формирует цифровую подпись, используя секретный ключ отправителя. Получатель проверяет подпись, используя открытый ключ отправителя.

Идея технологии электронной подписи состоит в следующем. Отправитель передает два экземпляра одного сообщения: открытое и расшифрованное его закрытым ключом (то есть обратно шифрованное). Получатель шифрует с помощью открытого ключа отправителя расшифрованный экземпляр. Если он совпадет с открытым вариантом, то личность и подпись отправителя считается установленной.

При практической реализации электронной подписи также шифруется не все сообщение, а лишь специальная контрольная сумма – хэш, защищающая послание от нелегального изменения. Электронная подпись здесь гарантирует как целостность сообщения, так и удостоверяет личность отправителя.

Безопасность любой криптосистемы определяется используемыми криптографическими ключами. В случае ненадежного управления ключами злоумышленник может завладеть ключевой информацией и получить полный доступ ко всей информации в системе или сети. Различают следующие виды функций управления ключами: генерация, хранение и распределение ключей.

Способы генерации ключей для симметричных и асимметричных криптосистем различны. Для генерации ключей симметричных криптосистем используются аппаратные и программные средства генерации случайных чисел. Генерация ключей для асимметричных криптосистем более сложна, так как ключи должны обладать определенными математическими свойствами.

Функция хранения предполагает организацию безопасного хранения, учета и удаления ключевой информации. Для обеспечения безопасного хранения ключей применяют их шифрование с помощью других ключей. Такой подход приводит к концепции иерархии ключей. В иерархию ключей обычно входит главный ключ (то есть мастер-ключ), ключ шифрования ключей и ключ шифрования

данных. Следует отметить, что генерация и хранение мастер-ключа является наиболее критическим вопросом криптозащиты.

Распределение – самый ответственный процесс в управлении ключами. Этот процесс должен гарантировать скрытность распределяемых ключей, а также быть оперативным и точным. Между пользователями сети ключи распределяют двумя способами:

- с помощью прямого обмена сеансовыми ключами;
- используя один или несколько центров распределения ключей.

4.3. Методы разграничение доступа

Виды методов разграничения доступа

После выполнения идентификации и аутентификации подсистема защиты устанавливает полномочия (совокупность прав) субъекта для последующего контроля санкционированного использования объектов информационной системы.

Обычно полномочия субъекта представляются: ***списком ресурсов***, доступным пользователю, ***и правами по доступу*** к каждому ресурсу из списка.

Существуют следующие методы разграничения доступа:

1) разграничение доступа по спискам;
2) использование матрицы установления полномочий;
3) разграничение доступа по уровням секретности и категориям;
4) парольное разграничение доступа.

При ***разграничении доступа по спискам*** задаются соответствия: каждому пользователю – список ресурсов и прав доступа к ним или каждому ресурсу – список пользователей и их прав доступа к данному ресурсу.

Списки позволяют установить права с точностью до пользователя. Здесь нетрудно добавить права или явным образом запретить доступ. Списки используются в подсистемах безопасности операционных систем и систем управления базами данных.

Использование ***матрицы установления полномочий*** подразумевает применение матрицы доступа (таблицы полномочий). В указанной матрице строками являются идентификаторы субъектов, имеющих доступ в информационную систему, а столбцами – объекты (ресурсы) информационной системы. Каждый элемент матрицы может содержать имя и размер предоставляемого ресурса, право доступа

(чтение, запись и др.), ссылку на другую информационную структуру, уточняющую права доступа, ссылку на программу, управляющую правами доступа и др.

Данный метод предоставляет более унифицированный и удобный подход, так как вся информация о полномочиях хранится в виде единой таблицы, а не в виде разнотипных списков. Недостатками матрицы являются ее возможная громоздкость и неоптимальность (большинство клеток – пустые).

Фрагмент матрицы установления полномочий показан в таблице 3.

Таблица 3

Матрица полномочий

	Диск c:\	Файл d:\prog. exe	Принтер
Пользователь I	Чтение Запись Удаление	Выполнение Удаление	Печать Настройка параметров
Пользователь 2	Чтение	Выполнение	Печать с 9:00 до 17:00
Пользователь 3	Чтение Запись	Выполнение	Печать с 17:00 до 9:00

Разграничение доступа по уровням секретности и категориям заключается в разделении ресурсов информационной системы по уровням секретности и категориям.

При разграничении по степени секретности выделяют несколько уровней, например: общий доступ, конфиденциально, секретно, совершенно секретно. Полномочия каждого пользователя задаются в соответствии с максимальным уровнем секретности, к которому он допущен. Пользователь имеет доступ ко всем данным, имеющим уровень (гриф) секретности не выше, чем ему определен, например, пользователь имеющий доступ к данным «секретно», также имеет доступ к данным «конфиденциально» и «общий доступ».

При разграничении по категориям задается и контролируется ранг категории пользователей. Соответственно, все ресурсы информационной системы разделяются по уровням важности, причем определенному уровню соответствует категория пользователей. В

качестве примера, где используются категории пользователей, приведем операционную систему Windows XP, подсистема безопасности которой по умолчанию поддерживает следующие категории (группы) пользователей: «администратор», «опытный пользователь», «пользователь» и «гость». Каждая из категорий имеет определенный набор прав. Применение категорий пользователей позволяет упростить процедуры назначения прав пользователей за счет применения групповых политик безопасности.

Парольное разграничение представляет использование методов доступа субъектов к объектам по паролю. При этом используются все методы парольной защиты. Очевидно, что постоянное использование паролей создает неудобства пользователям и временные задержки. Поэтому указанные методы используют в исключительных ситуациях.

На практике обычно сочетают различные методы разграничения доступа. Например, первые три метода усиливают парольной защитой.

Разграничение прав доступа является обязательным элементом защищенной информационной системы.

Мандатное и дискретное управление доступом

В ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации» и в документах Гостехкомиссии РФ определены два вида (принципа) разграничения доступа:

- дискретное управление доступом;
- мандатное управление доступом.

Дискретное управление доступом представляет собой разграничение доступа между поименованными субъектами и поименованными объектами. Субъект с определенным правом доступа может передать это право любому другому субъекту. Данный вид организуется на базе методов разграничения по спискам или с помощью матрицы.

Мандатное управление доступом основано на сопоставлении меток конфиденциальности информации, содержащейся в объектах (файлы, папки, рисунки) и официального разрешения (допуска) субъекта к информации соответствующего уровня конфиденциальности.

При внимательном рассмотрении можно заметить, что дискретное управление доступом есть не что иное, как произвольное управление

доступом, а мандатное управление реализует принудительное управление доступом.

4.4. Регистрация и аудит

Определение и содержание регистрации и аудита информационных систем

Регистрация является еще одним механизмом обеспечения защищенности информационной системы. Этот механизм основан на подотчетности системы обеспечения безопасности, фиксирует все события, касающиеся безопасности, такие как:

- вход и выход субъектов доступа;
- запуск и завершение программ;
- выдача печатных документов;
- попытки доступа к защищаемым ресурсам;
- изменение полномочий субъектов доступа;
- изменение статуса объектов доступа и т. д.

Для сертифицируемых по безопасности информационных систем список контролируемых событий определен рабочим документом Гостехкомиссии РФ: «Положение о сертификации средств и систем вычислительной техники и связи по требованиям безопасности информации».

Эффективность системы безопасности принципиально повышается в случае дополнения механизма регистрации механизмом аудита. Это позволяет оперативно выявлять нарушения, определять слабые места в системе защиты, анализировать закономерности системы, оценивать работу пользователей и т. д.

Аудит – это анализ накопленной информации, проводимый оперативно в реальном времени или периодически (например, раз в день). Оперативный аудит с автоматическим реагированием на выявленные нештатные ситуации называется активным.

Реализация механизмов регистрации и аудита позволяет решать следующие задачи обеспечения информационной безопасности:

- обеспечение подотчетности пользователей и администраторов;
- обеспечение возможности реконструкции последовательности событий;

- обнаружение попыток нарушений информационной безопасности;
- предоставление информации для выявления и анализа проблем.

Рассматриваемые механизмы регистрации и аудита являются сильным психологическим средством, напоминающим потенциальным нарушителям о неотвратимости наказания за несанкционированные действия, а пользователям – за возможные критические ошибки. Практическими средствами регистрации и аудита являются:

- различные системные утилиты и прикладные программы;
- регистрационный (системный или контрольный)журнал.

Первое средство является обычно дополнением к мониторингу, осуществляемого администратором системы. Комплексный подход к протоколированию и аудиту обеспечивается при использовании регистрационного журнала.

Регистрационный журнал – это хронологически упорядоченная совокупность записей результатов деятельности субъектов системы, достаточная для восстановления, просмотра и анализа последовательности действий, окружающих или приводящих к выполнению операций, процедур или совершению событий при транзакции с целью контроля конечного результата.

Обнаружение попыток нарушений информационной безопасности входит в функции активного аудита, задачами которого является оперативное выявление подозрительной активности и предоставление средств для автоматического реагирования на нее.

Под ***подозрительной активностью*** понимается поведение пользователя или компонента информационной системы, являющееся злоумышленным (в соответствии с заранее определенной политикой безопасности) или нетипичным (согласно принятым критериям).

Например, подсистема аудита, отслеживая процедуру входа (регистрации) пользователя в систему подсчитывает количество неудачных попыток входа. В случае превышения установленного порога таких попыток подсистема аудита формирует сигнал о блокировке учетной записи данного пользователя.

Этапы регистрации и методы аудита событий информационной системы

Организация регистрации событий, связанных с безопасностью информационной системы включает как минимум три этапа:

1) сбор и хранение информации о событиях;
2) защита содержимого журнала регистрации;
3) анализ содержимого журнала регистрации.

На первом этапе определяются данные, подлежащие сбору и хранению, период чистки и архивации журнала, степень централизации управления, место и средства хранения журнала, возможность регистрации шифрованной информации и др.

Регистрируемые данные должны быть защищены, в первую очередь, от несанкционированной модификации и, возможно, раскрытия.

Самым важным этапом является анализ регистрационной информации. Известны несколько методов анализа информации с целью выявления несанкционированных действий.

Статистические методы основаны на накоплении среднестатистических параметров функционирования подсистем и сравнении текущих параметров с ними.

Наличие определенных отклонений может сигнализировать о возможности появления некоторых угроз.

Эвристические методы используют модели сценариев несанкционированных действий, которые описываются логическими правилами, или модели действий, по совокупности приводящие к несанкционированным действиям.

4.5. Межсетевое экранирование

Классификация межсетевых экранов

Одним из эффективных механизмов обеспечения информационной безопасности в распределенных вычислительных сетях является экранирование, выполняющее функции разграничения информационных потоков на границе защищаемой сети.

Межсетевое экранирование повышает безопасность объектов внутренней сети за счет игнорирования неавторизованных запросов из внешней среды, тем самым обеспечивая все составляющие информационной безопасности. Кроме функций разграничения

доступа, экранирование обеспечивает регистрацию информационных обменов.

Функции экранирования выполняет ***межсетевой экран*** или брандмауэр (firewall), под которым понимают программную или программно-аппаратную систему, которая выполняет контроль информационных потоков, поступающих в информационную систему и/или выходящих из нее, и обеспечивает защиту информационной системы посредством фильтрации информации. Фильтрация информации состоит в анализе информации по совокупности критериев и принятии решения о ее приеме и/или передаче.

Межсетевые экраны классифицируются по следующим признакам:

- по месту расположения в сети – на внешние и внутренние, обеспечивающие защиту соответственно от внешней сети или защиту между сегментами сети;
- по уровню фильтрации, соответствующему эталонной модели OSI/ISO.

Внешние межсетевые экраны обычно работают только с протоколом TCP/IP глобальной сети Интернет. Внутренние сетевые экраны могут поддерживать несколько протоколов, например, при использовании сетевой операционной системы Novell Netware следует принимать во внимание протокол SPX/IPX.

Характеристика межсетевых экранов

Работа всех межсетевых экранов основана на использовании информации разных уровней модели OSI. Как правило, чем выше уровень модели OSI, на котором межсетевой экран фильтрует пакеты, тем выше обеспечиваемый им уровень защиты.

Межсетевые экраны разделяют на четыре типа:

- межсетевые экраны с фильтрацией пакетов;
- шлюзы сеансового уровня;
- шлюзы прикладного уровня;
- межсетевые экраны экспертного уровня.

Таблица 4

Типы межсетевых экранов и уровни модели ISO OSI

Уровень модели OSI	Протокол	Тип

Прикладной	Telnet, FTP, DNS, NFS, SMTP, HTTP	Шлюз прикладного уровня Межсетевой экран экспертного уровня
Сеансовый	TCP, UDP	Шлюз сеансового уровня
Транспортный	TCP, UDP	
Сетевой	IP, ICMP	Межсетевой экран с фильтрацией пакетов
Канальный	ARP, RAP	
Физический	Ethernet	

Межсетевые экраны с фильтрацией пакетов представляют собой маршрутизаторы или работающие на сервере программы, сконфигурированные таким образом, чтобы фильтровать входящие и исходящие пакеты. Поэтому такие экраны называют иногда пакетными фильтрами. Фильтрация осуществляется путем анализа IP-адреса источника и приемника, а также портов входящих TCP- и UDP-пакетов и сравнением их со сконфигурированной таблицей правил. Эти межсетевые экраны просты в использовании, дешевы, оказывают минимальное влияние на производительность вычислительной системы. Основным недостатком является их уязвимость при подмене адресов IP. Кроме того, они сложны при конфигурировании: для их установки требуется знание сетевых, транспортных и прикладных протоколов.

Шлюзы сеансового уровня контролируют допустимость сеанса связи. Они следят за подтверждением связи между авторизованным клиентом и внешним хостом (и наоборот), определяя, является ли запрашиваемый сеанс связи допустимым. При фильтрации пакетов шлюз сеансового уровня основывается на информации, содержащейся в заголовках пакетов сеансового уровня протокола TCP, т. е. функционирует на два уровня выше, чем межсетевой экран с фильтрацией пакетов. Кроме того, указанные системы обычно имеют функцию трансляции сетевых адресов, которая скрывает внутренние IP-адреса, тем самым исключая подмену IP-адреса. Однако в таких межсетевых экранах отсутствует контроль содержимого пакетов, генерируемых различными службами. Для исключения указанного недостатка применяются шлюзы прикладного уровня.

Шлюзы прикладного уровня проверяют содержимое каждого проходящего через шлюз пакета и могут фильтровать отдельные виды

команд или информации в протоколах прикладного уровня, которые им поручено обслуживать. Это более совершенный и надежный тип межсетевого экрана, использующий программы-посредники (proxies) прикладного уровня или агенты. Агенты составляются для конкретных служб сети Интернет (HTTP, FTP, Telnet и т. д.) и служат для проверки сетевых пакетов на наличие достоверных данных.

Шлюзы прикладного уровня снижают уровень производительности системы из-за повторной обработки в программе-посреднике. Это незаметно в Интернете при работе по низкоскоростным каналам, но существенно при работе во внутренней сети.

Межсетевые экраны экспертного уровня сочетают в себе элементы всех трех описанных выше категорий. Как и межсетевые экраны с фильтрацией пакетов, они работают на сетевом уровне модели OSI, фильтруя входящие и исходящие пакеты на основе проверки IP-адресов и номеров портов. Межсетевые экраны экспертного уровня также выполняют функции шлюза сеансового уровня, определяя, относятся ли пакеты к соответствующему сеансу. И, наконец, брандмауэры экспертного уровня берут на себя функции шлюза прикладного уровня, оценивая содержимое каждого пакета в соответствии с политикой безопасности, выработанной в конкретной организации.

Вместо применения связанных с приложениями программ-посредников, брандмауэры экспертного уровня используют специальные алгоритмы распознавания и обработки данных на уровне приложений. С помощью этих алгоритмов пакеты сравниваются с известными шаблонами данных, что теоретически должно обеспечить более эффективную фильтрацию пакетов.

4.6. Технология виртуальных частных сетей (VPN)

Сущность и содержание технологии виртуальных частных сетей

Технология виртуальных частных сетей (VPN – Virtual Private Network) является одним из эффективных механизмов обеспечения информационной безопасности при передаче данных в распределенных вычислительных сетях.

Виртуальные частные сети являются комбинацией нескольких самостоятельных сервисов (механизмов) безопасности:

- шифрования (с использованием инфраструктуры криптосистем) на выделенных шлюзах (шлюз обеспечивает обмен данными между вычислительными сетями, функционирующими по разным протоколам);
- экранирования (с использованием межсетевых экранов);
- туннелирования.

Сущность технологии VPN заключается в следующем.

На все компьютеры, имеющие выход в Интернет (вместо Интернета может быть и любая другая сеть общего пользования), устанавливается VPN-агенты, которые обрабатывают IP-пакеты, передаваемые по вычислительным сетям.

Перед отправкой IP-пакета VPN-агент выполняет следующие операции:

- анализируется IP-адрес получателя пакета, в зависимости от этого адреса выбирается алгоритм защиты данного пакета (VPN-агенты могут, поддерживать одновременно несколько алгоритмов шифрования и контроля целостности). Пакет может и вовсе быть отброшен, если в настройках VPN-агента такой получатель не значится;
- вычисляется и добавляется в пакет его имитоприставка, обеспечивающая контроль целостности передаваемых данных;
- пакет шифруется (целиком, включая заголовок IP-пакета, содержащий служебную информацию);
- формируется новый заголовок пакета, где вместо адреса получателя указывается адрес его VPN-агента (эта процедура называется инкапсуляцией пакета).

В результате этого обмен данными между двумя локальными сетями снаружи представляется как обмен между двумя компьютерами, на которых установлены VPN-агенты. Всякая полезная для внешней атаки информация, например, внутренние IP-адреса сети, в этом случае недоступна.

При получении IP-пакета выполняются обратные действия:

- из заголовка пакета извлекается информация о VPN-агенте отправителя пакета, если такой отправитель не входит в число разрешенных, то пакет отбрасывается (то же самое происходит при приеме пакета с намеренно или случайно поврежденным заголовком);
- согласно настройкам выбираются криптографические алгоритмы и ключи, после чего пакет расшифровывается и

проверяется его целостность (пакеты с нарушенной целостностью также отбрасываются);

- после всех обратных преобразований пакет в его исходном виде отправляется настоящему адресату по локальной сети.

Все перечисленные операции выполняются автоматически, работа VPN-агентов является незаметной для пользователей. Сложна только настройка VPN-агентов, которая может быть выполнена очень опытным пользователем. VPN-агент может находиться непосредственно на защищаемом компьютере (что особенно полезно для мобильных пользователей). В этом случае он защищает обмен данными только одного компьютера, на котором он установлен.

Понятие «туннеля» при передаче данных в сетях

Для передачи данных VPN-агенты создают виртуальные каналы между защищаемыми локальными сетями или компьютерами (такой канал называется «туннелем», а технология его создания называется «туннелированием»). Вся информация передается по туннелю в зашифрованном виде.

Одной из обязательных функций VPN-агентов является фильтрация пакетов, которая реализуется в соответствии с настройками VPN-агента, совокупность которых образует политику безопасности виртуальной частной сети. Для повышения защищенности виртуальных частных сетей на концах туннелей целесообразно располагать межсетевые экраны.

Контрольные вопросы по разделу №4

1. Что понимается под идентификацией и аутентификацией пользователя?
2. Перечислите возможные идентификаторы при реализации механизмов идентификации и аутентификации.
3. Что такое «электронный ключ»?
4. Какой из видов аутентификации (устойчивая аутентификация или постоянная аутентификация) более надежный?
5. Что входит в состав криптосистемы?
6. Как реализуются симметричный и асимметричный методы шифрования?

7. Что такое электронная цифровая подпись?
8. Перечислите методы разграничения доступа.
9. Какие методы управления доступом предусмотрены в руководящих документах Гостехкомиссии?
10. На чем основан механизм регистрации?
11. Какие события, связанные с безопасностью, подлежат регистрации?
12. Чем отличаются механизмы регистрации и аудита?
13. Какие этапы предусматривают механизмы регистрации и аудита?
14. В чем заключается принцип межсетевого экранирования?
15. Объясните принцип функционирования межсетевых экранов с фильтрацией пакетов.
16. Какие сервисы безопасности включает технология виртуальных частных сетей?
17. Почему при использовании технологии VPN IP-адреса внутренней сети недоступны внешней сети?
18. Чем определяется политика безопасности виртуальной частной сети?

ПРАКТИЧЕСКИЕ ЗАДАНИЯ

ПРАКТИЧЕСКАЯ РАБОТА 1

Восстановление зараженных файлов

Краткие теоретические сведения.

Макровирусы заражают файлы – документы и электронные таблицы популярных офисных приложений [10].

Для анализа макровирусов необходимо получить текст их макросов. Для нешифрованных («не - стелс») вирусов это достигается при помощи меню Сервис/Макрос. Если же вирус шифрует свои макросы или использует «стелс»-приемы, то необходимо воспользоваться специальными утилитами просмотра макросов.

Задание: восстановить файл, зараженный макровирусом

Алгоритм выполнения работы.

Для восстановления документов Word и Excel достаточно сохранить пораженные файлы в текстовый формат RTF, содержащий практически всю информацию из первоначальных документов и не содержащий макросы.

Для этого выполните следующие действия.

1. В программе **WinWord** выберите пункты меню «**Файл**» – «**Сохранить как**».

2. В открывшемся окне в поле «**Тип файла**» выберите «**Текст в формате RTF**» (рис. 7).

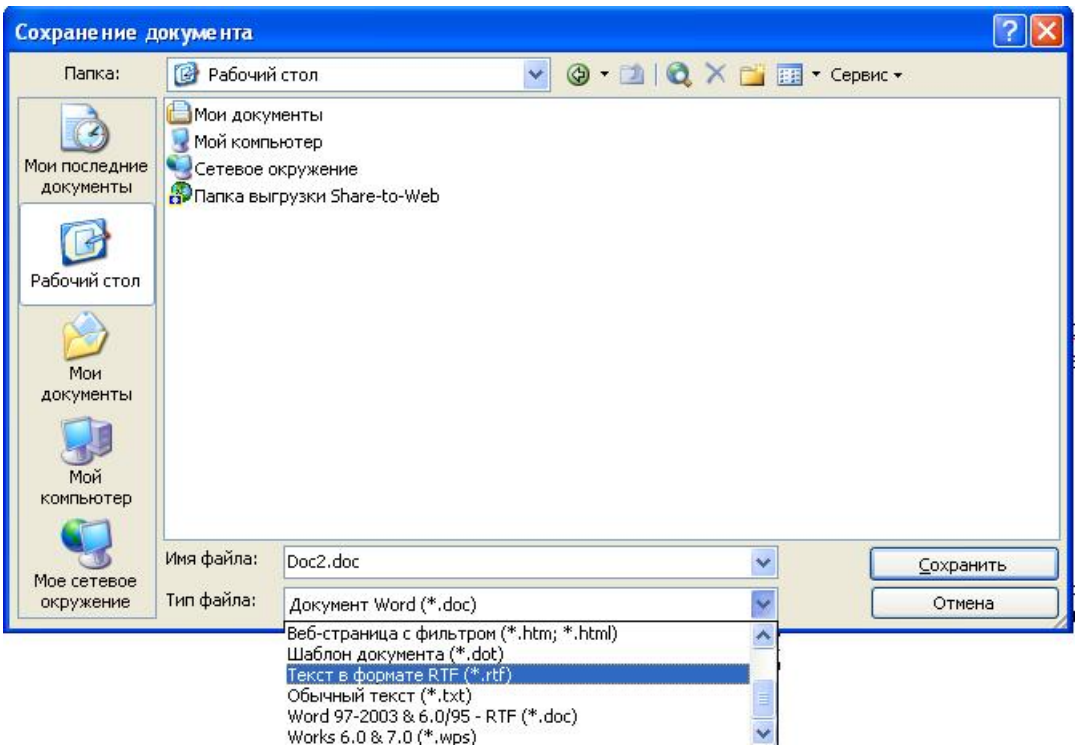

Рис. 7. Выбор типа файла

3. Выберите команду **Сохранить**, при этом имя файла оставьте прежним.

4. В результате появится новый файл с именем существующего, но с другим расширением.

5. Далее закройте **WinWord** и удалите все зараженные Word-документы и файл-шаблон **NORMAL.DOT** в папке **WinWord**.

6. Запустите **WinWord** и восстановите документы из RTF-файлов в соответствующий формат файла (рис. 8) с расширением (.doc).

7. В результате этой процедуры вирус будет удален из системы, а практически вся информация останется без изменений.

Примечание:

а) этот метод рекомендуется использовать, если нет соответствующих антивирусных программ;

б) при конвертировании файлов происходит потеря невирусных макросов, используемых при работе. Поэтому перед запуском описанной процедуры следует сохранить их исходный текст, а после обезвреживания вируса – восстановить необходимые макросы в первоначальном виде.

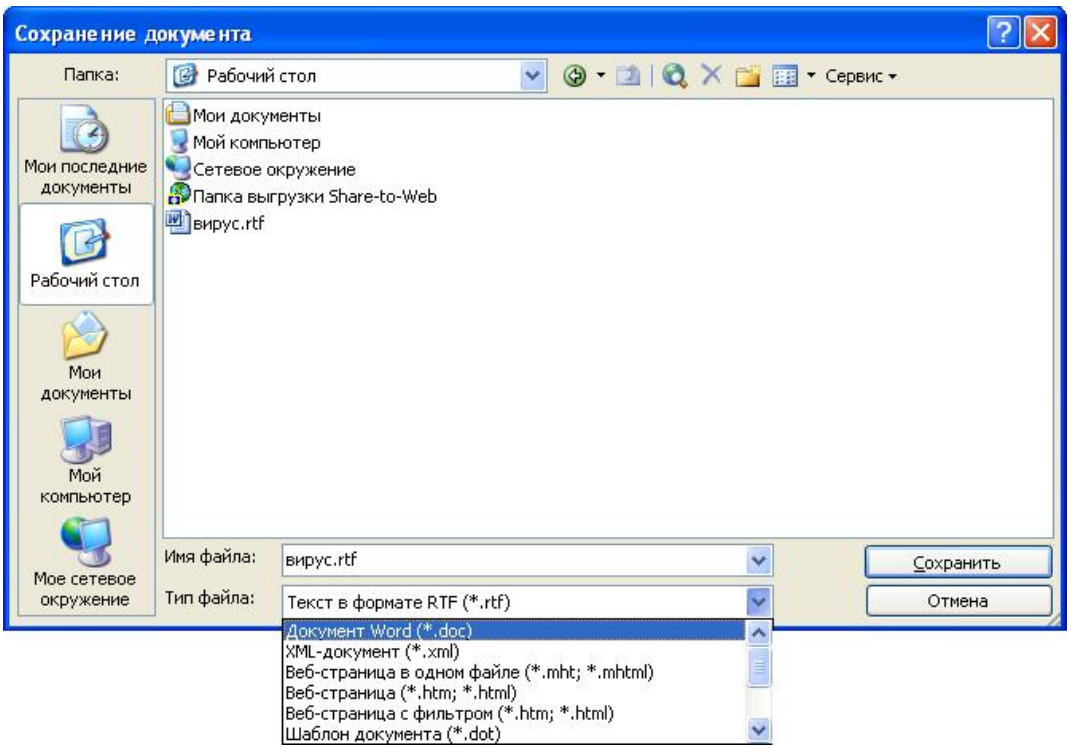

Рис. 8. Восстановление файла

8. Для последующей защиты файлов от макровирусов включите защиту от запуска макросов.

9. Для этого в **WinWord** выберите последовательно пункты меню: **Сервис - Макрос - Безопасность** (рис. 9).

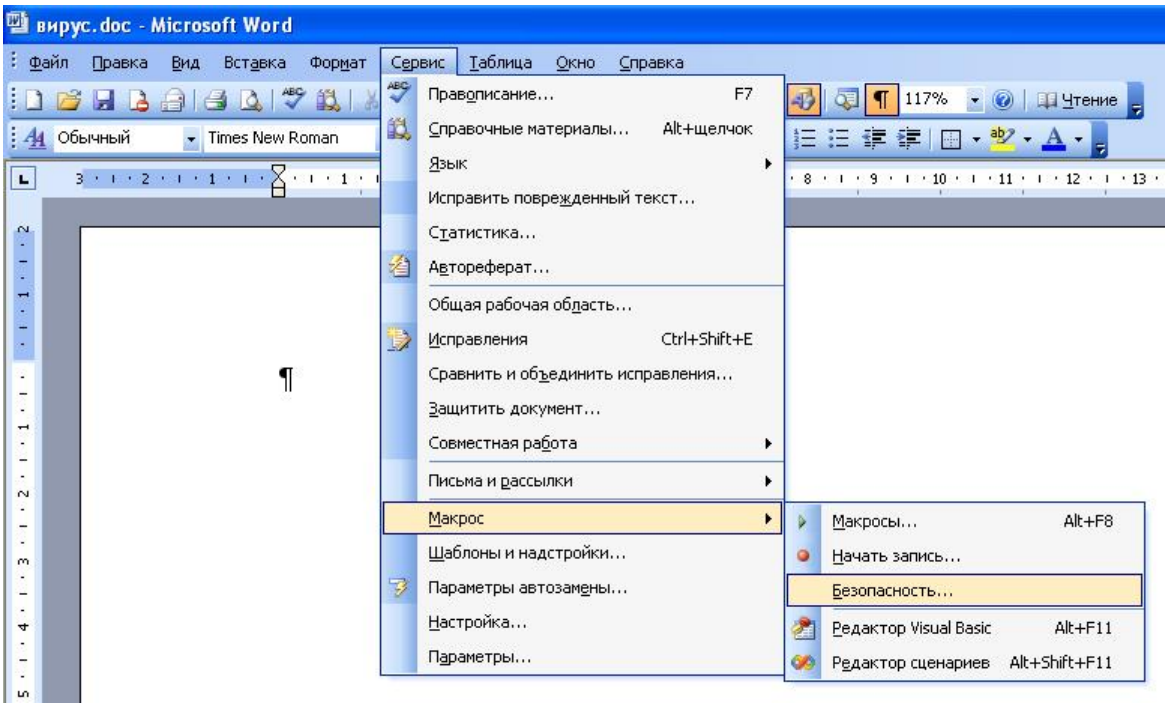

Рис. 9. Защита от макровирусов

10. В открывшемся окне на закладке **Уровень безопасности** отметьте пункт **Высокая** (рис. 10).

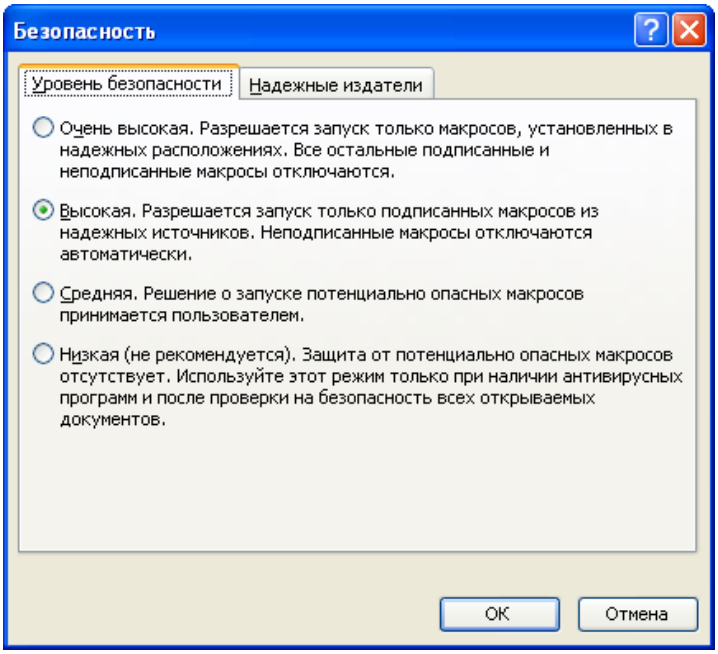

Рис. 10. Выбор уровня безопасности

Задания для самостоятельной работы

1. Создайте файл **virus.doc** (содержание – чистый лист) и выполните алгоритм восстановления файла (в предположении его заражения макровирусом).

2. Зафиксируйте этапы работы, используя команду **PrintScreen** клавиатуры (скопированные таким образом файлы вставьте в новый Word-документ для отчета преподавателю).

3. Сравните размеры файлов **virus.doc** и **virus.rtf**, используя пункт контекстного меню **Свойства** (для этого выделите в **Проводнике** файл, нажмите правую кнопку мыши и выберите пункт **Свойства**).

Контрольные вопросы

1. Какие файлы заражают макровирусы?
2. Как просмотреть код макровируса?
3. Как восстановить файл, зараженный макровирусом?

ПРАКТИЧЕСКАЯ РАБОТА 2
Профилактика проникновения «троянских программ»

Краткие теоретические сведения

Главное отличие «троянских программ» от компьютерных вирусов состоит в том, что они не размножаются на зараженном компьютере и не имеют встроенных возможностей к самораспространению. “Троянские кони” засылаются пользователям (обычно через электронную почту) непосредственно их авторами под видом каких-нибудь полезных утилит. На самом деле они производят несанкционированное внедрение на компьютеры и в корпоративные сети различного рода нежелательных программ. Именно этой особенности “Троянские кони” обязаны своим названием.

Троянские программы различаются между собой по тем действиям, которые они производят на зараженном компьютере.

Backdoor – троянские утилиты удаленного администрирования

Троянские программы этого класса являются утилитами удаленного администрирования компьютеров в сети. По своей функциональности они во многом напоминают различные системы администрирования, разрабатываемые и распространяемые фирмами-производителями программных продуктов.

Единственная особенность этих программ заставляет классифицировать их как вредные троянские программы: отсутствие предупреждения об инсталляции и запуске. При запуске «троянец» устанавливает себя в системе и затем следит за ней, при этом пользователю не выдается никаких сообщений о действиях троянца в системе. Более того, ссылка на «троянца» может отсутствовать в списке активных приложений. В результате «пользователь» этой троянской программы может и не знать о ее присутствии в системе, в то время как его компьютер открыт для удаленного управления.

Утилиты скрытого управления позволяют делать с компьютером все, что в них заложил автор: принимать или отсылать файлы, запускать и уничтожать их, выводить сообщения, стирать информацию, перезагружать компьютер и т. д. В результате эти троянцы могут быть использованы для обнаружения и передачи конфиденциальной информации, для запуска вирусов, уничтожения данных и т.п. – пораженные компьютеры оказываются открытыми для злоумышленных действий хакеров.

Таким образом, троянские программы данного типа являются одним из самых опасных видов вредоносного программного обеспечения, поскольку в них заложена возможность самых разнообразных злоумышленных действий, присущих другим видам троянских программ.

Отдельно следует отметить группу бэкдоров, способных распространяться по сети и внедряться в другие компьютеры, как это делают компьютерные черви. Отличает такие «троянцы» от червей тот факт, что они распространяются по сети не самопроизвольно (как черви), а только по специальной команде «хозяина», управляющего данной копией троянской программы.

Trojan-PSW – воровство паролей

Данное семейство объединяет троянские программы, «ворующие» различную информацию с зараженного компьютера, обычно –системные пароли (PSW – Password-Stealing-Ware). При запуске PSW-троянцы ищут системные файлы, хранящие различную конфиденциальную информацию (обычно номера телефонов и пароли доступа к интернету) и отсылают ее по указанному в коде «троянца» электронному адресу или адресам.

Существуют PSW-троянцы, которые сообщают и другую информацию о зараженном компьютере, например, информацию о системе (размер памяти и дискового пространства, версия операционной системы), тип используемого почтового клиента, IP-адрес и т.п. Некоторые троянцы данного типа «воруют» регистрационную информацию к различному программному обеспечению, коды доступа к сетевым играм и прочее.

Trojan-AOL – семейство троянских программ, «ворующих» коды доступа к сети AOL (America Online). Выделены в особую группу по причине своей многочисленности.

Trojan-Clicker – интернет-кликеры

Семейство троянских программ, основная функция которых – организация несанкционированных обращений к интернет-ресурсам (обычно к веб-страницам). Достигается это либо посылкой соответствующих команд браузеру, либо заменой системных файлов, в которых указаны «стандартные» адреса интернет-ресурсов (например, файл hosts в MS Windows).

У злоумышленника могут быть следующие цели для подобных действий:

- увеличение посещаемости каких-либо сайтов с целью увеличения показов рекламы;
- организация DoS-атаки (Denial of Service) на какой-либо сервер;
- привлечение потенциальных жертв для заражения вирусами или троянскими программами.

Trojan-Downloader – доставка прочих вредоносных программ

Троянские программы этого класса предназначены для загрузки и установки на компьютер-жертву новых версий вредоносных программ, установки «троянцев» или рекламных систем. Загруженные из интернета программы затем либо запускаются на выполнение, либо регистрируются «троянцем» на автозагрузку в соответствии с возможностями операционной системы. Данные действия при этом происходят без ведома пользователя.

Информация об именах и расположении загружаемых программ содержится в коде и данных троянца или скачивается троянцем с «управляющего» интернет-ресурса (обычно с веб-страницы).

Trojan-Dropper – инсталляторы прочих вредоносных программ

Троянские программы этого класса написаны в целях скрытной инсталляции других программ и практически всегда используются для «подсовывания» на компьютер-жертву вирусов или других троянских программ.

Данные троянцы обычно без каких-либо сообщений (либо с ложными сообщениями об ошибке в архиве или неверной версии операционной системы) сбрасывают на диск в какой-либо каталог (в корень диска C:, во временный каталог, в каталоги Windows) другие файлы и запускают их на выполнение.

Обычно структура таких программ следующая:

Основной код
Файл 1
Файл 2
...

«Основной код» выделяет из своего файла остальные компоненты (файл 1, файл 2, ...), записывает их на диск и открывает их (запускает на выполнение).

Обычно один (или более) компонент является троянской программой, и как минимум один компонент является «обманкой»: программой-шуткой, игрой, картинкой или чем-то подобным. «Обманка» должна отвлечь внимание пользователя и/или продемонстрировать то, что запускаемый файл действительно делает что-то «полезное», в то время как троянская компонента инсталлируется в систему.

В результате использования программ данного класса хакеры достигают двух целей:

- скрытная инсталляция троянских программ и/или вирусов;
- защита от антивирусных программ, поскольку не все из них в состоянии проверить все компоненты внутри файлов этого типа.

Trojan-Proxy – троянские прокси-сервера

Семейство троянских программ, скрытно осуществляющих анонимный доступ к различным интернет-ресурсам. Обычно используются для рассылки спама.

Trojan-Spy – шпионские программы

Данные троянцы осуществляют электронный шпионаж за пользователем зараженного компьютера: вводимая с клавиатуры информация, снимки экрана, список активных приложений и действия пользователя с ними сохраняются в какой-либо файл на диске и периодически отправляются злоумышленнику.

Троянские программы этого типа часто используются для кражи информации пользователей различных систем онлайновых платежей и банковских систем.

Trojan – прочие троянские программы

К данным троянцам относятся те из них, которые осуществляют прочие действия, попадающие под определение троянских программ, т.е. разрушение или злонамеренная модификация данных, нарушение работоспособности компьютера и прочее.

В данной категории также присутствуют «многоцелевые» троянские программы, например, те из них, которые одновременно шпионят за пользователем и предоставляют proxy-сервис удаленному злоумышленнику.

Trojan-Notifier – оповещение об успешной атаке

Троянцы данного типа предназначены для сообщения своему «хозяину» о зараженном компьютере. При этом на адрес «хозяина»

отправляется информация о компьютере, например, IP-адрес компьютера, номер открытого порта, адрес электронной почты и т.п. Отсылка осуществляется различными способами: электронным письмом, специально оформленным обращением к веб-странице «хозяина», ICQ-сообщением.

Данные троянские программы используются в многокомпонентных троянских наборах для извещения своего «хозяина» об успешной инсталляции троянских компонент в атакуемую систему.

Реестр операционной системы Windows – это большая база данных, где хранится информация о конфигурации системы. Этой информацией пользуются как операционная система Windows, так и другие программы. Реестр содержит данные, к которым Windows XP постоянно обращается во время загрузки, работы и её завершения, а именно:

- профили всех пользователей, то есть их настройки;
- конфигурация оборудования, установленного в операционной системе.
- данные об установленных программах и типах документов, создаваемых каждой программой;
- свойства папок и значков программ;
- данные об используемых портах.

Реестр имеет иерархическую древовидную структуру, состоящую из разделов, подразделов и ключей (параметров).

В некоторых случаях восстановить работоспособность системы после сбоя можно, загрузив работоспособную версию реестра, но для этого, естественно, необходимо иметь копию реестра. Основным средством для просмотра и редактирования записей реестра служит специализированная утилита «**Редактор реестра**».

Файл редактора реестра находится в папке Windows. Называется он **regedit.exe**. Для того, чтобы запустить эту программу, необходимо выбрать **Пуск** – **Выполнить** – **regedit.exe**. После запуска появится окно редактора реестра. Вы увидите список из 5 разделов (рис. 11):

- HKEY_CLASSES_ROOT.
- HKEY_CURRENT_USER.
- HKEY_LOCAL_MACHINE.
- HKEY_USERS.

- HKEY_CURRENT_CONFIG.

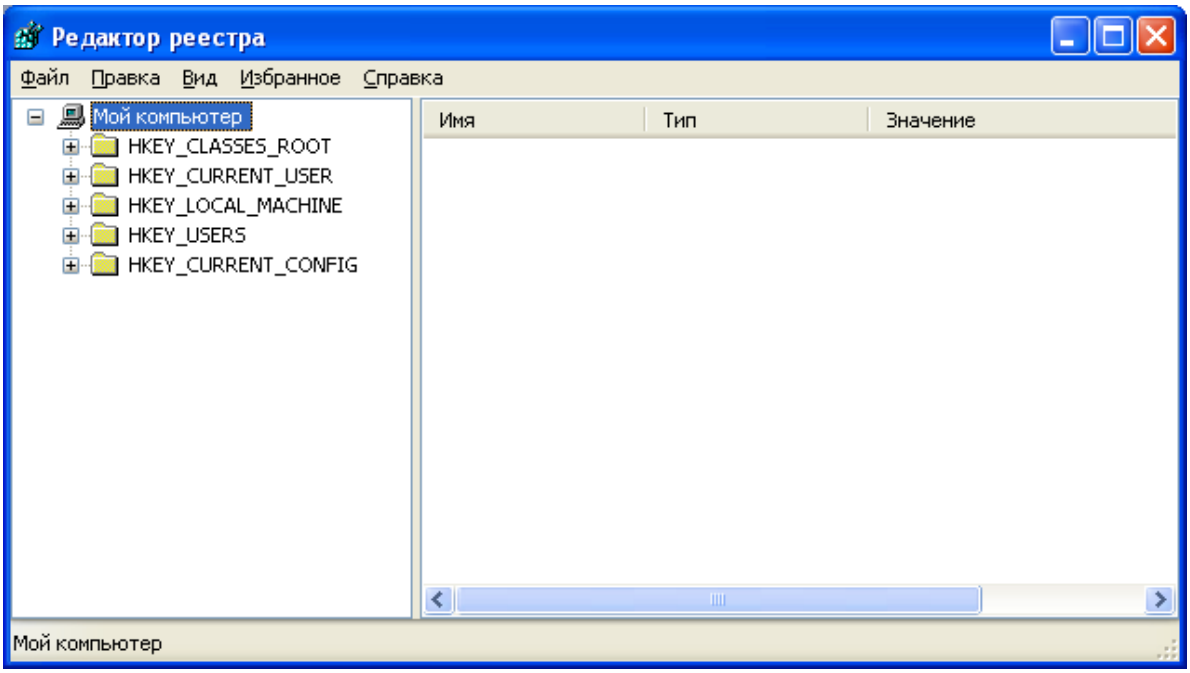

Рис. 11. Редактор реестра

Работа с разделами реестра аналогична работе с папками в Проводнике. Конечным элементом дерева реестра являются ключи или параметры, делящиеся на три типа (рис. 12):

- строковые (напр. «C:\Windows»);
- двоичные (напр. 10 82 AO 8F);
- DWORD - этот тип ключа занимает 4 байта и отображается в шестнадцатеричном и в десятичном виде (например, 0x00000020 (32)).

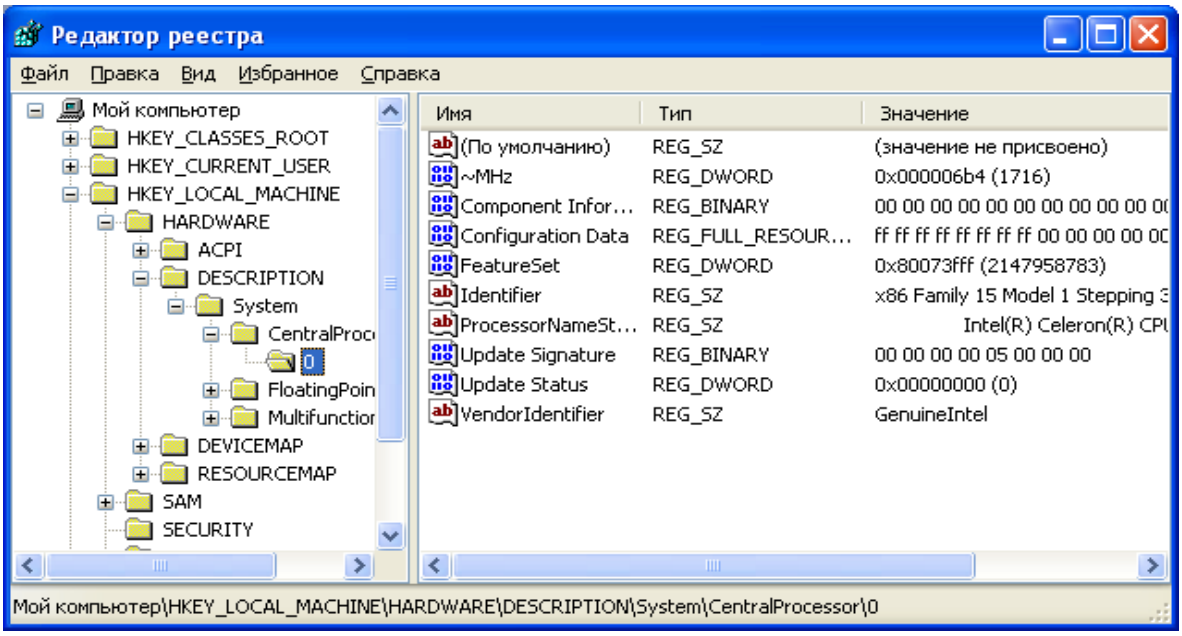

Рис. 12. Типы ключей

В Windows системная информация разбита на так называемые ульи (hive). Это обусловлено принципиальным отличием концепции безопасности этих операционных систем. Имена файлов ульев и пути к каталогам, в которых они хранятся, расположены в разделе **HKEY_LOCAL_MACH1NE\SYSTEM\CurrentControlSet\Control\ hivelist** (рис. 13).

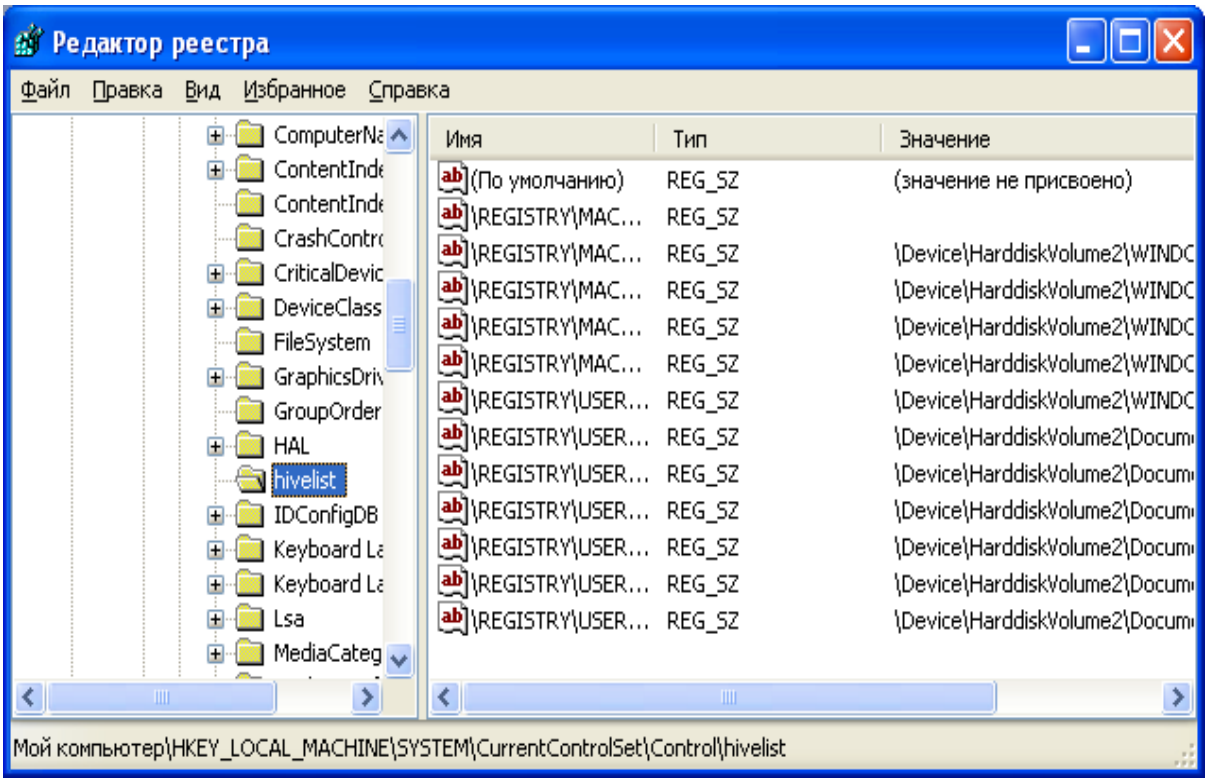

Рис. 13. Ульи

В таблице 1 даны краткие описания ульев реестра и файлов, в которых хранятся параметры безопасности.

Таблица 5

Характеристика основных разделов системного реестра

HKEY_LOCAL_MACHINE\SAM	Содержит информацию SAM (Security Access Manager), хранящуюся в файлах SAM, SAM.LOG, SAM.SAV в папке %System-root%\System32\Config
HKEY_LOCAL_MACHINE\SECURITY	Содержит информацию безопасности в файлах SECURITY, SECURITY.LOG, SECURITY.SAV в папке \%Systemroot%\System32\Config
HKEY_LOCAL_MACHINE\SYSTEM	Содержит информацию об аппаратных профилях этого подраздела. Информация хранится в файлах SYSTEM, SYSTEM.LOG, SYSTEM.SAV в папке \%Systemroot%\System32\Config
HKEY_CURRENT_CONFIG	Содержит информацию о подразделе System этого улья, которая хранится в файлах SYSTEM.SAV и SYSTEM.ALT в папке \%Systemroot%\System32\Config
HKEY_USERS\.DEFAULT	Содержит информацию, которая будет использоваться для создания профиля нового пользователя, впервые регистрирующегося в системе. Информация хранится в файлах DEFAULT, DEFAULT.LOG, DEFAULT.SAV в папке \%Systemroot%\System32\Config
HKEY_CURRENT_USER	Содержит информацию о пользователе, зарегистрированном в системе на текущий момент. Эта информация хранится в файлах NTUSER.DAT и NTUSER.DAT.LOG, расположенных в каталоге \%Systemroot%\Profiles\User name, где User name – имя пользователя

Задание: проверить потенциальные места записей «троянских программ» в системном реестре операционной системы Windows 2000 (XP).

Алгоритм выполнения работы

Потенциальными местами записей «троянских программ» в системном реестре являются разделы, описывающие программы, запускаемые автоматически при загрузке операционной системы от имени пользователей и системы.

1. Запустите программу **regedit.exe**.
2. В открывшемся окне выберите ветвь **HKEY_LOCAL_MACHINE** и далее **Software\ Microsoft\ WindowsNT\ CurrentVersion\ Winlogon** (щелкнуть по значку «папка»).
3. В правой половине открытого окна программы **regedit.exe** появится список ключей.
4. Найдите ключ **Userinit** (**REG_SZ**) и проверьте его содержимое.
5. По умолчанию (исходное состояние) 151 этот ключ содержит следующую запись **C:\WINDOWS\system32\userinit.exe** (рис. 14).

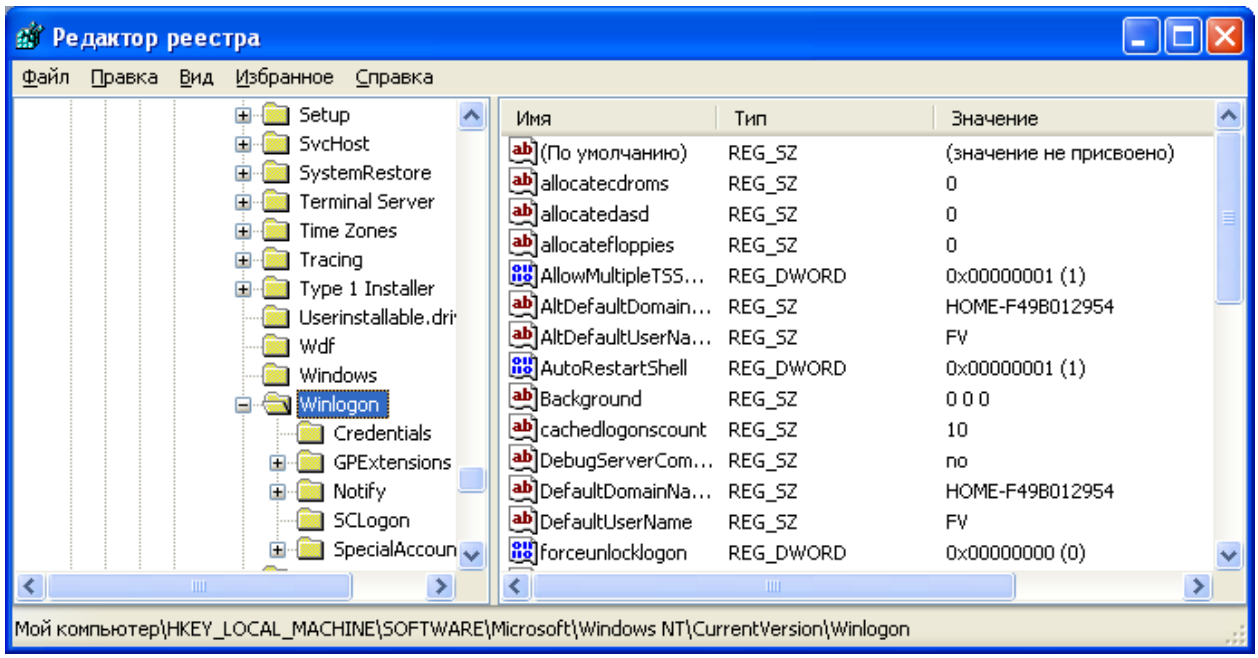

Рис. 14. Ключ Userinit

6. Если в указанном ключе содержатся дополнительные записи, то это могут быть «троянские программы».
7. В этом случае проанализируйте место расположения программы, обратите внимание на время создания файла и сопоставьте с Вашими действиями в это время.

8. Если время создания файла совпадает со временем Вашей работы в Интернете, то возможно, что в это время Ваш компьютер был заражен «троянским конем».

9. Для удаления этой записи необходимо дважды щелкнуть на названии ключа (или при выделенном ключе выбрать команду **Изменить** из меню **Правка** программы **regedit.exe**).

10. В открывшемся окне в поле **Значение** (рис. 15) удалите ссылку на подозрительный файл.

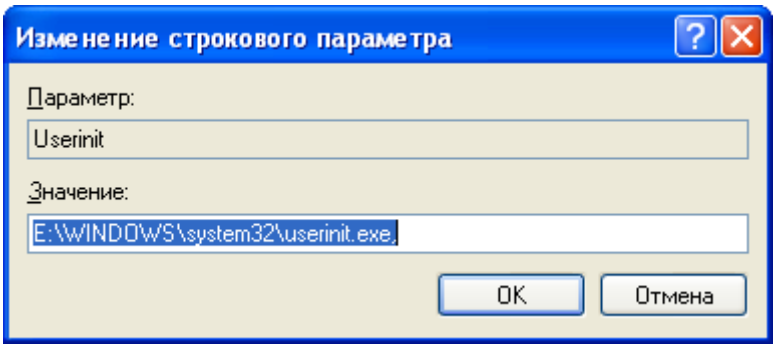

Рис. 15. Удаление ссылки

11. Закройте программу **regedit.exe**.

12. Перейдите в папку с подозрительным файлом и удалите его.

13. Перезагрузите операционную систему и выполните пункты задания 1-4.

14. Если содержимое рассматриваемого ключа не изменилось, то предполагаемый «троянский конь» удален из Вашей системы.

Еще одним потенциальным местом записей на запуск «троянских программ» является раздел автозапуска **Run**.

Для его проверки выполните следующее.

1. Запустите программу **regedit.exe**.

2. В открывшемся окне выберите ветвь **HKEY_LOCAL_MACHINE** и далее **Software**\ **Microsoft**\ **Windows**\ **CurrentVersion**\ **Run**\ ... (**REG_SZ**) (рис. 16).

3.

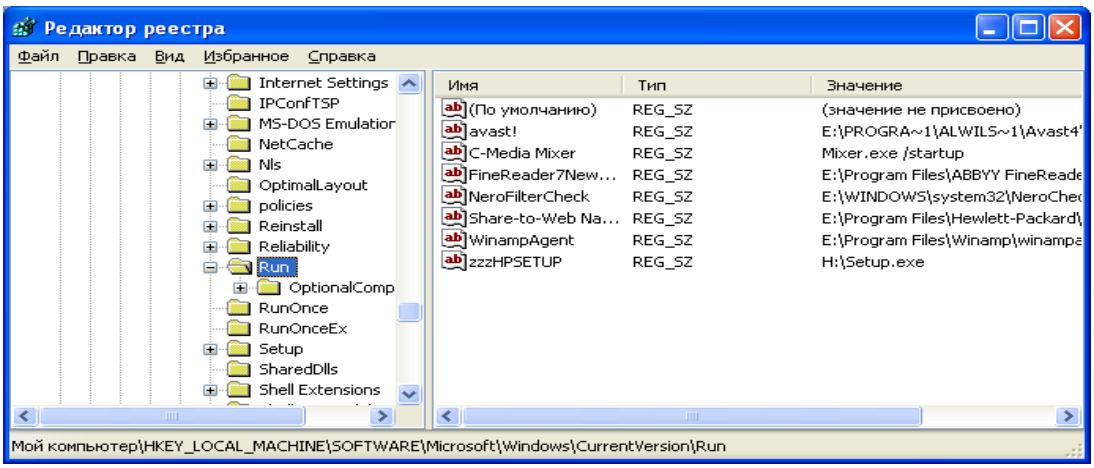

Рис. 16. Раздел автозапуска

4. В рассматриваемом примере автоматически запускается резидентный антивирус и его планировщик заданий, а также утилита, относящаяся к программе Nero (запись на CD).

5. Если в указанном разделе есть записи вызывающие подозрения, то выполните пункты 6-14 предыдущего задания.

Задания для самостоятельной работы

1. Проверьте содержимое ключа HKEY_LOCAL_MACHINE\ Software\ Microsoft\ WindowsNT\ CurrentVersion\ Winlogon\ System (REG_SZ).
2. Зафиксируйте этапы работы, используя команду PrintScreen клавиатуры.
3. Составьте отчет о результатах проверки.

Контрольные вопросы

1. Что такое реестр?
2. Поясните особенности «троянских программ».
3. Почему профилактика «троянских программ» связана с системным реестром?
4. Какие разделы и ключи являются потенциальными местами записей «троянских программ»?

ПРАКТИЧЕСКАЯ РАБОТА 3

Настройка безопасности почтового клиента Outlook Express

Краткие теоретические сведения

Почтовый клиент – это программа, предназначенная для приема и отправки электронной почты. Примером такой программы является программа Outlook Express. Для работы с электронной почтой почтовый клиент должен поддерживать протоколы SMTP (исходящая почта) и POP3 (входящая почта).

Одну из реальных угроз в современных глобальных сетях представляют электронные письма с вложенными программами-вирусами. Именно посредством электронной почты были проведены последние глобальные сетевые атаки. В связи с этим проблема защиты компьютера при работе с электронной почтой приобретает особую актуальность. Аналогично вопрос конфиденциальности и безопасности электронной почты с течением времени не только не теряет своей актуальности, но и ставится все более и более остро. Отправляя конфиденциальную информацию по электронной почте, необходимо иметь уверенность в том, что сообщения не перехватываются и не подделываются.

Outlook Express позволяет использовать цифровые идентификаторы или цифровые удостоверения для защиты электронной почты, в частности, для шифрования почтовых сообщений. По умолчанию Outlook Express автоматически добавляет сертификаты, которые приходят по почте, в адресную книгу Windows.

Цифровой идентификатор состоит из открытого ключа, личного ключа и цифровой подписи. Когда пользователь подписывает отправляемые им сообщения, он добавляет в состав сообщения свою цифровую подпись и открытый ключ. Комбинация цифровой подписи и открытого ключа называется сертификатом.

Цифровая подпись отправителя подтверждает получателю подлинность полученных сообщений. Открытый ключ отправителя получатель может использовать для отправки ему зашифрованной почты, расшифровать которую он сможет с помощью своего личного ключа. Таким образом, чтобы отправить зашифрованные сообщения в чей-либо адрес, необходимо включить в адресную книгу цифровые идентификаторы, ассоциированные с получателями. Благодаря этому

при помощи открытых ключей получателей Вы сможете зашифровывать отправляемые ими сообщения. Каждый получатель расшифрует полученное сообщение с помощью своего личного ключа.

Задание: разработать систему правил по управлению входящими сообщениями в Outlook Express и настроить Outlook Express для передачи сообщений с электронной цифровой подписью.

Алгоритм выполнения работы

А. Создание системы правил по обработке входящих сообщений электронной почты.

Расширенные правила управления сообщениями поддерживают большое количество критериев действий, включая блокирование отправителей сообщения и новые правила для групп новостей.

Для создания правила по обработке входящих сообщений электронной почты выполните следующие действия.

1. Откройте программу **Outlook Express.**
2. Последовательно выполните команды меню **Сервис – Правила для сообщений - Почта.**
3. В результате откроется диалоговое окно (рис. 17) Создать правило для почты.

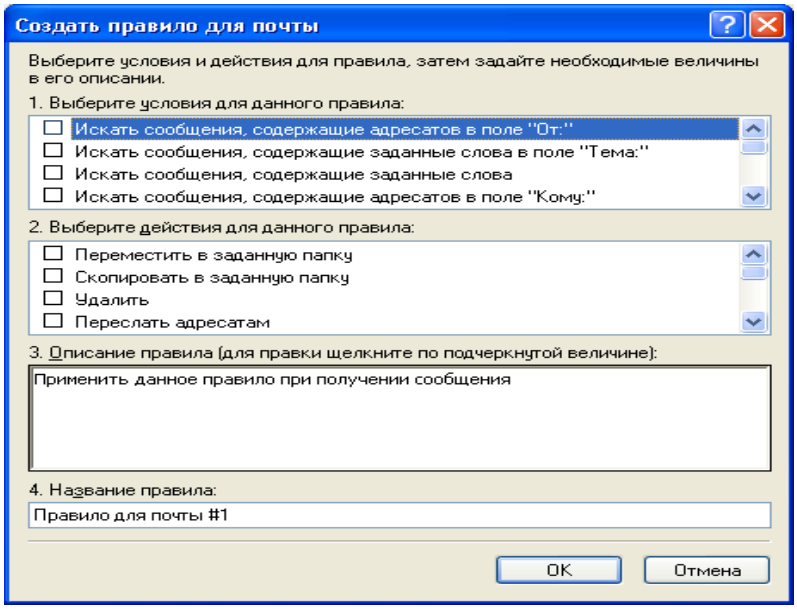

Рис. 17. Создание правила

4. Выберите условие создаваемого правила (например, для защиты от заражения компьютера вложенными в электронное письмо

файлами можно выбрать условие **Искать сообщение с вложениями**, рис. 18).

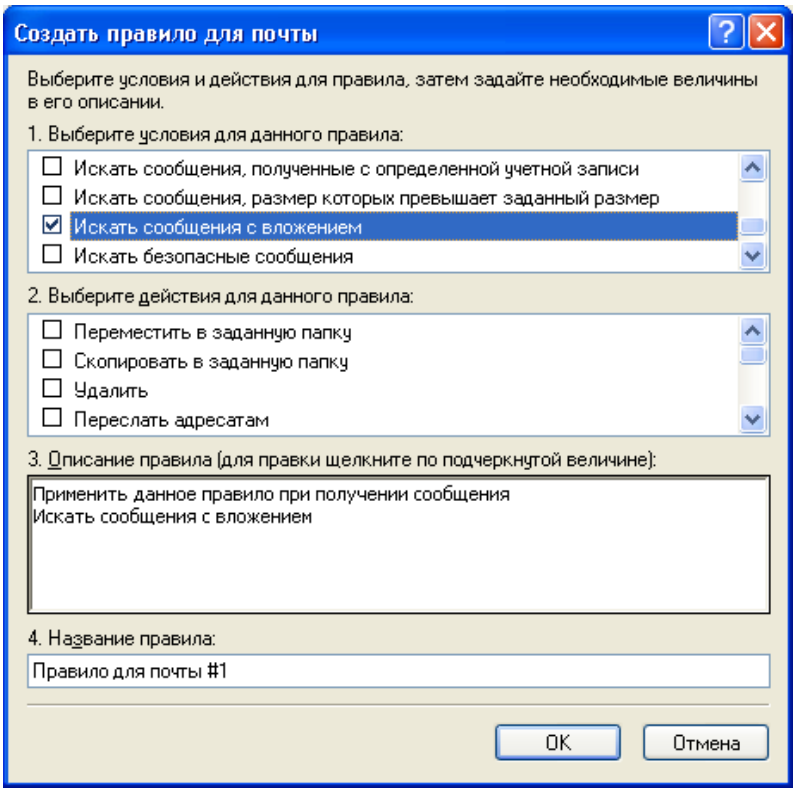

Рис. 18. Условие для правила

5. Выберите действие для данного правила (например, **Удалить с сервера**, рис. 19).

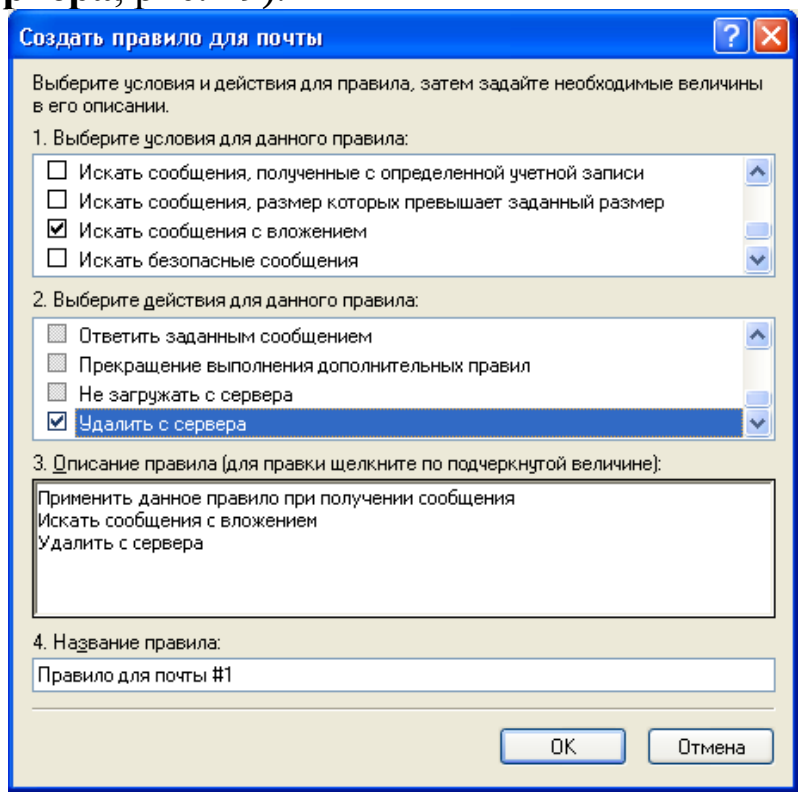

Рис. 19. Действие правила

6. Обратите внимание, что в поле 3 приводится описание созданного правила. После создания этого правила все письма содержащие вложения будут удалены с сервера.

7. Для завершения создания правила введите его имя в поле 4 – **Название правила.**

8. Для успешного создания правила нужно задать хотя бы одно условие. Если задано составное условие (то есть несколько условий), то по умолчанию должно выполниться хотя бы одно из простых условий в поле **Описание правила.**

9. Пример составного условия показан на рис. 20. В результате выполнения этого правила с сервера будут удалены все письма с вложениями, в которых еще в поле «Тема» содержится слово «вирус» (можно задать произвольное слово).

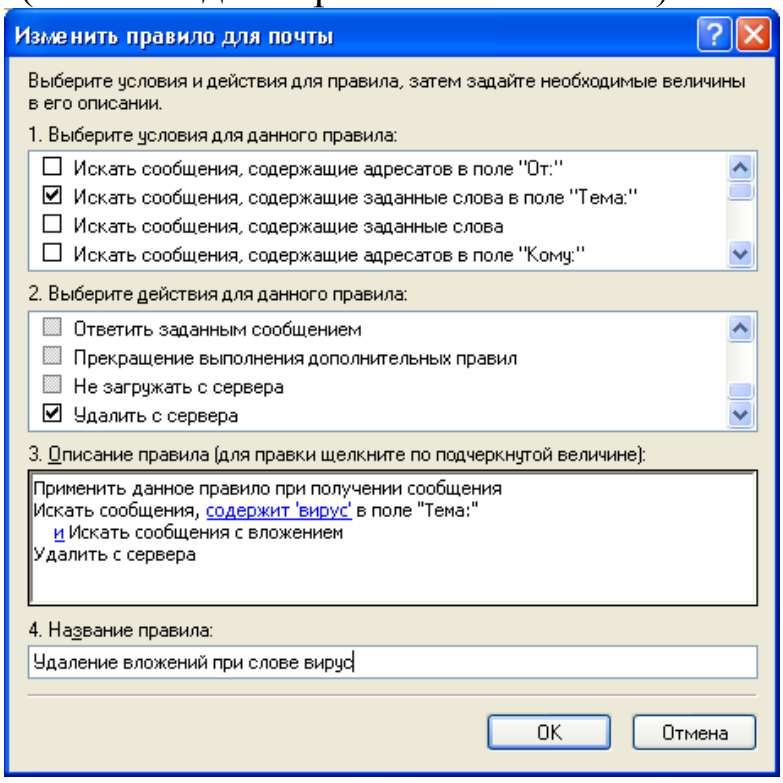

Рис. 20. Составное условие

10. Таким образом, комбинируя правила управления входящими сообщениями, можно существенно повысить защищенность компьютера при работе с электронной почтой.

В. Получение цифрового идентификатора.

Прежде чем отправлять сообщения, подписанные цифровой подписью и зашифрованные, необходимо получить цифровой идентификатор.

1. Для получения цифрового идентификатора необходимо заполнить заявку на получение цифрового идентификатора в организации, уполномоченной предоставлять этот сервис.

2. Для этого в окне **Параметры** (меню **Сервис – Параметры**) на вкладке **Безопасность** нажмите кнопку **Получить сертификат**.

3. В результате запустится веб-браузер, который обратится к странице на веб-узле Microsoft, где приводится перечень организаций, уполномоченных предоставлять этот сервис (например, у компании VeriSign можно бесплатно получить временный (на два месяца) цифровой идентификатор, позволяющий опробовать все режимы безопасности программы Outlook Express).

4. После заполнения формы с запросом на предоставление цифрового идентификатора Вы получите (через несколько минут) почтовое сообщение от VeriSign с инструкциями по установке полученного цифрового идентификатора.

5. Раскройте и прочтите письмо. В точности выполните приведенные в нем инструкции.

6. Подтвердите установку цифрового идентификатора.

С. Использование цифровой электронной подписи.

1. Для отправки сообщения, которое требуется подписать цифровой подписью, создайте новое сообщение.

2. Выберите в меню **Сервис** команду **Цифровая подпись**. В результате напротив поля **Кому** появится символ  подтверждающий включение электронной цифровой подписи (рис. 21).

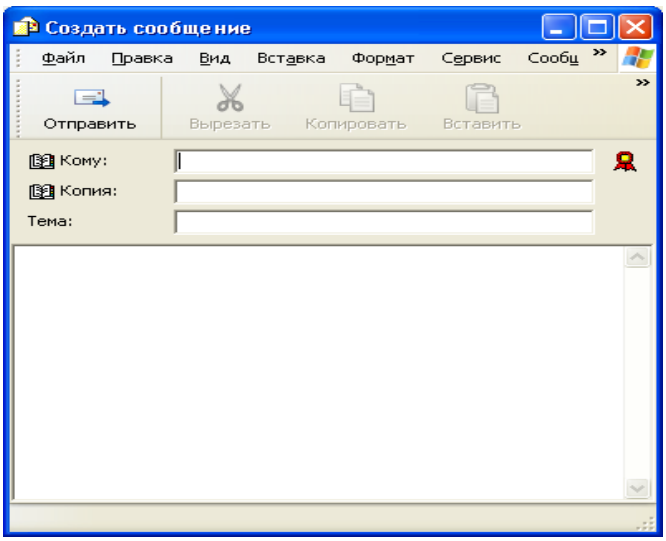

Рис. 21. Включение ЭЦП

3. Если отправляемое сообщение требуется также зашифровать, выберите в меню **Сервис** команду **Зашифровать**. В случае включения шифрования появится символ напротив поля **Копия** (рис. 22).

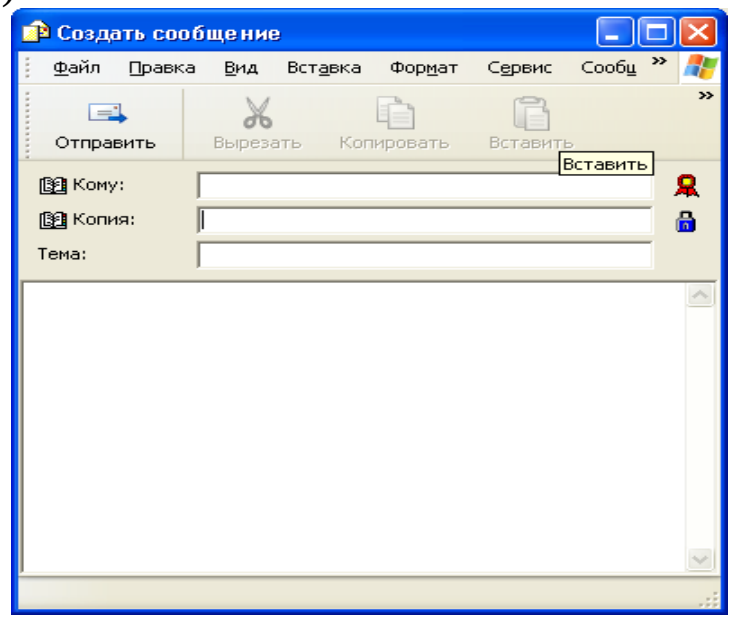

Рис. 22. Шифрование

D. Настройка опций обмена защищенной почтой.

1. Чтобы настроить работу с защищенными почтовыми сообщениями, выберите в меню **Сервис** команду **Параметры** и перейдите на вкладку **Безопасность** (рис. 23).

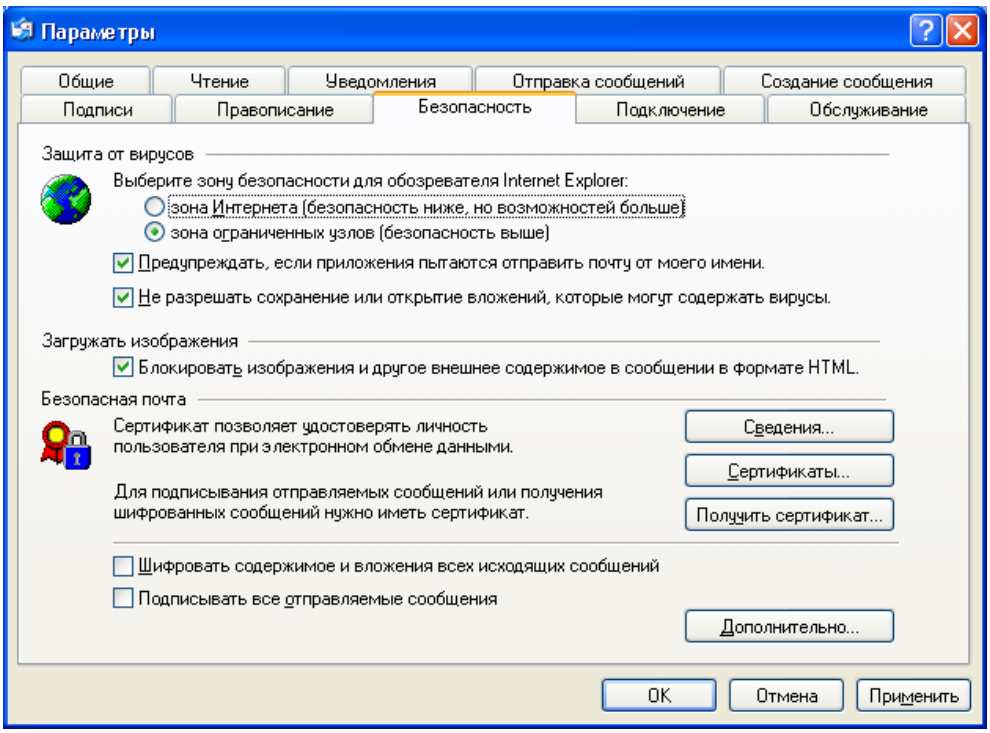

Рис. 23. Защищенная почта

2. Параметры, необходимые для настройки обмена защищенной почтой, находятся в группе **Безопасная почта**, кнопка **Дополнительно** (рис. 24).

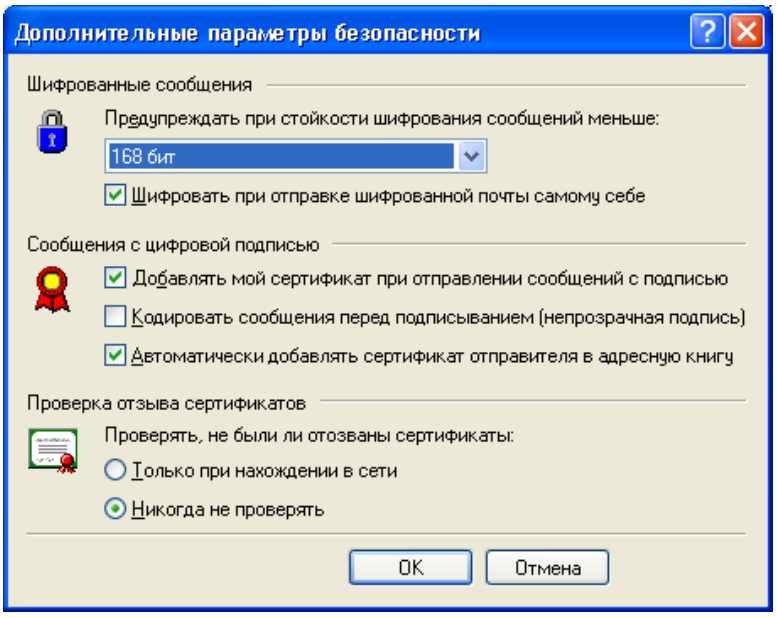

Рис. 24. Параметры защищенной почты

Задания для самостоятельной работы

1. Выполните задания A – D.
2. Создайте три новых правила (произвольных) управления сообщениями электронной почты и опишите их безопасные свойства, то есть как и от каких угроз можно ими защитить компьютер. Составьте отчет.

Контрольные вопросы

1. Для чего используется механизм электронной цифровой подписи?
2. Что понимается под сертификатом?
3. Какой метод шифрования использует электронная цифровая подпись?

ПРАКТИЧЕСКАЯ РАБОТА 4
Настройка параметров аутентификации Windows 2000/XP/7/10

Краткие теоретические сведения

В соответствии с сертификационными требованиями к системам безопасности операционных систем при подключении пользователей должен реализовываться механизм аутентификации и/или идентификации.

Идентификация и аутентификация применяются для ограничения доступа случайных и незаконных субъектов (пользователи, процессы) информационных систем к ее объектам (аппаратные, программные и информационные ресурсы).

Идентификация – присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным.

Аутентификация (установление подлинности) – проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности. Другими словами, аутентификация заключается в проверке: является ли подключающийся субъект тем, за кого он себя выдает.

Настройка параметров аутентификации рассматриваемых операционных систем выполняется в рамках локальной политики безопасности.

Оснастка «Локальная политика безопасности» используется для изменения политики учетных записей и локальной политики на локальном компьютере. При помощи оснастки «Локальная политика безопасности» можно определить:

- кто имеет доступ к компьютеру;
- какие ресурсы могут использовать пользователи на Вашем компьютере;
- включение и отключение записи действий пользователя или группы в журнале событий.

Задание: настроить параметры локальной политики безопасности операционной системы Windows 2000/XP/7/10.

Алгоритм выполнения работы

Для просмотра и изменения параметров аутентификации пользователей выполните следующие действия:

1. Выберите кнопку **Пуск** панели задач.
2. Откройте меню **Настроить – Панель управления**.
3. В открывшемся окне выберите ярлык **Администрирование – Локальная политика безопасности** (рис. 25).

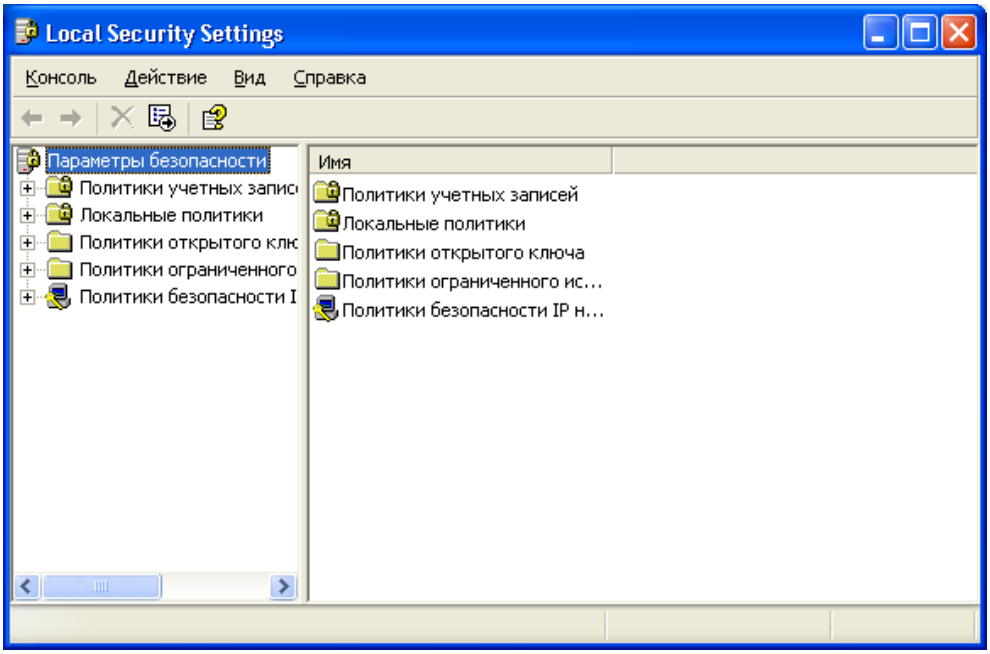

Рис. 25. Политика безопасности

4. Выберите пункт **Политика учетных записей** (этот пункт включает два подпункта: **Политика паролей** и **Политика блокировки учетной записи**).
5. Откройте подпункт **Политика паролей**. В правом окне появится список настраиваемых параметров (рис. 26).

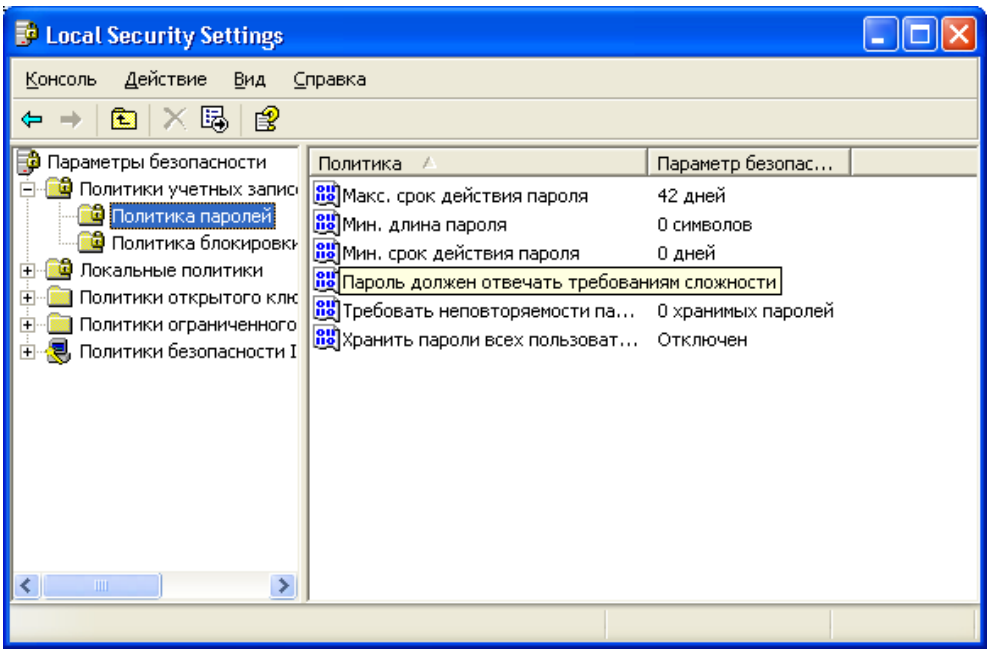

Рис. 26. Политика паролей

6. В показанном примере политика паролей соответствует исходному состоянию системы безопасности после установки операционной системы, при этом ни один из параметров не настроен. Значения параметров приведены в таблице 6.

7. Ознакомьтесь со свойствами всех параметров.

Таблица 6

Значения параметров Политики паролей

Параметр	Значение
Требовать неповторяемости паролей	Определяет число новых паролей, которые должны быть сопоставлены учетной записи пользователя, прежде чем можно будет снова использовать старый пароль. Это значение должно принадлежать диапазону от 0 до 24
Максимальный срок действия пароля	Определяет период времени (в днях), в течение которого можно использовать пароль, прежде чем система потребует от пользователя заменить его. Можно задать значение в диапазоне от 1 до 999 дней или снять всякие ограничения срока действия, установив число дней, равным 0

Минимальный срок действия пароля	Определяет период времени (в днях), в течение которого необходимо использовать пароль, прежде чем пользователь сможет заменить его. Можно задать значение в диапазоне от 1 до 999 дней или разрешить немедленное изменение, установив число дней, равным 0
Минимальная длина пароля	Определяет наименьшее число символов, которые может содержать пароль учетной записи пользователя. Можно задать значение в диапазоне от 1 до 14 символов или отменить использование пароля, установив число символов, равным 0
Пароль должен отвечать требованиям сложности	Определяет, должны ли пароли отвечать требованиям сложности. Если эта политика включена, пароли должны удовлетворять следующим минимальным требованиям. • Пароль не может содержать имя учетной записи пользователя или какую-либо его часть. • Пароль должен состоять не менее чем из шести символов. • В пароле должны присутствовать символы трех категорий из числа следующих четырех: 1) прописные буквы английского алфавита от A до Z; 2) строчные буквы английского алфавита от a до z; 3) десятичные цифры (от 0 до 9); 4) символы, не принадлежащие алфавитно-цифровому набору (например, !, $, #, %). Проверка соблюдения этих требований выполняется при изменении или создании паролей.

Хранить пароли всех пользователей в домене, используя обратимое шифрование	Определяет, следует ли в системах Windows 2000/XP/7/10 хранить пароли, используя обратимое шифрование. Эта политика обеспечивает поддержку приложений, использующих протоколы, которым для проверки подлинности нужно знать пароль пользователя. Хранить пароли, зашифрованные обратимыми методами, - это все равно, что хранить их открытым текстом. Поэтому данную политику следует использовать лишь в исключительных случаях, если потребности приложения оказываются важнее, чем защита пароля

8. Для изменения требуемого параметра выделите его и вызовите его свойства из контекстного меню после нажатия правой кнопки мыши (или дважды щелкните на изменяемом параметре).

9. В результате этого действия появится одно из окон, показанных на рисунке 27.

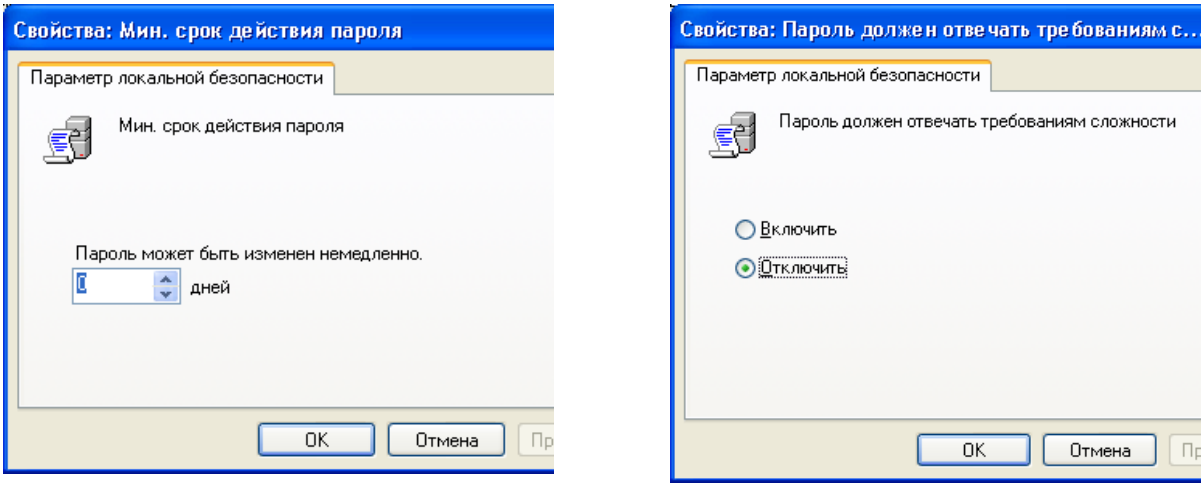

Рис. 27. Изменение параметров

10. Измените значение параметра и нажмите **Ок**.

11. Например (обязательно выполнить и сохранить), выберите параметр **Требовать неповторяемости паролей** и измените его значение на 1.

12. Для настройки **Политики блокировки учетной записи** выберите этот подпункт и откройте его.

13. Значения параметров данного подпункта Политики учетных записей приведены в таблице 7.

14. Ознакомьтесь со свойствами всех параметров.

15. Для изменения параметров воспользуйтесь алгоритмом, описанным в пунктах 8-10.

Задания для самостоятельной работы

1. Измените параметр «**Пароль должен отвечать требованиям сложности**» **Политики паролей** на «**Включен**» (рис. 27) и после этого попробуйте изменить пароль своей учетной записи. Зафиксируйте все сообщения системы, проанализируйте и введите допустимый пароль. Этот пароль является результатом выполнения Вашего задания.

Таблица 7

Значения параметров Политики блокировки учетных записей

Параметр	Значение
Пороговое значение блокировки	Определяет число неудачных попыток входа в систему, после которых учетная запись пользователя блокируется. Блокированную учетную запись нельзя использовать до тех пор, пока она не будет сброшена администратором или пока не истечет ее интервал блокировки. Можно задать значение в диапазоне от 1 до 999 или запретить блокировку данной учетной записи, установив значение 0
Блокировка учетной записи на	Определяет число минут, в течение которых учетная запись остается блокированной, прежде чем будет автоматически разблокирована. Этот параметр может принимать значения от 1 до 99 999 минут. Если установить значение 0, учетная запись будет блокирована на все время до тех пор, пока администратор не разблокирует ее явным образом. Если пороговое значение блокировки определено, данный интервал блокировки должен быть больше или равен интервалу сброса

Сброс счетчика блокировки через	Определяет число минут, которые должны пройти после неудачной попытки входа в систему, прежде чем счетчик неудачных попыток будет сброшен в 0. Этот параметр может принимать значения от 1 до 99 999 минут. Если определено пороговое значение блокировки, данный интервал сброса не должен быть больше интервала **Блокировка учетной записи на**

2. После успешного выполнения первого задания, измените пароль Вашей учетной записи, а в качестве нового пароля укажите прежний пароль. Все сообщения зафиксируйте, проанализируйте и объясните поведение системы безопасности.

3. Проведите эксперименты с другими параметрами **Политики учетных записей.**

Контрольные вопросы

1. Что такое аутентификация и идентификация?
2. Для чего применяются эти механизмы?
3. Что можно настроить с помощью оснастки **Локальная политика безопасности.**

ПРАКТИЧЕСКАЯ РАБОТА 5
Шифрующая файловая система EFS и управление сертификатами в Windows 2000/XP/7/10

Краткие теоретические сведения

Шифрующая файловая система EFS позволяет пользователям хранить данные на диске в зашифрованном виде.

Шифрование – это процесс преобразования данных в формат, не доступный для чтения другим пользователям. После того как файл был зашифрован, он автоматически остается зашифрованным в любом месте хранения на диске.

Расшифровка – это процесс преобразования данных из зашифрованной формы в его исходный формат.

При работе с шифрующей файловой системой EFS следует учитывать следующие сведения и рекомендации.

1. Могут быть зашифрованы только файлы и папки, находящиеся на томах **NTFS.**
2. Сжатые файлы и папки не могут быть зашифрованы. Если шифрование выполняется для сжатого файла или папки, файл или папка преобразуются к состоянию без сжатия.
3. Зашифрованные файлы могут стать расшифрованными, если файл копируется или перемещается на том, не являющийся томом **NTFS.**
4. При перемещении незашифрованных файлов в зашифрованную папку они автоматически шифруются в новой папке. Однако обратная операция не приведет к автоматической расшифровке файлов. Файлы необходимо явно расшифровать.
5. Не могут быть зашифрованы файлы с атрибутом «**Системный**» и файлы в структуре папок системный корневой каталог.
6. Шифрование папки или файла не защищает их от удаления. Любой пользователь, имеющий права на удаление, может удалить зашифрованные папки или файлы.
7. Процесс шифрование является прозрачным для пользователя.

Примечание. Прозрачное шифрование означает, что перед использованием файл не нужно расшифровывать. Можно как обычно открыть файл и изменить его. В системах прозрачного шифрования (шифрования «на лету») криптографические преобразования

осуществляются в режиме реального времени незаметно для пользователя. Например, пользователь записывает подготовленный в текстовом редакторе документ на защищаемый диск, а система защиты в процессе записи выполняет его шифрование.

Использование **EFS** сходно с использованием разрешений для файлов и папок. Оба метода используются для ограничения доступа к данным. Но злоумышленник, получивший несанкционированный физический доступ к зашифрованным файлам и папкам, не сможет их прочитать. При его попытке открыть или скопировать зашифрованный файл или папку появится сообщение, что доступа нет.

Шифрование и расшифровывание файлов выполняется установкой свойств шифрования для папок и файлов, как устанавливаются и другие атрибуты, например, «**только чтение**», «**сжатый**» или «**скрытый**». Если шифруется папка, все файлы и подпапки, созданные в зашифрованной папке, автоматически шифруются. Рекомендуется использовать шифрование на уровне папки. Шифрующая файловая система автоматически создает пару ключей шифрования для пользователя, если она отсутствует. Шифрующая файловая система использует алгоритм шифрования Data Encryption Standard (DESX).

Задание: включить и отключить шифрование файлов шифрующей файловой системой EFS. Экспортировать сертификат с ключами для расшифровки файлов на другом компьютере.

Алгоритм выполнения работы

А. Для включения режима шифрования выполните следующие действия.

1. Укажите файл или папку (например, создайте файл **шифр.doc** в папке **Мои документы**), которую требуется зашифровать, нажмите правую кнопку мыши и выберите в контекстном меню команду **Свойства.**
2. В появившемся окне свойств на вкладке **Общие** нажмите кнопку **Другие**. Появится окно диалога **Дополнительные атрибуты**.
3. В группе **Атрибуты сжатия и шифрования** установите флажок **Шифровать содержимое для защиты данных** и нажмите кнопку «**ОК**».

4. Нажмите кнопку **ОК** в окне свойств зашифровываемого файла или папки, в появившемся окне диалога укажите режим шифрования: **только к этой папке или к этой папке и всем вложенным папкам и файлам**.

Внимание! После выполнения этих действий файл с Вашей информацией будет автоматически зашифровываться. Просмотр его на другой ПЭВМ будет невозможен.

В. Для выключения режима шифрования выполните следующие действия.

1. Выделите файл **шифр.doc** в папке **Мои документы**.
2. Нажмите правую клавишу мыши и выберите пункт **Свойства**.
3. На вкладке **Общие** нажмите кнопку **Другие**.
4. В открывшемся окне диалога в группе **Атрибуты сжатия и шифрования** сбросьте флажок **Шифровать содержимое для защиты данных.**

Внимание! После выполнения этих действий файл с Вашей информацией не будет зашифровываться.

С. Создание резервной копии Сертификата средствами Windows 2000/XP/7/10.

Примечание. Резервная копия сертификата необходима для расшифровки данных после переустановки операционной системы или для просмотра зашифрованной информации на другой ПЭВМ.

Внимание! Перед переустановкой операционной системы обязательно создайте копии Сертификатов, так как после переустановки Вы не сможете расшифровать информацию.

Для создания резервной копии сертификата выполните следующие действия.

1. Выберите кнопку **Пуск** в панели задач.
2. Перейдите к пункту **Выполнить.**
3. В открывшемся окне в поле ввода введите команду **mmc.**
4. В результате откроется консоль управления **mmc.**

Примечание. Консоль ММС – это средство для создания, сохранения и открытия наборов средств администрирования,

называемых консолями. Консоли содержат такие элементы, как оснастки, расширения оснасток, элементы управления, задачи, мастера и документацию, необходимую для управления многими аппаратными, программными и сетевыми компонентами системы Windows. Можно добавлять элементы в существующую консоль MMC, а можно создавать новые консоли и настраивать их для управления конкретными компонентами системы.

5. В меню **Консоль** выберите команду **Добавить или удалить оснастку** (рис. 28) и нажмите кнопку **Добавить.**

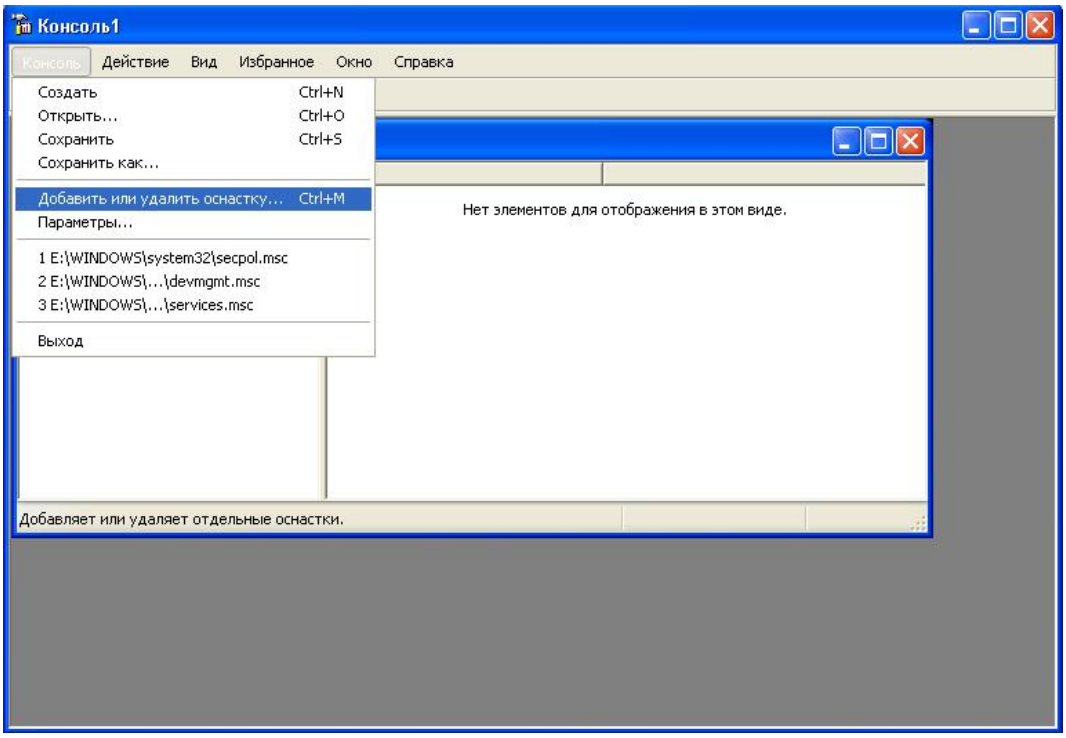

Рис. 28. Добавление оснастки

6. В поле **Оснастка** дважды щелкните **Сертификаты** (рис. 29), установите переключатель в положение **учетной записи компьютера** и нажмите кнопку **Далее.**

7. Выполните одно из следующих действий.

• Чтобы управлять сертификатами локального компьютера, установите переключатель в положение **локальным компьютером** и нажмите кнопку **Готово.**

• Чтобы управлять сертификатами удаленного компьютера, установите переключатель в положение **другим компьютером** и введите имя компьютера или нажмите кнопку **Обзор** для выбора компьютера, затем нажмите кнопку **Готово.**

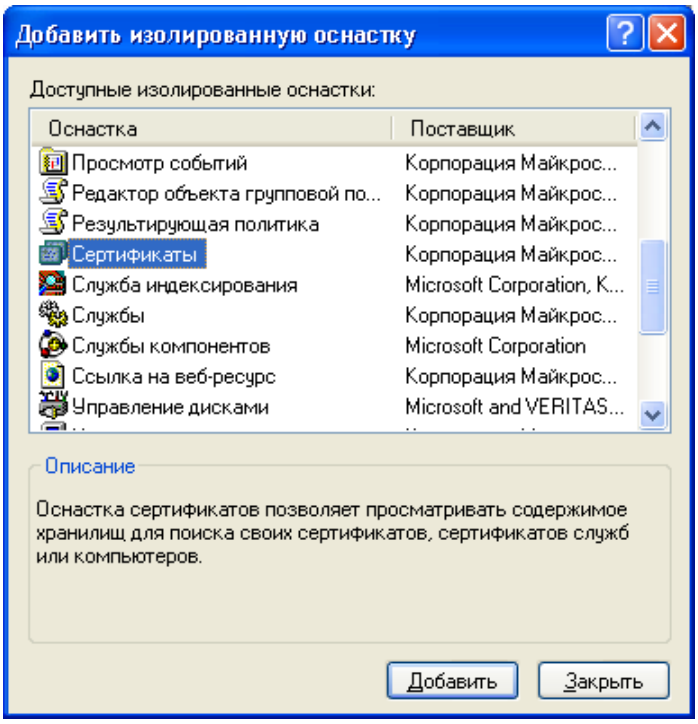

Рис. 29. Работа с сертификатами

8. Нажмите кнопку **Закрыть.**

9. В списке выбранных оснасток для новой консоли появится элемент **Сертификаты** (имя_компьютера).

10. Если на консоль не нужно добавлять другие оснастки, нажмите кнопку ОК.

11. Чтобы сохранить эту консоль, в меню Консоль выберите команду **Сохранить** и укажите имя оснастки **Сертификаты.**

12. Закройте окно **Консоли** и выберите команду **Пуск** и далее **Все программы**.

13. Найдите пункт **Администрирование** и выберите подпункт **Сертификаты** (теперь оснастка с **Сертификатами** доступна в меню **Пуск**).

14. В левом подокне оснастки Сертификаты откройте папку **Доверенные корневые сертификаты**, а затем папку **Сертификаты**. В правом подокне появится список сертификатов.

15. Укажите переносимый сертификат (например, первый в списке, рис. 30) и щелкните правой кнопкой мыши. В появившемся контекстном меню выберите команду **Все задачи** и далее выберите команду **Экспорт.**

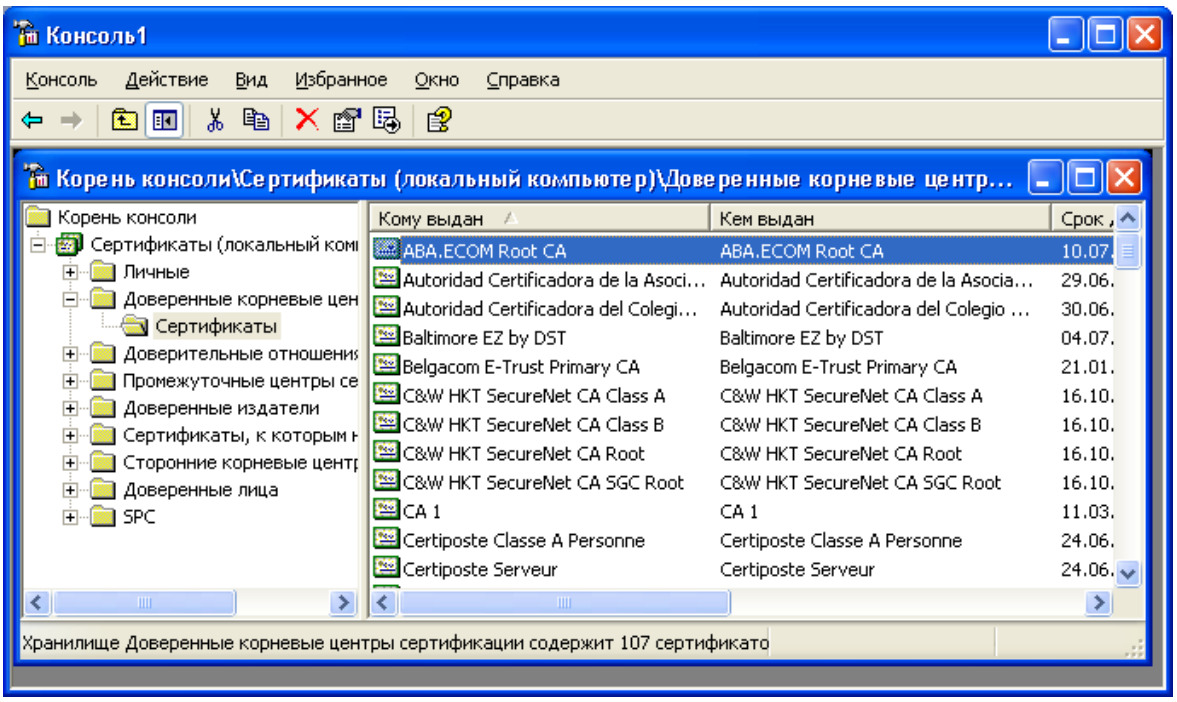

Рис. 30.Экспорт сертификата

16. В результате запустится **Мастер экспорта сертификатов**.
17. Нажмите кнопку **Далее**.
18. В следующем окне мастера выберите опцию **Да, экспортировать закрытый ключ**.
19. Затем нажмите кнопку **Далее**.
20. В следующем окне мастера доступен только один формат (PFX), предназначенный для персонального обмена информацией. Нажмите кнопку **Далее**.
21. В следующих окнах сообщите пароль (например, 11), защищающий данные файла сертификатах, а также путь сохранения файла (запишите путь к папке, в которой Вы сохранили копию Сертификата) сертификат.pfx.
22. Нажмите кнопку **Далее**.
23. Отобразится список экспортируемых сертификатов и ключей. Нажмите кнопку **Готово**.
24. Завершите работу Мастера экспорта сертификата нажатием кнопки **ОК** в окне диалога, сообщающем об успешном выполнении процедуры экспорта.

В результате сертификат и секретный ключ будут экспортированы в файл с расширением сертификат.pfx, который может быть скопирован на гибкий диск и перенесен на другой

компьютер или использован после переустановки операционной системы.

D. Для восстановления сертификата из резервной копии выполните следующие действия.

1. Перенесите созданный на предыдущем этапе файл с расширением сертификат.pfx на компьютер **(Вам необходимо вспомнить путь к копии Сертификата).**

2. Запустите оснастку **Сертификаты**, для этого выберите кнопку **Пуск** панели задач и далее **Все программы/Администрирование/Сертификаты**.

3. В окне структуры оснастки **Сертификаты** откройте папку **Доверенные корневые сертификаты**, затем папку **Сертификаты**. В правом подокне появится список Ваших сертификатов.

4. Щелкните правой кнопкой мыши на пустом месте правого подокна.

5. В появившемся контекстном меню выберите команду Все задачи.

6. В ее подменю выберите команду **Импорт** (Import).

7. Запустится Мастер импорта сертификатов.

8. Следуйте указаниям мастера – укажите местоположение файла сертификат.pfx и сообщите пароль защиты данного файла.

9. Для начала операции импорта нажмите кнопки **Готово** и **ОК**.

10. После завершения процедуры импорта нажмите кнопку **ОК** и закройте окно Мастера импорта.

В результате Ваших действий текущий пользователь или Вы сами получите возможность работать с зашифрованными данными на этом компьютере.

Задания для самостоятельной работы

1. Экспортируйте сертификат № 2 из папки **Промежуточные центры сертификации Root Agency** (сохраните иллюстрации для отчета).

2. Импортируйте экспортированный сертификат в папку **Личные** (сохраните иллюстрации для отчета).

Контрольные вопросы

1. Что входит в криптосистему?

2. Сравните методы шифрования с открытым и закрытым ключом (асимметричное и симметричное шифрование).
3. Что такое mmc?
4. Назначение шифрующей файловой системы EFS.

ПРАКТИЧЕСКАЯ РАБОТА 6
Назначение прав пользователей при произвольном управлении доступом в Windows 2000/XP/7/10

Краткие теоретические сведения

После выполнения идентификации и аутентификации подсистема защиты устанавливает полномочия (совокупность прав) субъекта для последующего контроля санкционированного использования объектов информационной системы.

Обычно полномочия субъекта представляются **списком ресурсов**, доступным пользователю и **правами по доступу** к каждому ресурсу из списка.

При разграничении доступа по спискам задаются соответствия: каждому пользователю – список ресурсов и прав доступа к ним или каждому ресурсу – список пользователей и их прав доступа к данному ресурсу.

Списки позволяют установить права с точностью до пользователя. Списки используются в подсистемах безопасности операционных систем и систем управления базами данных.

Задание: создать учетную запись и локальную группу, изменить принадлежность пользователя к локальной группе и блокировать учетную запись пользователя.

Алгоритм выполнения работы

А. Создание учетной записи.

1. Откройте оснастку **Управление компьютером** в разделе **Администрирование Панели управления** (рис. 31).

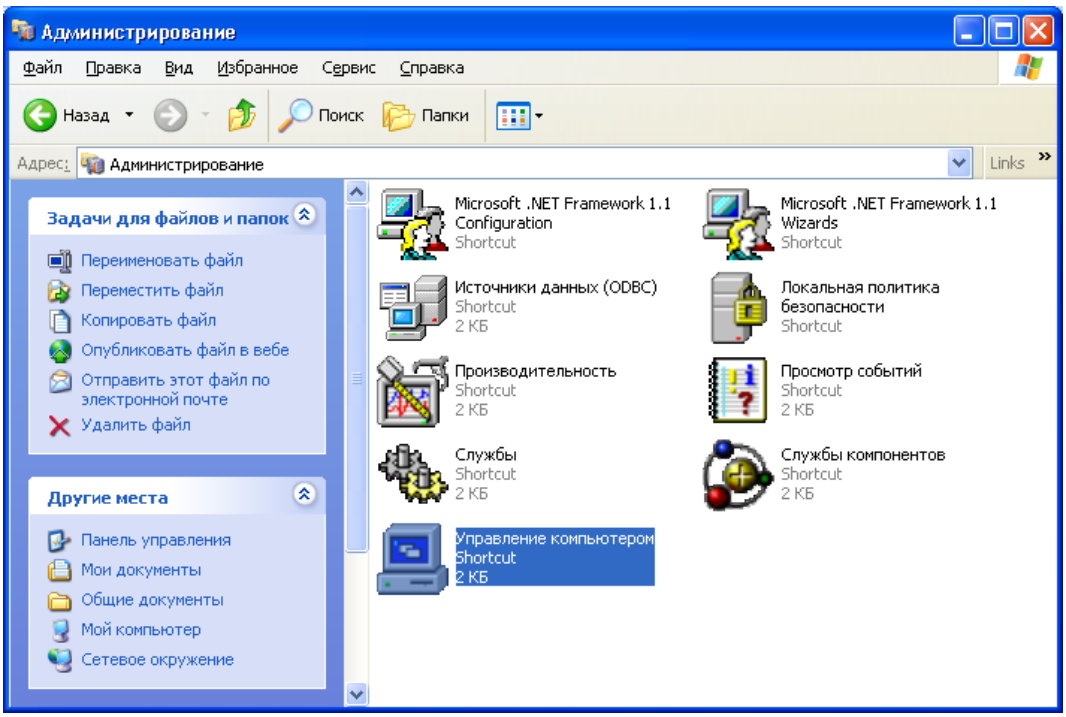

Рис. 31. Управление компьютером

2. В оснастке **Локальные пользователи и группы** установите указатель мыши на папку **Пользователи** и нажмите правую кнопку.

3. В появившемся контекстном меню выберите команду **Новый пользователь** (рис. 32). Появится окно диалога **Новый пользователь** (рис. 33).

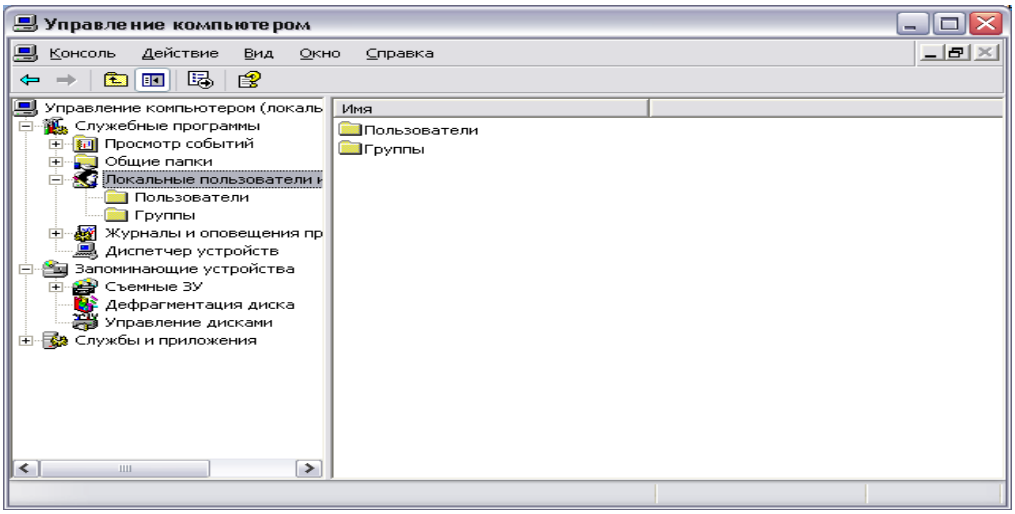

Рис. 32. Работа с пользователями

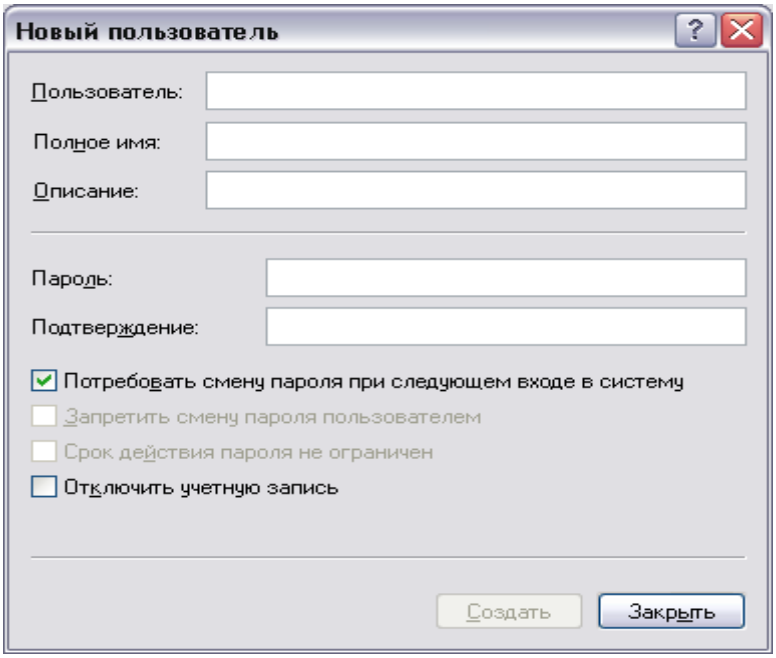

Рис.33. Добавление пользователя

4. В поле **Пользователь** введите имя создаваемого пользователя, например, свою фамилию.

Примечание. Имя пользователя должно быть уникальным для компьютера. Оно может содержать до 20 символов верхнего и нижнего регистра. Ниже приведены символы, применение которых в имени пользователя недопустимо: » / \ [] : ; = , +*?<> Имя пользователя не может состоять целиком из точек и пробелов.

5. В поле **Полное** имя введите полное имя создаваемого пользователя.

6. В поле **Описание** введите описание создаваемого пользователя или его учетной записи, например, «студент…… ».

7. В поле **Пароль** введите пароль пользователя и в поле **Подтверждение** подтвердите его правильность вторичным вводом.

Примечание: длина пароля не может превышать 14 символов.

8. Установите или снимите флажки:

- потребовать смену пароля при следующем входе в систему;
- запретить смену пароля пользователем;
- срок действия пароля не ограничен;
- отключить учетную запись.

9. Чтобы создать еще одного пользователя, нажмите кнопку **Создать** и повторите шаги с 1 по 8. Для завершения работы нажмите кнопку **Создать** и затем **Закрыть.**

B. Создание локальной группы.

1. В окне оснастки **Локальные пользователи и группы** установите указатель мыши на папке **Группы** и нажмите правую кнопку.

2. В появившемся контекстном меню выберите команду **Новая группа**.

3. В поле **Имя группы** (рис. 34) введите имя новой группы, например, **Студенты**.

Примечание: имя локальной группы должно быть уникальным в пределах компьютера. Оно может содержать до 256 символов в верхнем и нижнем регистрах.

4. В поле **Описание** введите описание новой группы.

5. В поле **Члены группы** можно сразу же добавить пользователей и группы, которые войдут в данную группу: для этого нужно нажать кнопку **Добавить** и выбрать их в списке.

Для завершения нажмите кнопку **Создать** и затем **Закрыть**.

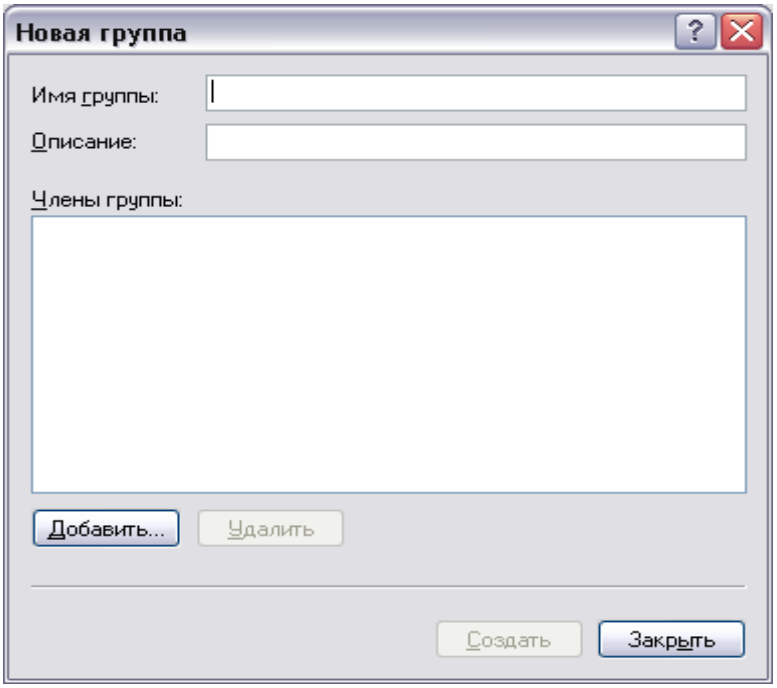

Рис.34. Создание группы

C. Изменение членства в локальной группе.

1. В окне оснастки **Локальные пользователи и группы** щелкните на папке **Группы**.

2. В правом подокне установите указатель мыши на модифицируемую группу и нажмите правую кнопку.

3. В появившемся контекстном меню выберите команду **Добавить в группу** или **Свойства**.

4. Для того, чтобы добавить новые учетные записи в группу, нажмите кнопку **Добавить** (рис. 35).

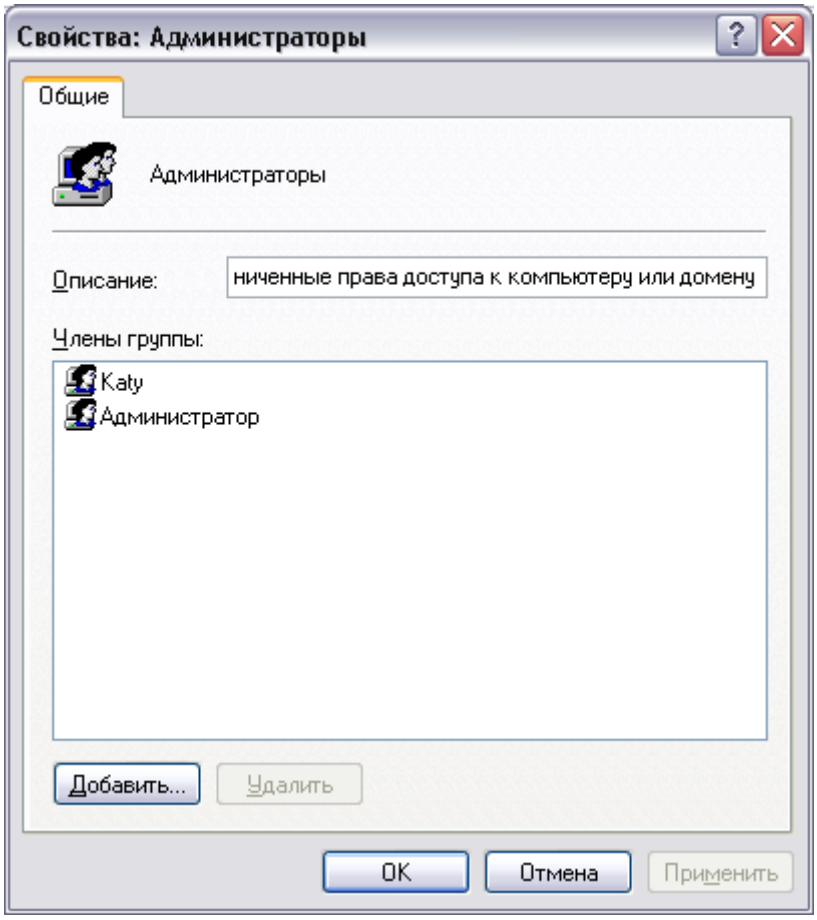

Рис.35.Заполнение группы

5. Далее следуйте указаниям окна диалога Выбор: **Пользователи или Группы.**

6. Для того, чтобы удалить из группы некоторых пользователей, в поле **Члены группы** (рис. 35) окна свойств группы выберите одну или несколько учетных записей и нажмите кнопку **Удалить**.

Примечание. В локальную группу можно добавлять как локальных пользователей, созданных на компьютере, так и пользователей и глобальные группы, созданные в домене, к которому принадлежит компьютер, или в доверяемых доменах. Встроенные группы не могут быть удалены. Удаленные группы не

могут быть восстановлены. Удаление группы не отражается на входящих в нее пользователей.

D. Временная блокировка учетной записи.

1. Откройте оснастку **Управление компьютером**.

2. Для этого либо выберите на Рабочем столе ярлык Мой компьютер и нажмите правую клавишу мыши, после чего выберите пункт контекстного меню **Управление**, либо воспользуйтесь разделом **Администрирование** в Панели управления.

3. В открывшейся оснастке выберите пункты **Служебные программы/Локальные пользователи и группы** (рис. 32).

4. Откройте папку **Пользователи** и выберите учетную запись **Гость**.

5. Нажмите правую клавишу мыши и выберите пункт **Свойства**.

6. В открывшемся окне снимите отметку пункта **Отключить учетную запись** (рис. 36).

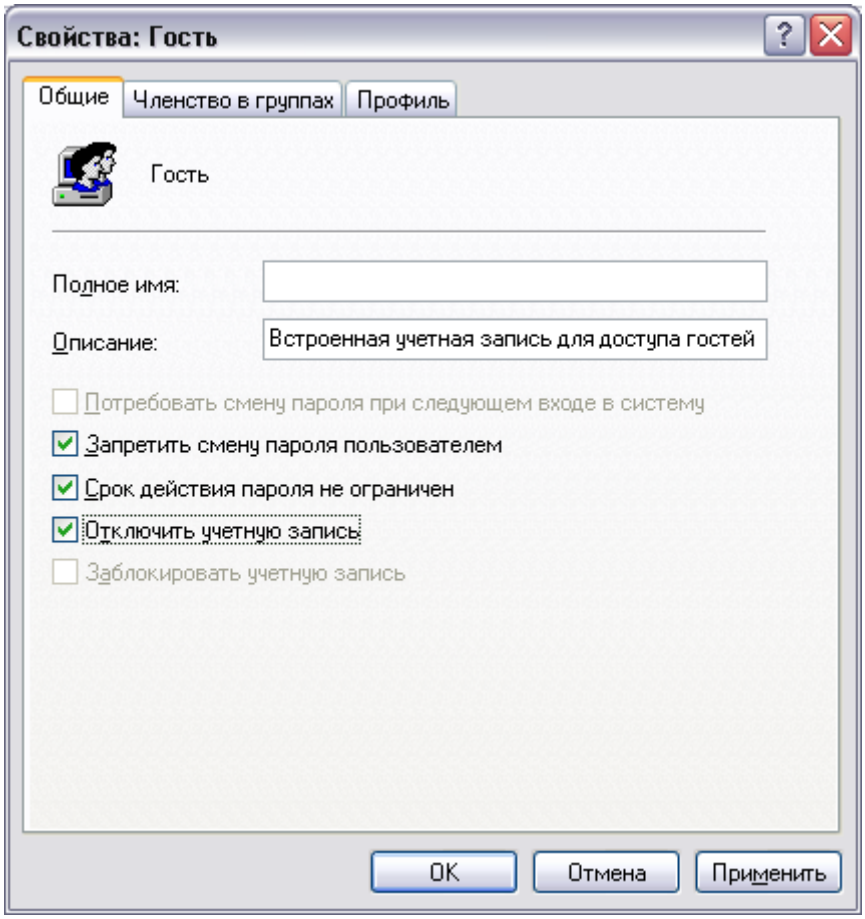

Рис. 36. Блокировка учетной записи

7. Нажмите кнопку **ОК** и сделайте вывод о состоянии учетной записи.

8. Выполните пункт 5 и отметьте пункт **Отключить учетную запись.**

Задания для самостоятельной работы

1. Создайте учетную запись с именем ПЗ-6, используя команду Print Screen клавиатуры, сохраните копию экрана со списком пользователей Вашего компьютера (для этого после нажатия клавиши Print Screen вставьте скопированное изображение в новый документ Word) для представления в качестве отчета.
2. Создайте группу **Информационная безопасность** и, как в первом задании, сохраните окно со списком групп Вашего компьютера для отчета.
3. Заблокируйте учетную запись ПЗ-8/44 и после этого удалите.

Контрольные вопросы

1. Какие методы управления доступом Вам известны?
2. Чем отличается мандатное управление доступом от дискретного?
3. Допустимо ли имя пользователя П38/44? Почему?

ПРАКТИЧЕСКАЯ РАБОТА 7

Настройка параметров регистрации и аудита в Windows 2000/XP/7/10

Краткие теоретические сведения

Регистрация является еще одним механизмом обеспечения защищенности информационной системы. Этот механизм основан на подотчетности системы обеспечения безопасности, фиксирует все события, касающиеся безопасности. Эффективность системы безопасности принципиально повышается в случае дополнения механизма регистрации механизмом аудита. Это позволяет оперативно выявлять нарушения, определять слабые места в системе защиты, анализировать закономерности системы, оценивать работу пользователей и т. д.

Аудит – это анализ накопленной информации, проводимый оперативно, в реальном времени или периодически (например, раз в день). Оперативный аудит с автоматическим реагированием на выявленные нештатные ситуации называется активным.

Практическими средствами регистрации и аудита являются:

- различные системные утилиты и прикладные программы;
- регистрационный (системный или контрольный) журнал.

Первое средство является обычно дополнением к мониторингу, осуществляемому администратором системы. Комплексный подход к протоколированию и аудиту обеспечивается при использовании регистрационного журнала.

Регистрационный журнал – это хронологически упорядоченная совокупность записей результатов деятельности субъектов системы, достаточная для восстановления, просмотра и анализа последовательности действий, окружающих или приводящих к выполнению операций, процедур или совершению событий при транзакции с целью контроля конечного результата.

Задание: активизировать механизмы регистрации и аудита операционной системы Windows 2000 (XP) и настроить параметры просмотра аудита папок и файлов.

Алгоритм выполнения работы

А. Активизация механизма регистрации и аудита с помощью оснастки Локальные политики безопасности.

1. Выберите кнопку **Пуск** панели задач.
2. Откройте меню **Настроить/Панель управления.**
3. В открывшемся окне выберите ярлык **Администрирование/Локальная политика безопасности.**
4. Выберите пункт **Политика аудита** (рис. 37).
5. Для включения или отключения параметров аудита выберите требуемый параметр и дважды щелкните левой клавишей мыши.
6. Для каждого параметра можно задать аудит успехов или; отказов, либо вообще отключить аудит событий данного типа (рис. 38).
7. Значения параметров политики аудита приведены в табл. 8.
8. По умолчанию все параметры политики аудита выключены.
9. Включите аудит успеха и отказа для всех параметров.
10. Для этого выполните пункт 5.
11. Нажмите кнопку **ОК**.

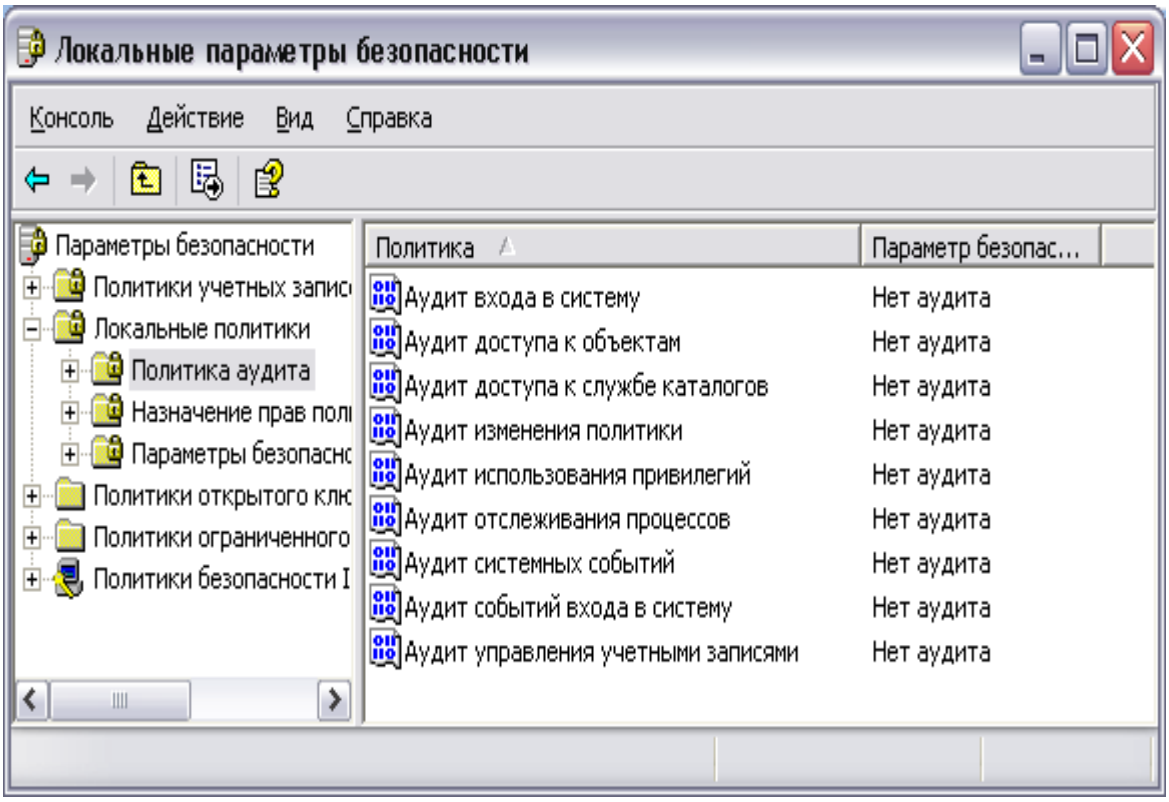

Рис.37. Политика аудита

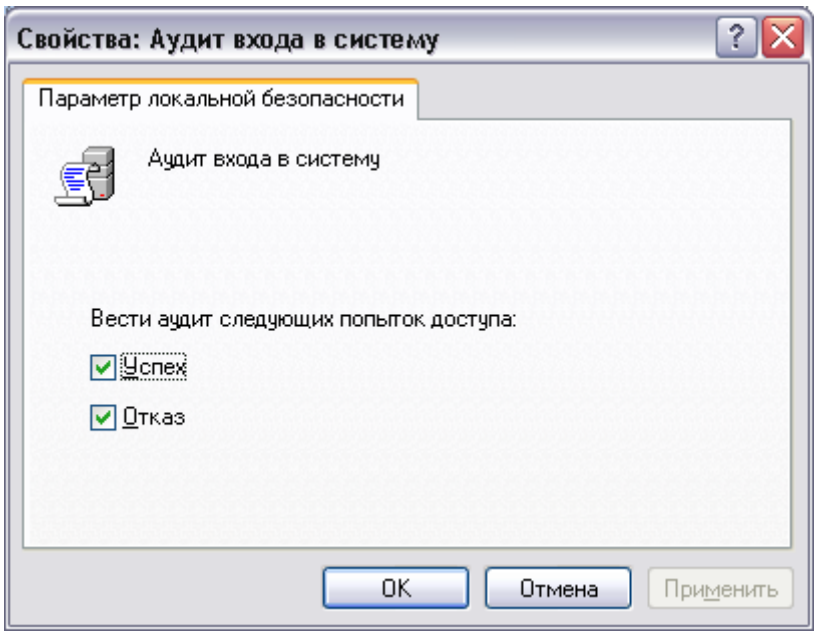

Рис.38. Настройка аудита

Таблица 8

Значение параметров аудита системы

Параметр	Значение
Аудит событий входа в систему	Определяет, подлежит ли аудиту каждая попытка входа в систему пользователя войти в систему или выйти из нее на другом компьютере при условии, что данный компьютер используется для проверки подлинности учетной записи. Если этот параметр политики определен, можно задать аудит успехов или отказов, либо вообще отключить аудит событий данного типа. Аудит успехов означает создание записи аудита для каждой успешной попытки входа в систему. Аудит отказов означает создание записи аудита для каждой неудачной попытки входа в систему

Аудит управления учетными записями	Определяет, подлежат ли аудиту все события, связанные с управлением учетными записями на компьютере. К таким событиям относятся следующие события: ❖ создание, изменение или удаление учетной записи пользователя или группы; ❖ переименование, отключение или включение учетной записи пользователя; ❖ задание или изменение пароля
Аудит доступа к службе каталогов	Определяет, подлежит ли аудиту событие доступа пользователя к объекту каталога Active Directory, для которого задана собственная системная таблица управления доступом
Аудит входа в систему	Определяет, подлежит ли аудиту каждая попытка пользователя войти в систему или выйти из нее на данном компьютере, или подключиться к нему через сеть
Аудит доступа к объектам	Определяет, подлежит ли аудиту событие доступа пользователя к объекту - например, к файлу, папке, разделу реестра, принтеру и т. п. - для которого задана собственная системная таблица управления доступом
Аудит изменения политики	Определяет, подлежит ли аудиту каждый факт изменения политик назначения прав пользователей, политик аудита или политик доверительных отношений.
Аудит использования привилегий	Определяет, подлежит ли аудиту каждая попытка пользователя воспользоваться предоставленным ему правом

Аудит отслеживания процессов	Определяет, подлежат ли аудиту такие события, как активизация программы, завершение процесса, повторение дескрипторов и косвенный доступ к объекту
Аудит системных событий	Определяет, подлежат ли аудиту события перезагрузки или отключения компьютера, а также события, влияющие на системную безопасность или на журнал безопасности

В. Настройка и просмотр аудита папок и файлов (доступно только на томах NTFS).

1. Установите указатель мыши на файл или папку, для которой следует выполнить аудит, и нажмите правую кнопку.
2. В появившемся контекстном меню выберите команду **Свойства**.
3. В окне свойств папки или файла перейдите на вкладку **Безопасность**.
4. На вкладке Безопасность нажмите кнопку **Дополнительно** и затем перейдите на вкладку **Аудит**.
5. Если Вы хотите настроить аудит для нового пользователя или группы на вкладке **Аудит** нажмите кнопку **Добавить**.
6. Появится диалоговое окно **Выбор**: **Пользователь, Компьютер или Группа**.
7. Выберите имя нужного пользователя или группы и нажмите кнопку ОК. Откроется окно диалога **Элемент аудита для**. Здесь Вы сможете ввести все необходимые параметры аудита.
8. В списке **Применять** укажите, где следует выполнять аудит (это поле ввода доступно только для папок).
9. В группе **Доступ** следует указать, какие события следует отслеживать: окончившиеся успешно (Успех), неудачно (Отказ) или оба типа событий.
10. **Применять этот аудит к объектам и контейнерам только внутри этого контейнера** – определяет, распространяются ли введенные Вами настройки аудита на файлы и папки, находящиеся ниже по дереву каталогов файловой системы (флажок не установлен). В обратном случае установите флажок (или

выберите в списке) **Применять опцию Только для этой папки.** Это позволит не выполнять аудит для тех объектов файловой системы, которые не представляют интереса.

11. После завершения настройки аудита для папки или файла нажмите несколько раз кнопку ОК, чтобы закрыть все окна диалога.

12. Если Вы хотите просмотреть или изменить настройки аудита для уже существующего пользователя или группы, нажмите кнопку **Показать/Изменить**. Появится окно диалога **Элемент аудита для.** Здесь Вы сможете выполнить все необходимые изменения параметров аудита для выбранного Вами пользователя или группы. По окончании внесения изменений нажмите кнопку ОК.

Примечание. После включения аудита операционная система Windows 2000/XP/7/10 начинает отслеживать события, связанные с безопасностью. Полученную в результате информацию можно просмотреть с помощью оснастки **Просмотр событий**. При просмотре журнала событий можно выяснить, кто предпринял попытку выполнения неразрешенного ему действия. Для того чтобы иметь возможность настраивать аудит для файлов и папок, необходимо иметь права администратора.

С. Просмотр событий в журнале событий.

1. Выберите кнопку **Пуск** панели задач.

2. Откройте меню **Настроить/Панель управления.**

3. В открывшемся окне выберите ярлык **Администрирование** и далее **Просмотр событий.**

4. В открывшемся окне выберите пункт **Безопасность**(рис. 39).

5. В правой половине открытого окна появится список всех зарегистрированных событий.

6. Для просмотра требуемого события вызовите его свойства из контекстного меню или дважды щелкните по его названию левой клавишей мыши.

7. В результате появится окно, как показано на рис. 40.

8. В показанном примере зафиксирован успех отключения учетной записи Гость пользователем Админ 8.05.04 в 18.28.31.

9.В примере, показанном на рис. 41, зафиксирован отказ входа в систему пользователю NT AUTHORITY\SYSTEM (системная учетная запись) 08.05.04 в 17:39:58 по причине «неизвестное имя пользователя или неверный пароль».

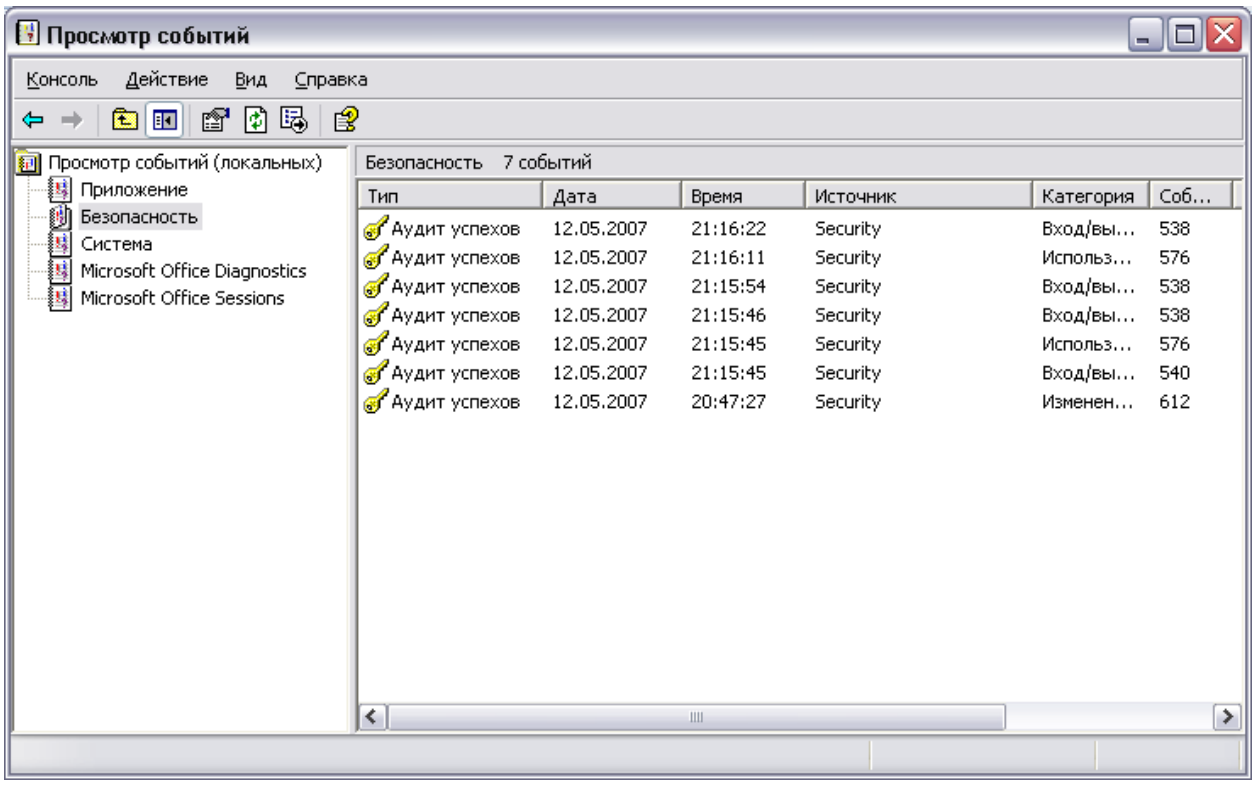

Рис.39. События безопасности

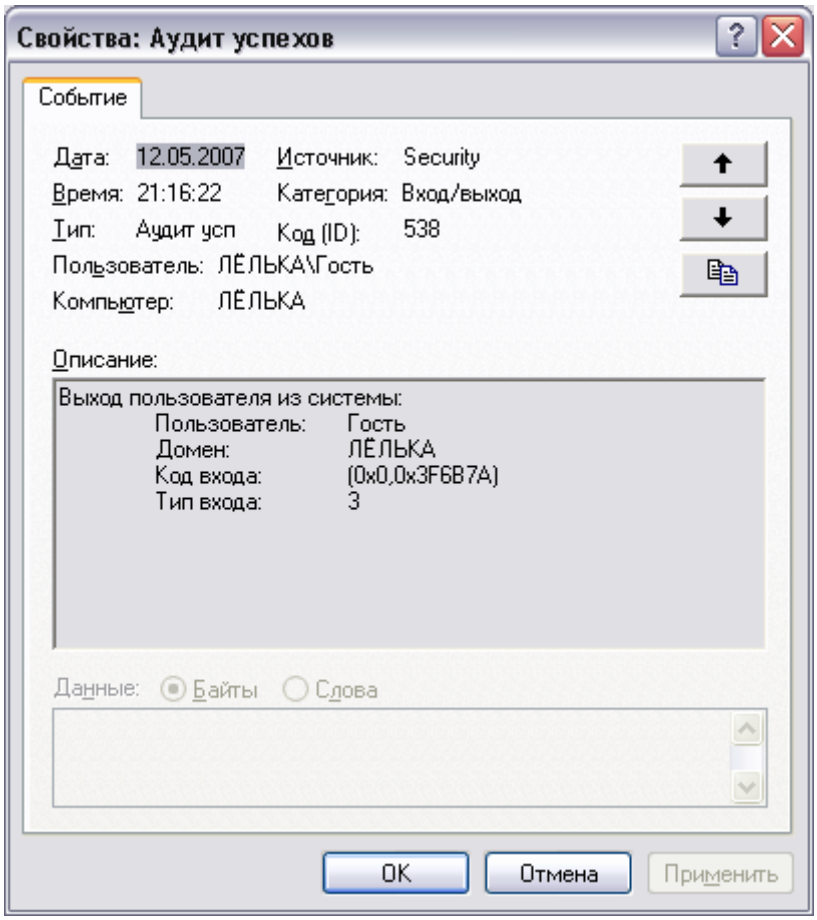

Рис.40. Успешное событие

10.Таким образом, просмотр журнала событий позволяет в полной мере проанализировать действия пользователей и процессов.

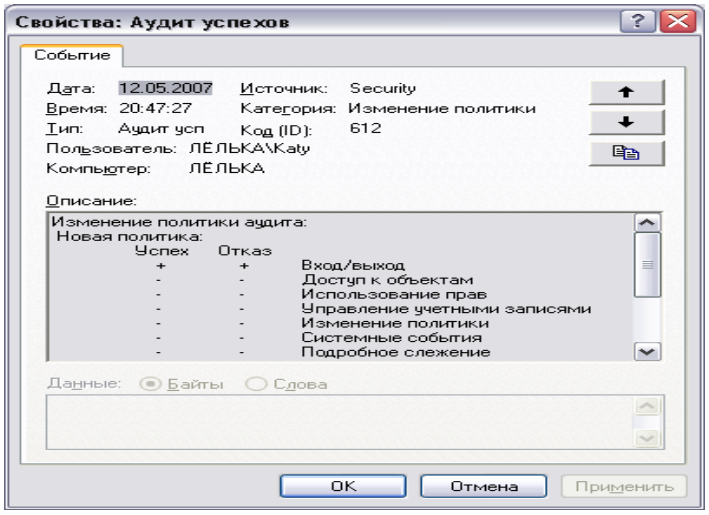

Рис.41. Событие - отказ

Задания для самостоятельной работы

1. Включите аудит успеха и отказа всех параметров (используйте задание А).
2. Выйдите из системы и предпримите попытку входа в операционную систему с неверным паролем. Откройте журнал событий, найдите соответствующую запись и скопируйте экран в буфер (Print Screen) для отчета.
3. Удалите созданную ранее учетную запись ПЗ-6 и зафиксируйте все события системного журнала, связанные с этим действием для отчета.

Контрольные вопросы

1. Чем отличаются регистрация и аудит?
2. Что является средствами регистрации и аудита?
3. Какие события фиксируются в системном журнале?
4. Что фиксирует система при регистрации событий?

ПРАКТИЧЕСКАЯ РАБОТА 8

Управление шаблонами безопасности в Windows 2000/XP/7/10

Краткие теоретические сведения

Управление шаблонами безопасности в Windows 2000/XP/7/10 осуществляется с помощью **Редактора шаблонов безопасности**, реализованного в виде оснастки **MMC**.

Он предназначен для создания и редактирования текстовых файлов конфигурации безопасности операционной системы Windows 2000/XP/7/10. Такие файлы значительно легче переносятся с одной системы на другую, чем соответствующие им базы данных безопасности.

Созданные при помощи оснастки **Шаблоны безопасности** текстовые файлы хранятся на жестком диске и при необходимости могут быть импортированы в базу данных безопасности. В этом случае все хранимые настройки безопасности начнут действовать.

Значения параметров обеспечения безопасности заносятся в текстовые файлы с расширением inf, называемые **Шаблонами безопасности**

Примечание. Новые **Шаблоны безопасности** не изменяют все старые настройки параметров системы безопасности, они лишь дополняют их, увеличивая (инкрементируя) степень защищенности компьютера.

Задание: загрузить редактор Шаблона безопасности, редактировать шаблон безопасности и сохранить его с новым именем.

Алгоритм выполнения работы

А. Загрузка оснастки Шаблоны безопасности.

1. Выберите кнопку **Пуск** в панели задач.
2. Перейдите к пункту **Выполнить.**
3. В открывшемся окне в поле ввода введите команду **mmc.**
4. В результате откроется консоль управления **mmc.**
5. В меню Консоль выберите команду **Добавить или удалить оснастку** (рис. 42) и нажмите кнопку **Добавить.**
6. В поле **Оснастка** дважды щелкните **Шаблоны безопасности.**

7. Нажмите кнопку **Закрыть**.

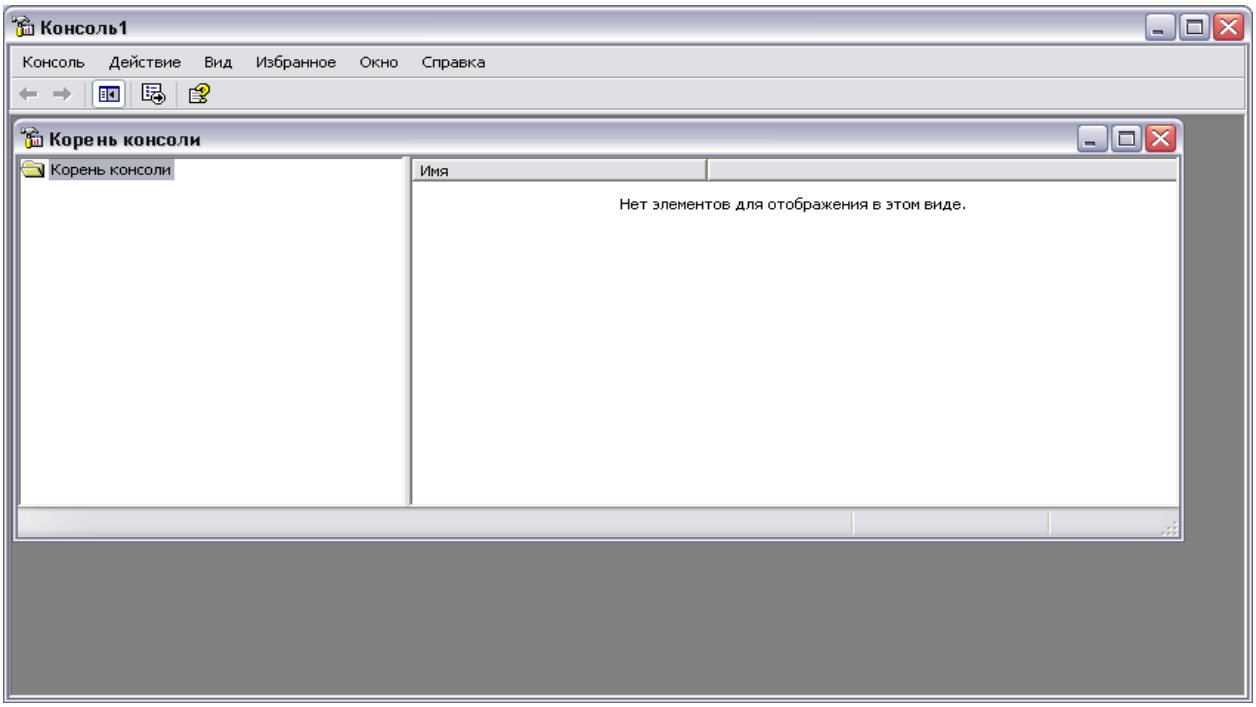

Рис.42. Добавление оснастки

8. В списке выбранных оснасток для новой консоли появится элемент **Шаблоны безопасности**.

9. Если на консоль не нужно добавлять другие оснастки, нажмите кнопку **ОК**.

10. Чтобы сохранить эту консоль, в меню **Консоль** выберите команду **Сохранить** и укажите имя оснастки **Шаблоны безопасности**.

11. Закройте окно **Консоли** и выберите команду **Пуск** и далее **Все программы**.

12. Найдите пункт **Администрирование** и выберите подпункт **Шаблоны безопасности** (Теперь оснастка с **Шаблоны безопасности** доступна в меню **Пуск**).

13. Для просмотра значений имеющихся шаблонов в окне оснастки откройте, например, узел **Шаблоны безопасности**, щелчком выберите шаблон безопасности compatws (рис. 43) и просмотрите его папки **Политика учетных записей**, **Локальная политика** и др.

14. Помимо раскрытого шаблона безопасности compatws.inf существуют и другие стандартные шаблоны, конфигурации которых

позволяют получить различные по надежности системы безопасности.

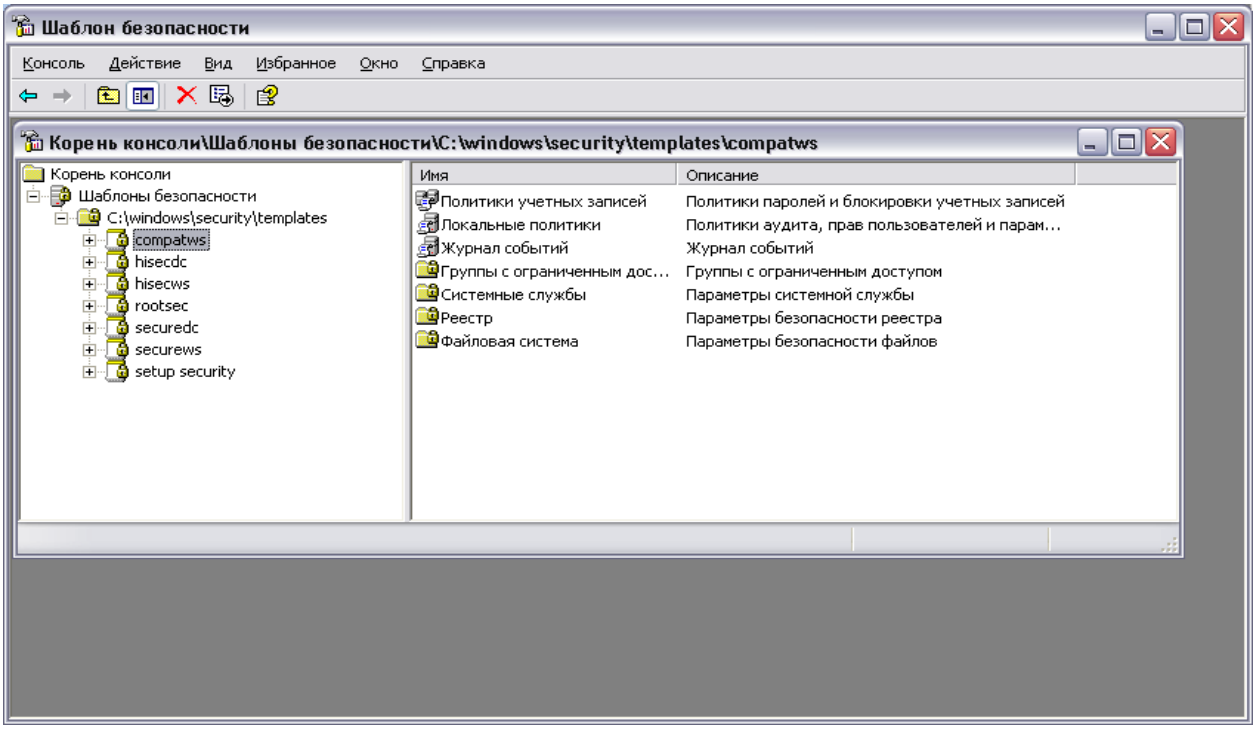

Рис. 43. Шаблон безопасности

Б. Редактирование и сохранение шаблона безопасности.

1. Щелкните на одном из стандартных шаблонов безопасности (например, compatws), которые Вы видите в окне оснастки **Шаблоны безопасности**.

2. Если Вы хотите модифицировать какую-либо настройку безопасности, дважды щелкните на ней и отредактируйте значения параметров (рис. 44, 45).

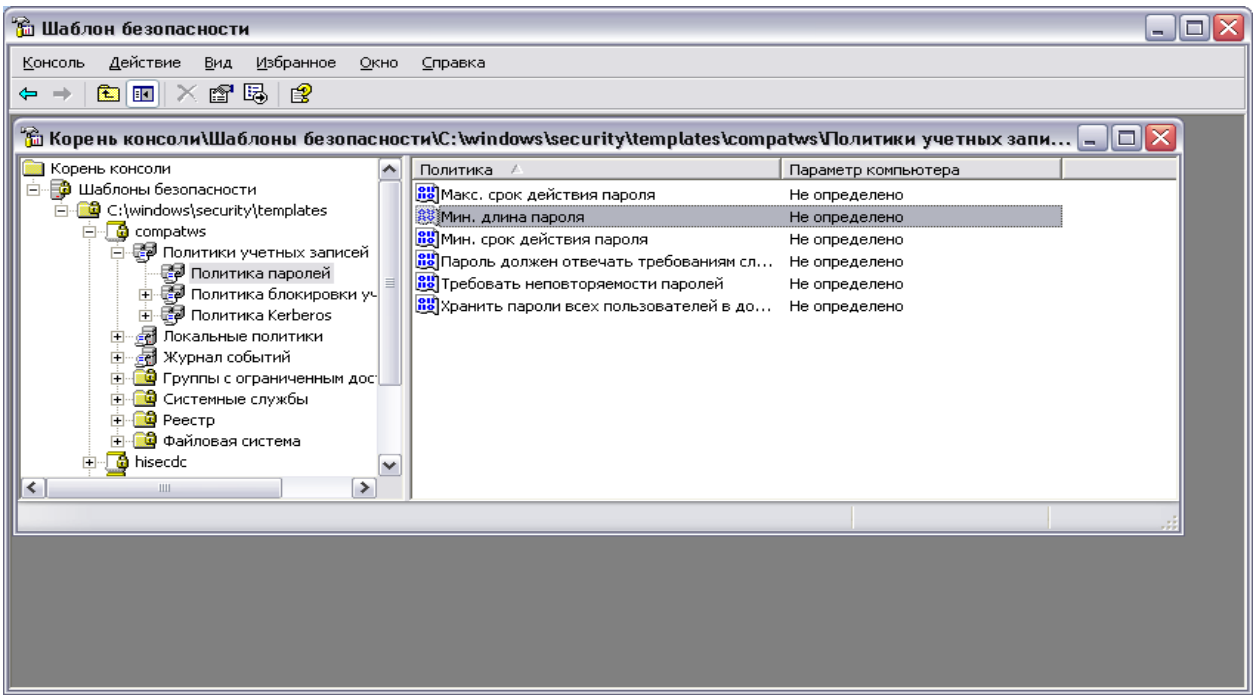

Рис. 44. Модификация шаблона

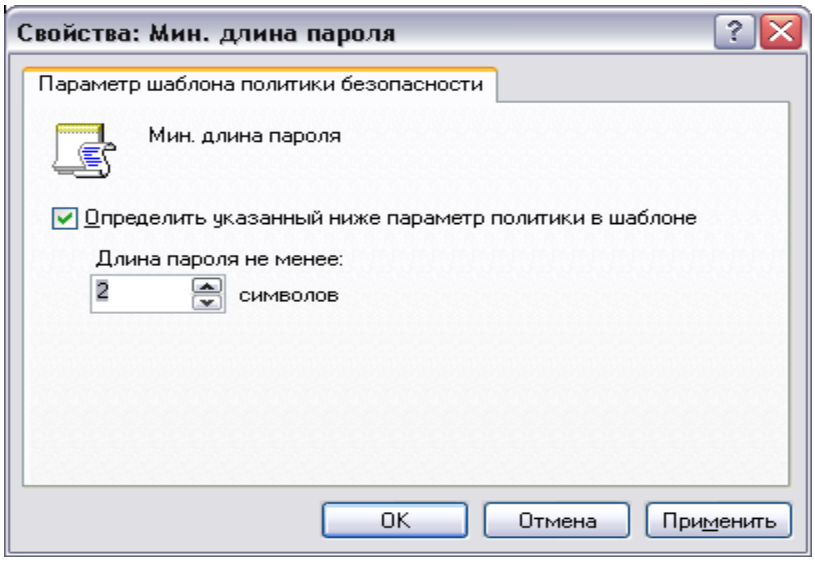

Рис.45. Изменение параметра

3. Для сохранения откорректированного стандартного шаблона безопасности под другим именем выполните следующие действия.

4. Укажите откорректированный стандартный шаблон (например, compatws), и нажмите правую кнопку мыши.

5. В появившемся контекстном меню выберите команду **Сохранить как**.

6. Введите с клавиатуры новое имя файла (например, custom). По умолчанию шаблоны безопасности располагаются в каталоге %**SystemRoot**%**Secunfy** **Templates**.

7. Пользовательский шаблон будет добавлен в определенную заранее конфигурацию безопасности и сохранен под введенным Вами именем.

Настроив Шаблон безопасности для одной ПЭВМ, Вы можете перенести его и на другие ПЭВМ Вашей рабочей группы. Шаблоны безопасности являются гибким и удобным инструментом по настройке системы безопасности операционной системы.

Задания для самостоятельной работы

Создайте на базе существующего Шаблона безопасности новый шаблон и дайте ему имя ПЗ-8. После этого зафиксируйте список шаблонов, скопировав изображение экрана в буфер и далее в файл для отчета.

Контрольные вопросы

1. Для чего используются Шаблоны безопасности?
2. В каком месте на диске хранятся (по умолчанию) шаблоны безопасности?
3. Какие разделы включает стандартный Шаблон безопасности?

ПРАКТИЧЕСКАЯ РАБОТА 9

Настройка и использование межсетевого экрана в Windows XP/7/10

Краткие теоретические сведения

Межсетевое экранирование повышает безопасность объектов внутренней сети за счет игнорирования неавторизованных запросов из внешней среды, тем самым обеспечивая все составляющие информационной безопасности. Кроме функций разграничения доступа, экранирование обеспечивает регистрацию информационных обменов.

Функции экранирования выполняет **межсетевой экран** или брандмауэр (firewall), под которым понимают программную или программно-аппаратную систему, которая выполняет контроль информационных потоков, поступающих в информационную систему и/или выходящих из нее, и обеспечивает защиту информационной системы посредством фильтрации информации. Фильтрация информации состоит в анализе информации по совокупности критериев и принятии решения о ее приеме и/или передаче.

Брандмауэр в Windows XP/7/10 – это система защиты подключения к Интернету (Internet Connection Firewall, ICF), представляет собой программу настройки ограничений, регулирующих обмен данными между Интернетом и небольшой сетью или локальным компьютером. Брандмауэр ICF необходимо установить для любого компьютера, имеющего прямое подключение к Интернету.

При включении брандмауэра для локального компьютера, подключенного к Интернету с помощью модема удаленного доступа, брандмауэр ICF обеспечивает защиту этого подключения.

Задание: активизировать встроенный брандмауэр операционной системы Windows XP/7/10 и настроить его параметры.

Алгоритм выполнения работы

А. Активизация встроенного межсетевого экрана.

1. Откройте компонент **Сетевые подключения**.

2. Для этого выберите последовательно **Пуск – Панель управления – Сетевые подключения** (рис. 46).

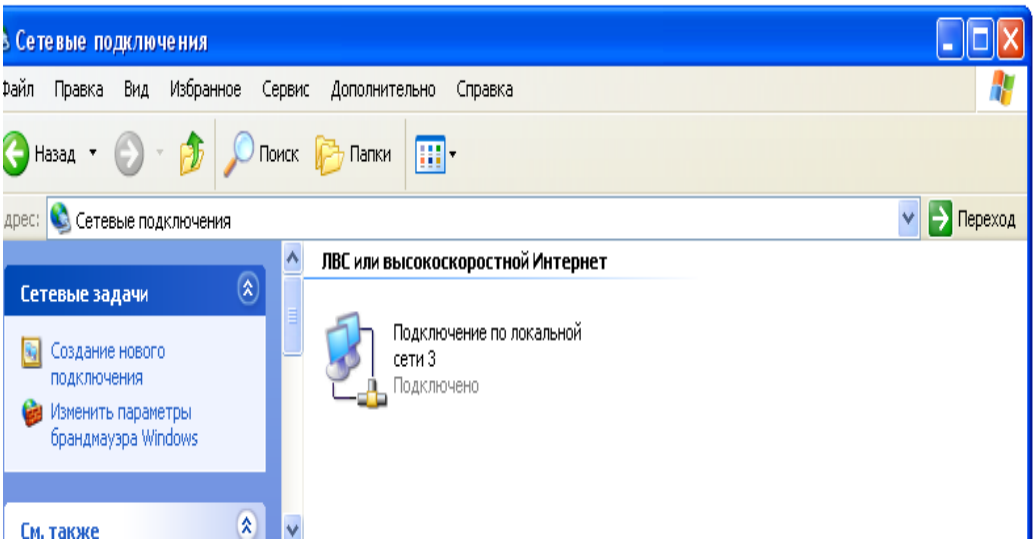

Рис. 46. Сетевое подключение

3. Выделите подключение удаленного доступа, подключение по локальной сети или высокоскоростное подключение к Интернету, которое требуется защитить брандмауэром, и затем выберите в контекстном меню (при выделенном подключении нажать правую клавишу мыши) команду **Свойства** (рис. 47).

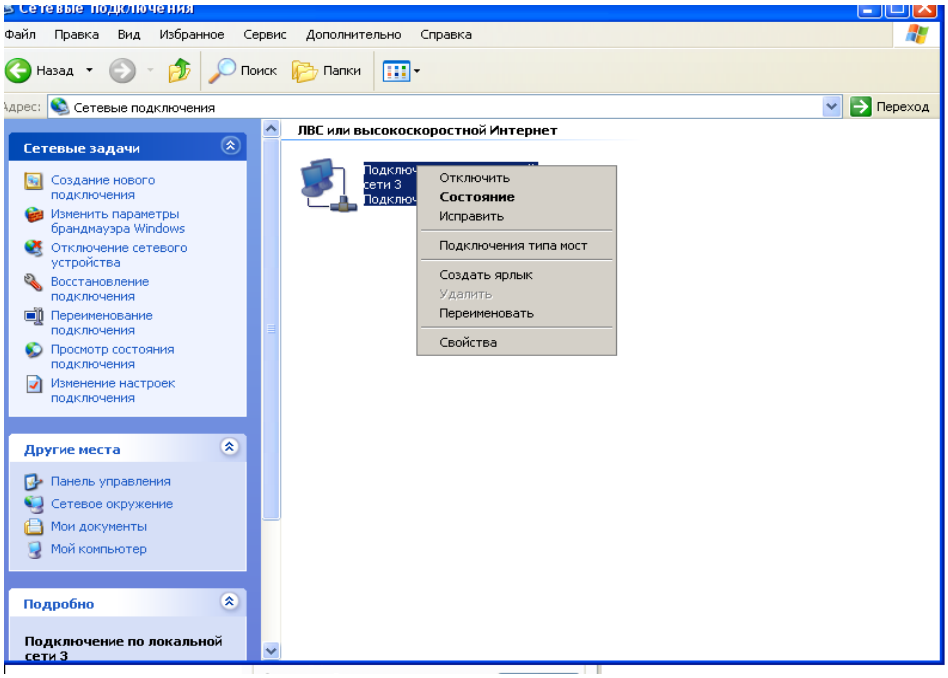

Рис. 47. Свойства подключения

4. На вкладке **Дополнительно** в группе **Брандмауэр подключения к Интернету** (рис. 48) отметьте пункт **Защитить мое подключение к Интернету.**

Примечание. Для отключения брандмауэра достаточно снять флажок **Защитить мое подключение к Интернету.**

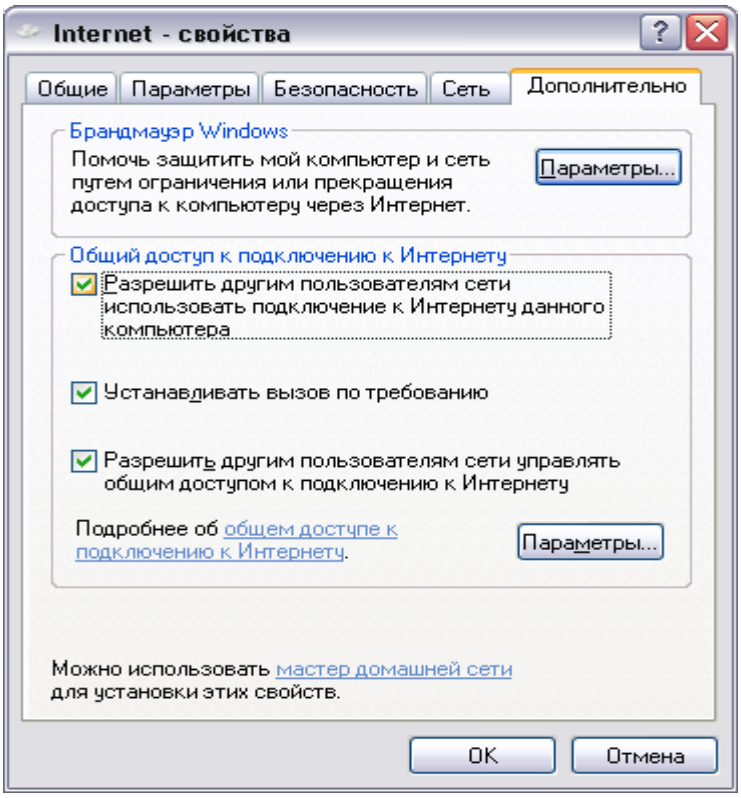

Рис.48. Брандмауэр

В. Настройка параметров брандмауэра.

1.Выполните пункты 1-3 предыдущего задания.

2.Выберите кнопку **Параметры** в нижней части открытого окна (рис. 48);

3.В результате откроется окно **Дополнительные параметры** (рис. 49) с тремя закладками (Службы, Ведение журнала безопасности и ICMP).

4.Выберите закладку **Службы.**

Примечание. На закладке Службы вы можете в явном виде указать службы Интернета, прохождение трафика которых вы допускаете. Например, чтобы обеспечить прохождение веб-страниц из Интернета на компьютер, необходимо включить службу «Веб-сервер HTTP».

5.Отметьте все службы.

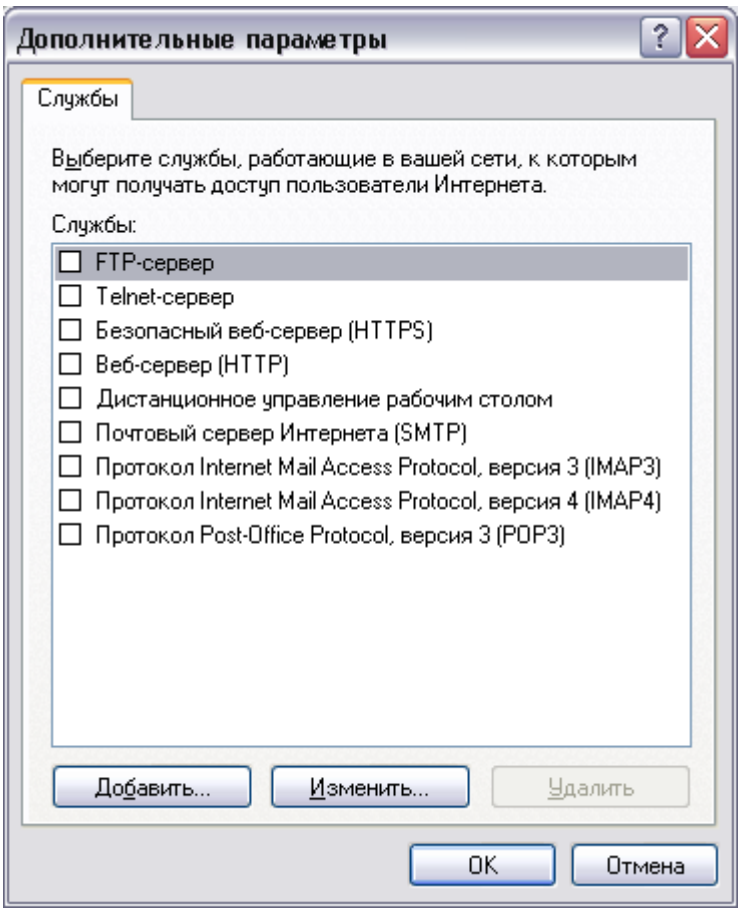

Рис.49. Параметры брандмауэра

6. Выберите закладку **Ведение журнала безопасности** (рис. 50).

Примечание. Для брандмауэра подключения к Интернету предусмотрен журнал безопасности для записи событий, связанных с его работой. Журнал безопасности ICF поддерживает следующие возможности.

Запись пропущенных пакетов. Этот параметр задает запись в журнал сведений обо всех потерянных пакетах, исходящих из сети (компьютера) или из Интернета. Если установить флажок Записывать потерянные пакеты, будут собираться сведения о каждом пакете, который пытался пройти через ICF, но был обнаружен и отвергнут брандмауэром.

Запись успешных подключений. Этот параметр задает запись в журнал сведений обо всех успешных подключениях, инициированных из сети (компьютера) или из Интернета.

7. Отметь пункты **Записывать пропущенные пакеты** и **Записывать успешные подключения** (рис.50). Обратите внимание на расположение журнала безопасности.

Примечание. Журнал безопасности брандмауэра состоит из двух разделов. В заголовке содержатся сведения о версии журнала и полях, в которые можно записывать данные. Содержимое заголовка имеет вид статического списка. Содержимое журнала безопасности представляет собой откомпилированные данные, которые вводятся при обнаружении трафика, пытающегося пройти через брандмауэр. Поля журнала заполняются слева направо, как они расположены на странице. Для того чтобы в журнал вводились данные, необходимо выбрать хотя бы один параметр ведения журнала или оба параметра.

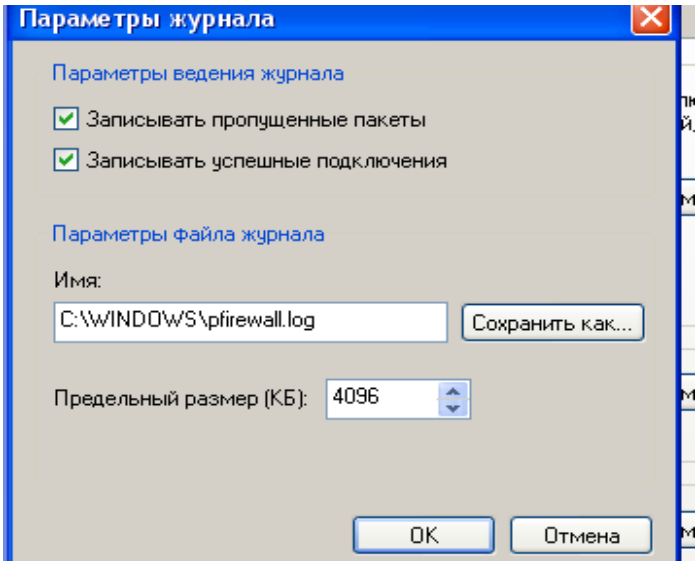

Рис. 50. Журнал безопасности

8. Теперь Ваш брандмауэр настроен и готов к защите Вашего компьютера от внешних угроз.

Задания для самостоятельной работы

1. Настройте брандмауэр на работу с Веб-сервером (HTTP), FTP-сервером и зафиксируйте соответствующее окно для отчета.
2. Включите журнал безопасности.
3. После выполнения задания 1 и 2 подключитесь к Интернету и посетите любой веб-сервер.
4. Завершите работу в Интернете и просмотрите журнал безопасности.
5. Зафиксируйте записи журнала безопасности для отчета.

Контрольные вопросы

1. Что такое брандмауэр?
2. Какие бывают брандмауэры?

3.Что фиксирует журнал безопасности брандмауэра?

ПРАКТИЧЕСКАЯ РАБОТА 10

Создание VPN-подключения средствами Windows 2000/XP/7/10

Краткие теоретические сведения

Технология виртуальных частных сетей (VPN – Virtual Private Network) является одним из эффективных механизмов обеспечения информационной безопасности при передаче данных в распределенных вычислительных сетях.

Виртуальные частные сети являются комбинацией нескольких самостоятельных сервисов (механизмов) безопасности: шифрования, экранирования и туннелирования.

Задание: создать VPN-подключение и выполнить его настройку.

Алгоритм выполнения работы

А. Создание VPN-подключения.

1. Откройте компонент **Сетевые подключения**. Для этого выберите последовательно **Пуск – Панель управления – Сетевые подключения (Центр управления сетями и общим доступом).**
2. Выберите пункт **Создание нового подключения (Настройка нового подключения или сети)** и нажмите кнопку **Далее.**
3. В зависимости от операционной системы выполните следующие действия:

■для Windows XP/7/10 – в открывшемся окне выберите пункт **Подключить к сети на рабочем месте** (рис. 51, только для XP) и нажмите **Далее**. После этого выберите **Подключение к виртуальной частной сети** (рис. 52) и нажмите **Далее.**

■для Windows 2000 – в открывшемся окне выберите пункт **Подключение к виртуальной частной сети через Интернет** и нажмите **Далее.**

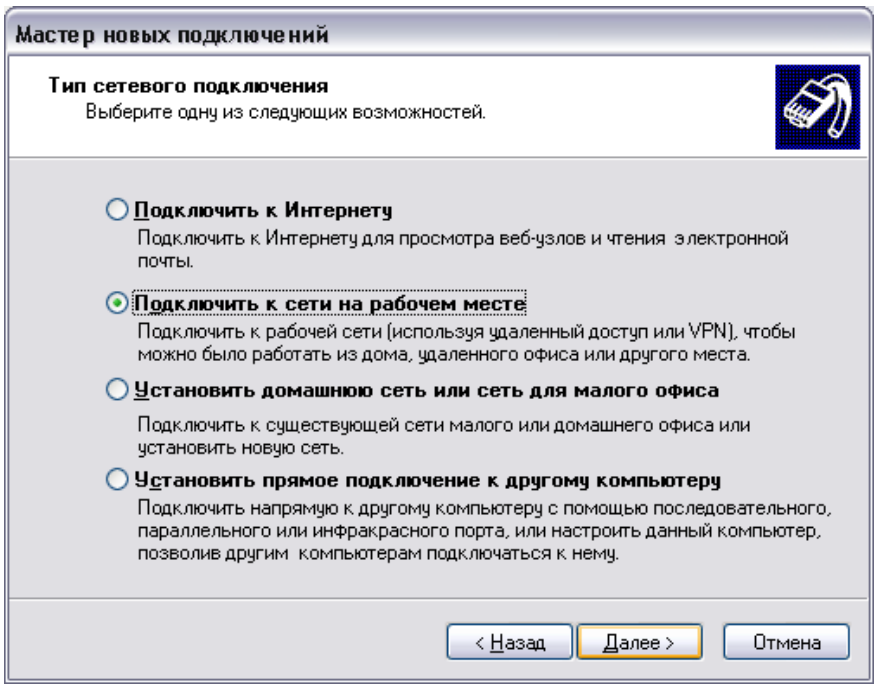

Рис. 51. VPN подключение для Windows XP/7/10

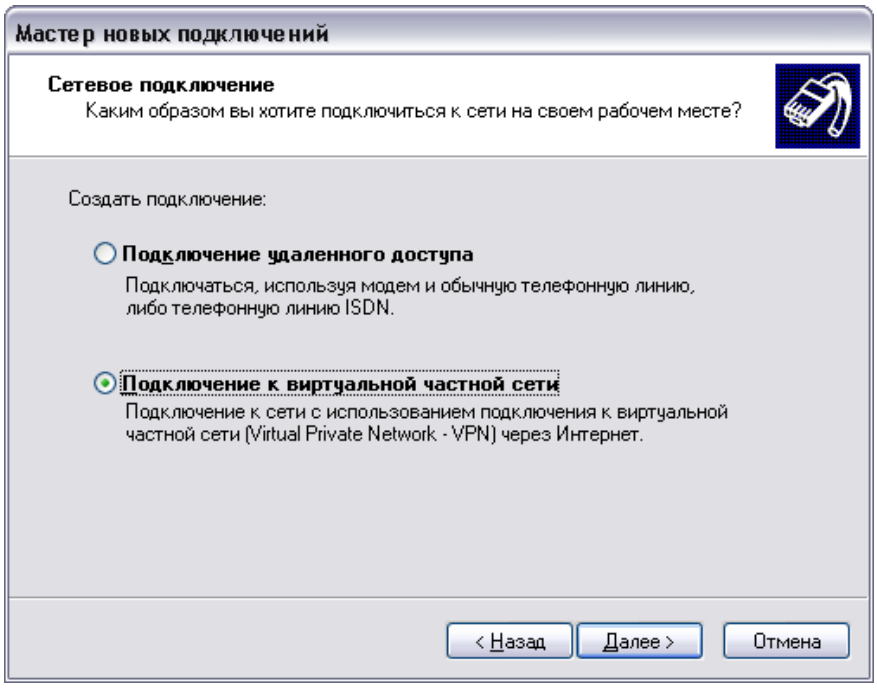

Рис. 52. VPN подключение для Windows 2000

5. Введите имя подключения и перейдите к следующему шагу командой **Далее**.

6. Если перед установкой «туннельного доступа» требуется подключение к провайдеру услуг Интернета, то выберите (рис. 53) **Набрать номер для следующего предварительного**

подключения и, выбрав нужное подключение, нажмите **Далее**. В противном случае, выберите **Не набирать номер для предварительного подключения** и нажмите **Далее.**

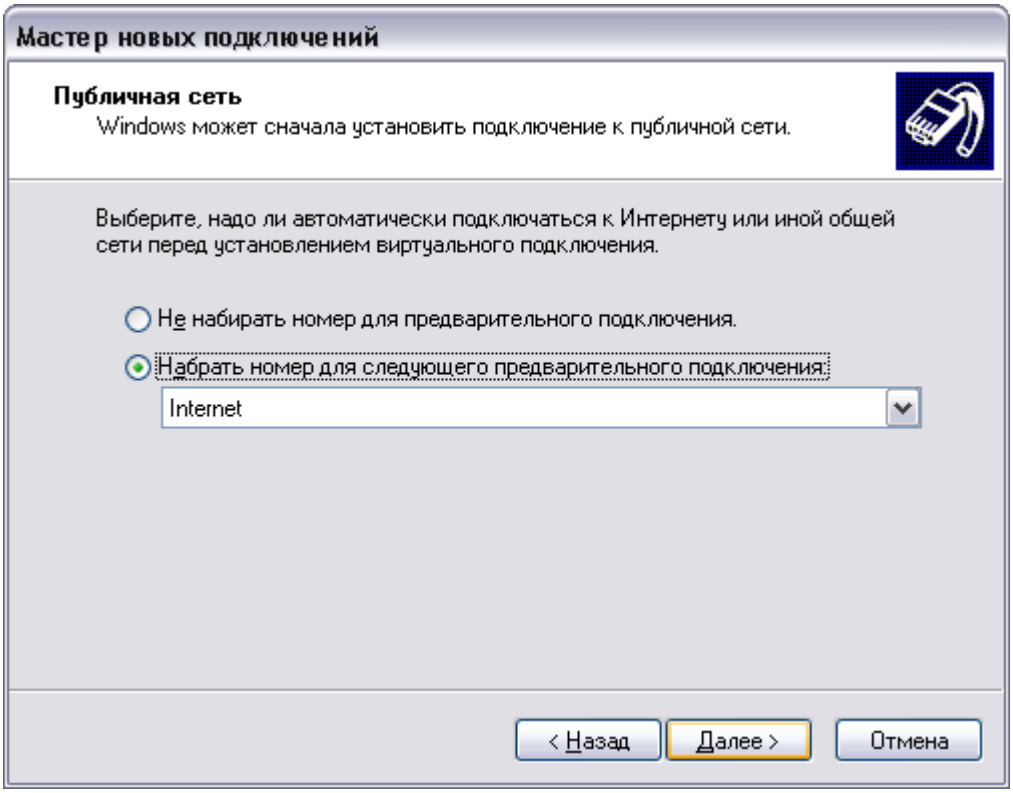

Рис.53. Установка номера

7. Введите имя узла (сети) или его IP-адрес (например 122.122.122.122), к которому идет подключение (рис.54).

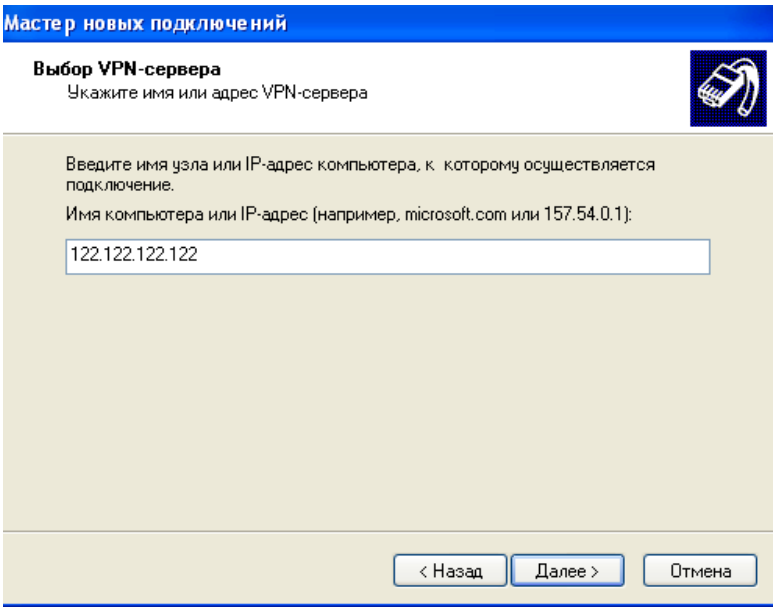

Рис. 54. Указание адреса

8. Завершите работу Мастера сетевых подключений.

9. В результате в папке Подключения появится новое подключение (рис. 55).

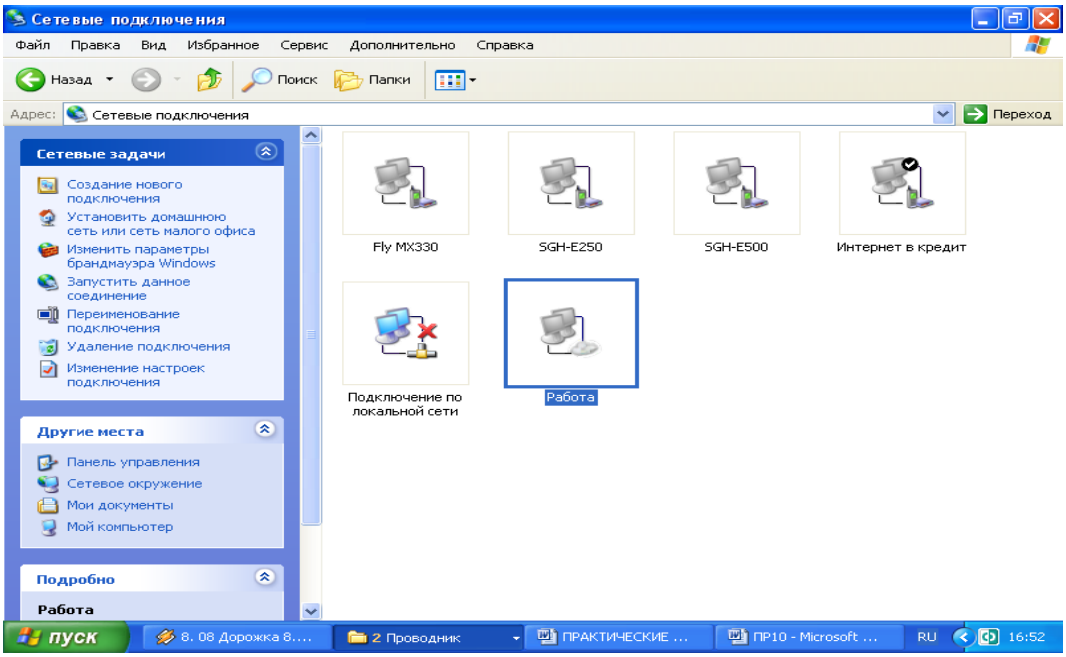

Рис.55. Список подключений

10. Для настройки параметров подключения выделите подключение VPN и вызовите его свойства из контекстного меню (нажатие правой клавиши мыши).

11. Рассмотрите все имеющиеся параметры VPN-подключения и при необходимости воспользуйтесь соответствующими разделами справки.

Задания для самостоятельной работы

Создайте VPN-подключение к узлу с адресом 122.122.122.122 и зафиксируйте окно его свойств (Print Screen) на закладке Общие (как показано на рис. 5) в качестве отчета.

Контрольные вопросы

1. Какие механизмы безопасности используются при реализации VPN-подключения?

2. Что такое «туннель» и в чем состоит принцип «туннелирования»?

3. В чем заключаются защитные функции виртуальных частных сетей?

ЗАКЛЮЧЕНИЕ

Проблема обеспечения, информационной безопасности широка и многогранна. За внешней тривиальностью, заключающейся в обеспечении трех составляющих информационной безопасности (доступности, целостности и конфиденциальности информации) скрывается значительный перечень мероприятий: от общих решений, принимаемых в интересах всего общества и государства, до частных решений применительно к отдельному носителю информации.

На сегодняшний день в нашей стране в целом сформирована единая политика в сфере обеспечения информационной безопасности. Для этого принят целый ряд основополагающих законов, также разработаны ключевые оценочные стандарты средств автоматизированной обработки, хранения, отображения и обмена информацией.

Опыт ведущих развитых стран показывает, что по мере все большей автоматизации и информатизации общественной жизни проблема информационной безопасности будет все больше обостряться.

Наличие проблем с обеспечением защищенности информации и поддерживающей ее инфраструктуры на сегодняшний день сдерживает развитие таких перспективных экономических направлений, как электронная коммерция, электронный бизнес, безбумажный документооборот и др., которые могут реально повысить эффективность функционирования целых отраслей производства и сферы сервисных услуг.

В нашей стране все более востребованными становятся услуги специалистов, занимающихся вопросами защиты информации. На этом фоне появляются крупные компании, оказывающие подобные услуги, разрабатывающие специализированные аппаратно-программные комплексы защиты информации, что дополнительно подтверждает актуальность проблемы обеспечения информационной безопасности.

В связи с этим можно отметить, что современный человек, хоть как-то связанный с информационными технологиями и средствами автоматизации обработки информации, должен представлять основные источники и угрозы информационной безопасности, а самое главное, должен знать основные приемы безопасной работы. Именно с этой точки зрения излагался материал данного пособия.

Пользователи, у которых данный материал вызвал дополнительный интерес, могут воспользоваться литературой, приведенной в конце каждого раздела. Наиболее актуальную информацию по проблеме обеспечения информационной безопасности можно найти в периодических изданиях, а также в глобальной сети Интернет.

СЛОВАРЬ ТЕРМИНОВ

Информационная безопасность – это защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб владельцам или пользователям информации.

Защита информации – это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Доступность – это гарантия получения требуемой информации или информационной услуги пользователем за определенное время.

Целостность – гарантия того, что информация сейчас существует в ее исходном виде, то есть при ее хранении или передаче не было произведено несанкционированных изменений.

Конфиденциальность – гарантия доступности конкретной информации только тому кругу лиц, для кого она предназначена.

Государственная тайна – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

Система защиты государственной тайны – совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях.

Средства защиты информации – технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

Политика безопасности – это комплекс предупредительных мер по обеспечению информационной безопасности организации. Политика безопасности включает правила, процедуры и руководящие принципы в области безопасности, которыми руководствуется организация в своей деятельности.

Угроза «информационной безопасности» – это потенциальная возможность нарушения режима информационной безопасности. Преднамеренная реализация угрозы называется ***атакой*** на информационную систему.

Программный вирус – это исполняемый или интерпретируемый программный код, обладающий свойством несанкционированного распространения и самовоспроизведения в автоматизированных системах или телекоммуникационных сетях с целью изменить или уничтожить программное обеспечение и/или данные, хранящиеся в автоматизированных системах.

Удаленная угроза – потенциально возможное информационное разрушающее воздействие на распределенную вычислительную сеть, осуществляемая программно по каналам связи.

Идентификация – присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным.

Аутентификация (установление подлинности) – проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности.

Электронная цифровая подпись – представляет собой относительно небольшое количество дополнительной аутентифицирующей информации, передаваемой вместе с подписываемым текстом.

Аудит – это анализ накопленной информации, проводимый оперативно, в реальном времени или периодически (например, раз в день).

Активный аудит – оперативный аудит с автоматическим реагированием на выявленные нештатные ситуации.

Межсетевой экран (брандмауэр, firewall) – это программная или программно-аппаратная система, которая контролирует информационные потоки, поступающие в информационную систему и/или выходящие из нее, также обеспечивает защиту информационной системы посредством фильтрации информации. Фильтрация информации состоит в анализе информации по совокупности критериев и принятии решения о ее приеме и/или передаче.

ВАРИАНТЫ ТЕСТОВЫХ КОНТРОЛЬНЫХ ЗАДАНИЙ

Вариант №1

1. Информационная безопасность характеризует защищенность:
   - пользователя информационной системы;
   - информации и поддерживающей ее инфраструктуры;
   - источника информации;
   - носителя информации.
2. Что из перечисленного является составляющей информационной безопасности?:
   - нарушение целостности информации;
   - проверка прав доступа к информации;
   - доступность информации;
   - выявление нарушителей.
3. Конфиденциальность информации гарантирует:
   - доступность информации кругу лиц, для кого она предназначена;
   - защищенность информации от потери;
   - защищенность информации от фальсификации;
   - доступность информации только автору.
4. Сколько уровней формирования режима информационной безопасности?:
   - три;
   - четыре;
   - два;
   - пять.
5. Какой из перечисленных уровней не относится к уровням формирования режима информационной безопасности?:
   - законодательно-правовой;
   - информационный;
   - административный (организационный);
   - программно-технический.
6. Средства защиты информации какого из уровней формирования режима информационной безопасности связаны непосредственно с защищаемой информацией?:
   - законодательно-правовой;

- информационный;
- административный (организационный);
- программно-технический.

7. Основополагающим документом по информационной безопасности в РФ является:

- Конституция РФ;
- Уголовный кодекс;
- Закон о средствах массовой информации;
- Закон об информационной безопасности.

8. Сколько категорий государственных информационных ресурсов определяет Закон «Об информации, информатизации и защите информации»?:

- три;
- четыре;
- два;
- пять.

9. Неправомерный доступ к компьютерной информации наказывается штрафом:

- от пяти до двадцати минимальных размеров оплаты труда;
- от двухсот до пятисот минимальных размеров оплаты труда;
- от ста пятидесяти до двухсот минимальных размеров оплаты труда;
- до трехсот минимальных размеров оплаты труда.

10. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети наказывается ограничением свободы на срок:

- до года;
- до двух лет;
- до пяти лет;
- до трех месяцев.

11. Подберите словосочетание к данному определению:

_____ – это защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб владельцам или пользователям информации.

- компьютерная безопасность;
- информационная безопасность;

- защита информации;
- защита государственной тайны.

12. Что из перечисленного является задачей информационной безопасности?:

- устранение неисправностей аппаратных средств;
- устранение последствий стихийных бедствий;
- защита технических и программных средств информатизации от ошибочных действий персонала;
- восстановление линий связи.

13. Выберите правильную иерархию пространства требований в «Общих критериях»:

- класс – семейство – компонент – элемент;
- элемент – класс – семейство – компонент;
- компонент – семейство – класс – элемент;
- семейство – компонент – класс – элемент;

14. Что не относится к механизмам безопасности в соответствии с X.800?:

- шифрование;
- электронная цифровая подпись;
- механизм управления доступом;
- механизм подотчетности.

15. Сколько классов СВТ по уровню защищенности от НСД к информации определено в руководящем документе Гостехкомиссии «СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации»?:

- три;
- семь;
- пять;
- четыре.

16. Подберите словосочетание к данному определению:

_____ – комплекс предупредительных мер по обеспечению информационной безопасности организации.

- информационная политика;
- политика безопасности;
- информационная безопасность;
- защита информации.

17. Что не рассматривается в политике безопасности?

- требуемый уровень защиты данных;
- роли субъектов информационных отношений;
- анализ рисков;
- защищенность механизмов безопасности.

18. Подберите словосочетание к данному определению:

_____ – это исполняемый или интерпретируемый программный код, обладающий свойством несанкционированного распространения и самовоспроизведения в автоматизированных системах или телекоммуникационных сетях с целью изменить или уничтожить программное обеспечение и/или данные, хранящиеся в автоматизированных системах.

- троянская программа;
- компьютерный вирус;
- программный вирус;
- вирус;

19. Основная особенность компьютерных вирусов заключается:

- в возможности их самопроизвольного внедрения в различные объекты операционной системы;
- в возможности нарушения информационной безопасности;
- в возможности заражения окружающих;
- в их постоянном существовании.

20. По особенностям алгоритма работы вирусы бывают

- резидентные и стелс-вирусы;
- полиморфик-генераторы и загрузочные вирусы;
- макро-вирусы и логические бомбы;
- утилиты скрытого администрирования;

21.«Маски» вирусов используются:

- для поиска известных вирусов;
- для создания известных вирусов;
- для уничтожения известных вирусов;
- для размножения вирусов.

22. Подберите слово к данному определению:

_____ – это достаточно труднообнаруживаемые вирусы, не имеющие сигнатур, то есть не содержащие ни одного постоянного участка кода.

- полиморфик-вирусы;

- стелс-вирусы;
- макро-вирусы;
- конструкторы вирусов;

23. Угроза перехвата данных может привести:

- к нарушению доступности данных;
- к нарушению доступности и целостности данных;
- к нарушению целостности данных;
- к нарушению конфиденциальности данных.

24. Идентификация и аутентификации применяются:

- для повышения физической защиты информационной системы;
- для ограничения доступа случайных и незаконных субъектов к информационной системе;
- для защиты от компьютерных вирусов;
- для обеспечения целостности данных.

25. Подберите слово к данному определению

_____ – присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным.

- аутентификация;
- идентификация;
- аутентичность;
- конфиденциальность.

26. Подберите слово к данному определению

_____ – проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности.

- аутентификация;
- идентификация;
- целостность;
- конфиденциальность.

27. Что из перечисленного не является идентификатором при аутентификации?:

- пароль;
- особенности поведения пользователя;
- персональный идентификатор;
- секретный ключ.

28. Постоянные пароли относятся к:

- статической аутентификации;
- временной аутентификации;
- устойчивой аутентификации;
- постоянной аутентификации.

29. Подберите словосочетание к данному определению:

_____ – представляет собой относительно небольшое количество дополнительной аутентифицирующей информации, передаваемой вместе с подписываемым текстом.

- закрытый ключ шифрования;
- электронная цифровая подпись;
- вирусная маска;
- открытый ключ шифрования.

30. К какому из перечисленных методов управления доступом относится определение?

_____ – основано на сопоставлении меток конфиденциальности информации, содержащейся в объектах, и официального разрешения субъекта к информации соответствующего уровня конфиденциальности.

- мандатное управление доступом;
- принудительное управление доступом;
- дискретное управление доступом;
- статистическое управление доступом.

Вариант №2

1. Что из перечисленного является составляющей информационной безопасности?:
   - целостность информации;
   - несанкционированный доступ к информации;
   - санкционированный доступ к информации;
   - антивирусная защита.
2. Доступность информации гарантирует:
   - неизменность информации в любое время;
   - получение требуемой информации за определенное время;
   - получение требуемой информации за неопределенное время;
   - защищенность информации от возможных угроз.
3. На каком из уровней формирования режима информационной безопасности разрабатывается политика безопасности?
   - информационный;
   - административный (организационный);
   - законодательно-правовой;
   - программно-технический.
4. Программно-технический уровень формирования режима информационной безопасности включает:
   - три подуровня;
   - два подуровня;
   - шесть подуровней.
5. Неправомерный доступ к компьютерной информации наказывается лишением свободы:
   - до пяти лет;
   - до трех лет;
   - до года;
   - до двух лет.
6. Создание, использование и распространение вредоносных программ для ЭВМ наказывается:
   - лишением свободы до года;
   - штрафом до двадцати минимальных размеров оплаты труда;

- лишением свободы до трех лет и штрафом от двухсот до пятисот минимальных размеров оплаты труда;
- исправительными работами до пяти лет;

7. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети наказывается:
- штрафом до ста минимальных размеров оплаты труда;
- ограничением свободы;
- лишением свободы;
- штрафом до пятисот минимальных размеров оплаты труда.

8. Наиболее общую, «предметную» группировку требований в «Общих критериях» определяет:
- класс требований;
- элемент требований;
- компонент требований;
- семейство требований.

9. Какой документ определяет сервисы безопасности для вычислительных сетей?:
- «оранжевая» книга;
- рекомендации X.800;
- рекомендации X.200;
- рекомендации X.450.

10. Сколько классов автоматизированных систем, подлежащих защите от несанкционированного доступа к информации, определено в руководящем документе Гостехкомиссии «АС. Защита от НСД к информации. Классификация АС и требования по защите информации»?:
- девять;
- семь;
- пять;
- двенадцать.

11. Что не является содержанием административного уровня формирования режима информационной безопасности?:
- разработка политики безопасности;
- проведение анализа угроз и расчета рисков;
- выбор механизмов обеспечения информационной безопасности.
- внедрение механизмов безопасности.

12. Подберите словосочетание к данному определению:

_____ – это потенциальная возможность нарушения режима информационной безопасности.

- несанкционированный доступ к информации;
- просмотр конфиденциальной информации;
- угроза «информационной безопасности»;
- фальсификация информации.

13. Что не является причиной случайных воздействий на информационную систему?:

- отказы и сбои аппаратуры;
- ошибки персонала;
- помехи в линиях связи из-за воздействий внешней среды;
- подбор пароля.

14. Что является самым эффективным при борьбе с не преднамеренными случайными ошибками?:

- определение степени ответственности за ошибки;
- резервирование аппаратуры;
- максимальная автоматизация и строгий контроль;
- контроль действий пользователя.

15. Какая организация в РФ разрабатывает стандарты и руководящие документы, направленные на обеспечение информационной безопасности?:

- Гостехкомиссия;
- Гостехнадзор;
- Государственная Дума;
- Гостехконтроль.

16. Что из перечисленного не относится к вредоносным программам?:

- логическая бомба;
- «троянский конь»;
- макро - вирус;
- конструкторы вирусов;

17. Какой из вирусов при инфицировании компьютера оставляет в оперативной памяти свою часть, которая затем перехватывает обращения операционной системы к объектам заражения и внедряется в них?:

- нерезидентный вирус;

- файловый вирус;
- резидентный вирус;
- загрузочный вирус.

18. Что из перечисленного не относится к вредоносным программам?:

- файловый вирус;
- логическая бомба;
- «троянский конь»;
- конструкторы вирусов;

19. Главной функцией полиморфик - генератора является:

- поиск новых вирусов;
- удаление антивирусной программы;
- шифрование тела вируса;
- размножение вируса.

20. Подберите словосочетание к данному определению:

_____ – потенциально возможное информационное разрушающее воздействие на распределенную вычислительную сеть, осуществляемая программно по каналам связи.

- перехват данных;
- удаленная угроза;
- угроза информационной безопасности;
- программный вирус;

21. Для повышения защищенности вычислительных сетей при установлении виртуального соединения наиболее надежно:

- повысить уровень физической защиты линий связи;
- использовать криптоалгоритмы с открытым ключом;
- выбрать оптимальный канал передачи данных;
- использовать межсетевой экран.

22. Что из перечисленного не является идентификатором при аутентификации?:

- пароль;
- секретный ключ;
- персональный идентификатор;
- отпечатки пальцев.

23. Что из перечисленного не относится к категориям аутентификации?:

- статическая аутентификация;

- временная аутентификация;
- устойчивая аутентификация;
- постоянная аутентификация.

24. Что из перечисленного не входит в криптосистему?:
- алгоритм шифрования;
- набор ключей, используемых для шифрования;
- полиморфик-генератор;
- система управления ключами.

25.Что не является задачей криптосистемы?:
- обеспечение конфиденциальности;
- регистрация и аудит нарушений;
- обеспечение целостности данных;
- аутентификация данных и их источников.

26. При асимметричном шифровании для шифрования и расшифровки используются:
- два взаимосвязанных ключа;
- один открытый ключ;
- один закрытый ключ;
- два открытых ключа.

27. Для контроля целостности передаваемых по сетям данных используется:
- аутентификация данных;
- электронная цифровая подпись;
- аудит событий;
- межсетевое экранирование.

28. Какой вид разграничения доступа определен в документах Гостехкомиссии РФ?:
- принудительное управление доступом;
- дискретное управление доступом;
- произвольное управление доступом;
- статистическое управление доступом.

29. Подберите слово к данному определению:

_____ – это анализ накопленной информации, проводимый оперативно, в реальном времени или периодически (например, раз в день).
- аудит;
- аутентификация;

- регистрация;
- идентификация.

30. Какой механизм безопасности является сильным психологическим средством?:

- VPN;
- аутентификация;
- идентификация;
- регистрация и аудит.

Вариант №3

1. Целостность информации гарантирует:
- существование информации в исходном виде;
- принадлежность информации автору;
- доступ информации определенному кругу пользователей;
- защищенность информации от несанкционированного доступа.

2. Какой из уровней формирования режима информационной безопасности включает комплекс мероприятий, реализующих практические механизмы защиты информации?:
- законодательно-правовой;
- информационный;
- административный (организационный);
- программно-технический.

3. Какой из уровней формирования режима информационной безопасности включает физический подуровень?:
- административный (организационный);
- законодательно-правовой;
- информационный;
- программно-технический.

4. Создание, использование и распространение вредоносных программ для ЭВМ, повлекшее тяжкие последствия, наказывается лишением свободы:
- до пяти лет;
- до шести лет;
- до семи лет;
- до четырех лет.

5. Минимальный набор требований в «Общих критериях» определяет:
- класс требований;
- элемент требований;
- компонент требований;
- семейство требований.

6. Сколько классов защищенности межсетевых экранов определено в руководящем документе Гостехкомиссии «СВТ. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации»?:

- три;
- семь;
- пять;
- шесть.

7. Что не является содержанием административного уровня формирования режима информационной безопасности?:
- разработка политики безопасности;
- настройка механизмов безопасности;
- проведение анализа угроз и расчета рисков;
- выбор механизмов обеспечения информационной безопасности.

8. Аутентичность связана:
- с проверкой прав доступа;
- с доказательством авторства документа;
- с изменением авторства документа;
- с контролем целостности данных.

9. Что из перечисленного является компьютерным вирусом?:
- полиморфик-генератор;
- утилита скрытого администрирования;
- макро-вирус;
- логическая бомба.

10. Какие вирусы заражают файлы-документы и электронные таблицы офисных приложений?:
- файловый вирус;
- сетевой вирус;
- макро-вирус;
- загрузочный вирус.

11. Самошифрование и полиморфичность используются для:
- саморазмножения вируса;
- максимального усложнения процедуры обнаружения вируса;
- расшифровки тел вируса;
- для скрытия действий антивирусной программы.

12. Одним из наиболее эффективных способов борьбы с вирусами является:
- использование антивирусного программного обеспечения;
- профилактика компьютерных вирусов;

- ограничение доступа пользователей к ЭВМ;
- шифрование данных.

13. Выберете вид антивирусных программ, перехватывающих «вирусоопасные » ситуации и сообщающих об этом пользователю:
- иммунизатор;
- блокировщик;
- сканер;
- CRC-сканер.

14. Какой вид антивирусных программ основан на подсчете контрольных сумм для присутствующих на диске файлов/ системных секторов?:
- иммунизатор;
- блокировщик;
- сканер;
- CRC-сканер.

15. Что из перечисленного не является причиной успешной реализации удаленных угроз в вычислительных сетях?:
- отсутствие выделенного канала связи между объектами вычислительной сети;
- взаимодействие объектов без установления виртуального канала;
- отсутствие в распределенных вычислительных сетях криптозащиты сообщений;
- взаимодействие объектов с установлением виртуального канала.

16. Что из перечисленного не является идентификатором при идентификации?:
- голос;
- рисунок радужной оболочки глаза;
- персональный идентификатор;
- отпечатки пальцев.

17. Какая категория аутентификации использует динамические данные аутентификации, меняющиеся с каждым сеансом работы?:
- статическая аутентификация;
- временная аутентификация;
- устойчивая аутентификация;

- постоянная аутентификация.

18. Какая категория аутентификации защищает данные от несанкционированной модификации?:

- постоянная аутентификация;
- временная аутентификация;
- статическая аутентификация;
- устойчивая аутентификация.

19.Что не является задачей криптосистемы?:

- обеспечение конфиденциальности;
- обеспечение целостности данных;
- аутентификация данных и их источников;
- межсетевое экранирование.

20. При симметричном шифровании для шифрования и расшифровки используются:

- два ключа разной длины;
- два разных по значению ключа;
- один и тот же ключ;
- два открытых ключа.
- Что из перечисленного не является функцией управления криптографическими ключами?:
- генерация;
- хранение;
- распределение;
- изучение.

22. Что из перечисленного не относится к разграничению доступа пользователей?:

- матрицы установления полномочий;
- парольное разграничение доступа;
- разграничение криптографических ключей;
- разграничение доступа по спискам.

23. Какой вид разграничения доступа определен в документах Гостехкомиссии РФ?:

- эвристическое управление доступом;
- мандатное управление доступом;
- принудительное управление доступом;
- статистическое управление доступом.

24. К какому из перечисленных методов управления доступом относится определение?:

_____ – представляет собой разграничение доступа между поименованными субъектами и поименованными объектами.

- мандатное управление доступом;
- дискретное управление доступом;
- принудительное управление доступом;
- статистическое управление доступом.

25. Какой из механизмов безопасности основан на подотчетности системы обеспечения безопасности?:

- аудит;
- аутентификация;
- регистрация;
- шифрование.

26. Подберите словосочетание к данному определению:

_____ – это хронологически упорядоченная совокупность записей результатов деятельности субъектов системы, достаточная для восстановления, просмотра и анализа последовательности действий, окружающих или приводящих к выполнению операций, процедур или совершению событий при транзакции с целью контроля конечного результата.

- матрица полномочий;
- регистрационный журнал;
- справочник безопасности;
- журнал учета времени работы на ЭВМ.

27. Что из перечисленного относится к аудиту безопасности?:

- сбор информации о событиях;
- хранение информации о событиях;
- защита содержимого журнала регистрации;
- анализ содержимого журнала регистрации.

28. Идентификация и аутентификации применяются:

- для регистрации событий безопасности;
- для выявления попыток несанкционированного доступа;
- для обеспечения целостности данных;
- для ограничения доступа случайных и незаконных субъектов информационной системы к ее объектам.

29. Подберите словосочетание к данному определению:

_____ – программная или программно-аппаратная система, которая выполняет контроль информационных потоков, поступающих в информационную систему и/или выходящих из нее, и обеспечивает защиту информационной системы посредством фильтрации информации.

- межсетевой экран;
- криптоалгоритм;
- сервер удаленного доступа;
- криптосистема.

30. Виртуальные частные сети включают следующие сервисы безопасности:

- экранирование и аудит;
- шифрование и туннелирование;
- регистрацию и контроль доступа;
- шифрование и электронную цифровую подпись.

Соответствие вопросов и ответов тестовых заданий

№ вопроса	Номер правильного ответа		
	Вариант № 1	Вариант № 2	Вариант № 3
1	2	1	1
2	3	2	3
3	1	2	4
4	1	1	3
5	2	4	3
6	4	3	3
7	1	2	2
8	4	1	2
9	2	2	3
10	2	1	3
11	2	4	2
12	3	3	1
13	1	4	2
14	4	3	4
15	2	1	4
16	2	3	3
17	4	3	3
18	3	1	1
19	1	3	4
20	1	2	3
21	1	2	4
22	1	4	3
23	4	2	2
24	2	3	2
25	2	2	3
26	1	1	2
27	2	2	4
28	1	2	4
29	2	1	1
30	1	4	2

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1.Касперский Е. Компьютерные вирусы. - М.:Эдель, 2018.

2.Касперский Е. Компьютерные вирусы, 2013. - Электронная энциклопедия. - Режим доступа к энциклопедии: http://www.viruslist.com/viruslistbooks.html

3.Щербаков А. Ю. Введение в теорию и практику компьютерной безопасности. - М.: Издательство Молгачева СВ., 2018.

4.Фролов А. В., Фролов Г. В. Осторожно: компьютерные вирусы. - М.: ДИАЛОГ-МИФИ, 2018.

5.Галатенко В. А. Основы информационной безопасности. - М: Интернет-Университет Информационных Технологий - ИНТУИТ.РУ, 2019.

6.Медведовский И.Д., Семьянов П.В., Леонов Д.Г., Лукацкий А.В. Атака из Internet. - М.: Солон-Р, 2019.

7.Медведовский И.Д., Семьянов П.В., Платонов В.В. Атака через Internet / Под ред. проф. П.Д. Зегжды. - НПО «Мир и семья-95», 2017.

8.Башлы П.Н. Современные сетевые технологии. Учебное пособие. - М: Горячая линия - Телеком, 2016.

9.Башлы П.Н. Информационная безопасность: Учебник. Ростов-на-Дону: Фолиант, 2019.

10. Карпов Е.А., Котенко И.В., Котухов М.М., Марков А.С.,Парр Г.А., Рунеев А.Ю. Законодательно-правовое и организационно-техническое обеспечение информационной безопасности автоматизированных систем и информационно-вычислительных сетей / Под редакцией И.В. Котенко. - СПб.: ВУС, 2019.

11. Спортак Марк, Паппас Френк. Компьютерные сети и сетевые технологии. - М.: ТИД «ДС», 2018.

12. Грязное Е., Панасенко С. Безопасность локальных сетей // Электронный журнал «Мир и безопасность» № 2, 2019. - Режим доступа к журн.: http://daily.sec.ru.

13. Ярочкин В.И. Информационная безопасность: Учебник для вузов. М.: Академический проспект, 2018.

14. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. - М.: ДМК, 2020.

15. Партыка Т.Л., Попов И.И. Информационная безопасность. Учебное пособие. - М.: ФОРУМ: ИНФРА-М, 2017.

16. Завгородний В.И. Комплексная защита информации в компьютерных системах: Учебное пособие. -М.: Логос; ПБОЮЛ Н.А., 2021.

17. П.Ю.Белкин, О.О. Михальский, В.Г. Проскурин и др. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных: Учеб. Пособие для вузов.- М.: Радио и связь, 2019. –168 с.

18. Проскурин В.Г., Крутов С.В. и др. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах: Учеб. Пособие для вузов.- М.: Радио и связь, 2018. –168 с.

19. Касперский Е. Компьютерные вирусы: что это такое и как с ними бороться. М.: СК Пресс, 2008.

20. Хореев А.А. Защита информации от утечки по техническим каналам. Часть 1. «Технические каналы утечки информации»/ М: Государственная техническая комиссия Российской Федерации, 2018.

21. Интернет-ресурсы. Web-сервер подразделения по выявлению и пресечению преступлений, совершаемых с использованием поддельных кредитных карт, и преступлений, совершаемых путем несанкционированного доступа в компьютерные сети и базы данных. Режим доступа: http://www.cyberpolice.ru

22. Интернет-ресурсы. Порталы по информационной безопасности. Режим доступа: http://infosecurity.report.ru , http://www.void.ru

23. Интернет-ресурсы. Российский криптографический портал. Режим доступа: http://www.cryptography.ru