Международный консорциум «Электронный университет»

Московский государственный университет экономики, статистики и информатики

Евразийский открытый институт

Сычев Ю.Н.

Основы информационной безопасности

Учебно-практическое пособие

Москва 2007

УДК 004.056
ББК –018.2*32.973
С 958

Сычев Ю.Н. **ОСНОВЫ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ** Учебно-практическое пособие. – М.: Изд. центр ЕАОИ, 2007. – 300 с.

СОДЕРЖАНИЕ

Сведения об авторе, разработавшим данный курс

Сычев Юрий Николаевич, кандидат экономических наук, доцент, профессор кафедры «Сетевая экономика и мировые информационные ресурсы».

Последние из опубликованных работ:

1. Защита информации // Сб. научн. тр. – М.: МЭСИ, 1999.
2. Оценка защищенности автоматизированных систем обработки информации методом интервального оценивания // Сб. научн. тр. – М.: МЭСИ, 2001.
3. Информационная безопасность: Учебное пособие, руководство по изучению дисциплины, практикум, тесты, учебная программа. – М.: МЭСИ, 2002.
4. Оптимизация затрат на применение системы защиты информации // Сб. научн. тр. – М.: МЭСИ, 2002.
5. Повышение вероятности отсутствия рисков скрытых вирусных искажений информации // Сб. научн. тр. – М.: МЭСИ, 2002.
6. Информационная безопасность: Учебное пособие, руководство по изучению дисциплины, практикум, тесты, учебная программа. – М.: МЭСИ, 2004.
7. Управление безопасностью и безопасность бизнеса: Учебное пособие, руководство по изучению дисциплины, практикум, тесты, учебная программа. – М.: МЭСИ, 2005.
8. Оценивание вероятности отсутствия рисков скрытых умышленных искажений информации // Сб. научн. тр. «Моделирование и проектирование информационных систем». - М.: МЭСИ, 2005.
9. Оценивание вероятности отсутствия рисков скрытых вирусных искажений информации // Сб. научн. тр. «Моделирование и проектирование информационных систем». – М.: МЭСИ, 2005.
10. Безопасность жизнедеятельности в чрезвычайных ситуациях: Учебное пособие, руководство по изучению дисциплины, практикум, тесты, учебная программа. – М.: МЭСИ, 2005.
11. Информационная безопасность Учебное пособие, руководство по изучению дисциплины, практикум, тесты, учебная программа. – М.: МЭСИ, 2007.
12. Безопасность жизнедеятельности в чрезвычайных ситуациях – М.: Финансы и статистика, 2007.
13. Безопасность жизнедеятельности: Учебное пособие, руководство по изучению дисциплины, практикум, тесты, учебная программа. – М.:МЭСИ, 2007.

Цели и задачи дисциплины

Содержание дисциплины «Основы информационной безопасности» для специальностей «Прикладная информатика в экономике», «Математическое обеспечение и администрирование информационных систем» ориентировано на получение студентами знаний по существующим угрозам безопасности информации, подбору и применению современных методов и способов защиты информации.

Цели преподавания дисциплины:

Основной целью курса является ознакомление студентов с тенденцией развития информационной безопасности, с моделями возможных угроз, терминологией и основными понятиями теории безопасности информации, а так же с нормативными документами России, по данному вопросу и правилами получения соответствующих сертификатов и лицензий.

Сфера профессионального использования:

Изучение дисциплины формирует знания и навыки, необходимые специалистам по защите информации и администраторам локальных сетей.

Для изучения данной дисциплины студент должен

- *знать:* основы теории вероятностей и математической статистики, особенности построения локальных и глобальных сетей, а так же программирование.

Тема 1.

Актуальность информационной безопасности, понятия и определения

Изучив тему 1, студент должен:
знать:

- статистику проявления компьютерных преступлений и наносимый ими ущерб;
- классификацию пользователей и злоумышленников в сети Интернет;
- причины уязвимости сети Интернет;
- основные понятия и определения, используемые при изучении информационной безопасности.
- статистику проявления компьютерных преступлений и наносимый ими ущерб.

уметь:

- объяснить необходимость изучения информационной безопасности.

акцентировать внимание на понятиях:

- безопасность информации, угроза безопасности информации, несанкционированный доступ, нарушитель, злоумышленник, защита информации, целостность информации, аутентификация, верификация, идентификация.

Содержание темы (дидактические единицы и их характеристика):

Информация – это дорогой товар, который всегда будет пользоваться большим спросом. Поэтому преступники различными способами пытаются завладеть информацией для ее продажи, изменения в свою пользу или уничтожения. Другие специалисты в основном ради самоутверждения разрабатывают и внедряют различные вредоносные программы – «компьютерные вирусы», которые направлены на уничтожение целых баз данных, изменение работы компьютерных систем, похищения и модификации информации и программ.

Цели и задачи изучения темы: Получение статистических знаний об атаках, которым подвергаются компьютерные системы и потерях банков. Изучение основных понятий и определений, используемых при изучении дисциплины.

Порядок изучения темы

Распределение бюджета времени по теме:

– количество часов, отведенных на практические занятия, из них в компьютерной аудитории – 4/4;
– количество часов, отведенных на самостоятельную работу, – 16.

Виды самостоятельной работы студентов:

– изучение учебного пособия «Информационная безопасность»;
– подготовка к участию в форуме по теме «Компьютерные преступления»;
– изучение дополнительной литературы;
– выполнение тестовых заданий по теме.

Методические указания по изучению вопросов темы

При изучении учебных вопросов:

- изучить тему 1 по учебному пособию «Информационная безопасность»;
- изучить дополнительные материалы;
- принять участие в форуме по теме «Компьютерные преступления»;

Вопросы темы

1.1. Актуальность информационной безопасности.
1.2. Национальные интересы РФ в информационной сфере и их обеспечение.
1.3. Классификация компьютерных преступлений.
1.4. Способы совершения компьютерных преступлений.
1.5. Пользователи и злоумышленники в Интернете.
1.6. Причины уязвимости сети Интернет.

1.1. Актуальность информационной безопасности

Проблема защиты информации от постороннего доступа и нежелательных воздействий на нее возникла давно, с той поры, когда человеку по каким-либо причинам не хотелось делиться ею ни

с кем или не с каждым человеком. С развитием человеческого общества, появлением частной собственности, государственного строя, борьбой за власть и дальнейшим расширением масштабов человеческой деятельности информация приобретает цену. Ценной становится та информация, обладание которой позволит ее существующему и потенциальному владельцам получить какой-либо выигрыш: материальный, политический, военный и т. д.

Еще 25-30 лет назад задача защиты информации могла быть эффективно решена с помощью организационных мер и отдельных программно-аппаратных средств разграничения доступа и шифрования. Появление персональных ЭВМ, локальных и глобальных сетей, спутниковых каналов связи, эффективной технической разведки и конфиденциальной информации существенно обострило проблему защиты информации.

Проблема надежного обеспечения сохранности информации является одной из важнейших проблем современности.

Особенностями современных информационных технологий являются:

- увеличение числа автоматизированных процессов в системах обработки данных и важность принимаемых на их основе решений;
- территориальная разнесенность компонентов компьютерной системы и передача информации между этими компонентами;
- усложнение программных и аппаратных средств компьютерных систем;
- накопление и длительное хранение больших массивов данных на электронных носителях;
- интеграция в единую базу данных информации различной направленности;
- непосредственный доступ к ресурсам компьютерной системы большого количества пользователей различной категории и с различными правами доступа в системе;
- рост стоимости ресурсов компьютерных систем.

Рост количества и качества угроз безопасности информации в компьютерных системах не всегда ведет к адекватному ответу на создание надежной системы и безопасных информационных технологий. В большинстве коммерческих и государственных организаций, не говоря о простых пользователях, в качестве средств защиты используются только антивирусные программы и разграничение прав доступа пользователей на основе паролей.

Деятельность любой организации в наше время связана с получением и передачей информации. Информация в настоящее время является стратегически важным товаром. Потеря информационных ресурсов или завладение секретной информацией конкурентами, как правило, наносит предприятию значительный ущерб и даже может привести к банкротству.

За последние 20 лет информационные технологии проникли во все сферы управления и ведения бизнеса. Сам же бизнес из реального мира давно переходит в мир виртуальный, а поэтому весьма зависим от вирусных, хакерских и прочих атак.

Первые преступления с использованием компьютерной техники появились в России в 1991 г., когда были похищены 125,5 тыс. долларов США во Внешэкономбанке СССР. В 2003 г. в России было возбуждено 1602 уголовных дела по ст.272 УК РФ («Неправомерный доступ к компьютерной информации») и 165 («Причинение имущественного ущерба путем обмана и злоупотребления доверием»).

По данным Института Компьютерной Безопасности, общий ущерб, который нанесли компьютерные вирусы за последние 5 лет, оценивается как минимум в 54 млрд долл. По данным журнала «Security Magazine», средний размер ущерба от «физического» ограбления банка составляет 2500 долл., а от компьютерного мошенничества – 500 тыс долл.

В последнее время количество компьютерных преступлений неуклонно увеличивается, возрастает их удельный вес по размерам похищаемых сумм и другим видам ущерба в общей доле материальных потерь от обычных видов преступлений. О динамике и масштабах этих преступных посягательств наглядно свидетельствуют следующие данные, полученные путем анализа и обобщения статистической информации, полученной из Главного информационного центра МВД России:

- за последние 10 лет их количество возросло в 22,3 раза и продолжает увеличиваться, в среднем в 3,5 раза ежегодно;
- ежегодный размер материального ущерба от рассматриваемых преступных посягательств составляет 613,7 млн руб.;
- средний ущерб, причиняемый потерпевшему от 1 компьютерного преступления, равен 1,7 млн руб.;
- с определенной долей успеха расследуется лишь около 49% преступлений;
- обвинительные приговоры выносятся лишь в 25,5% случаев от общего числа возбужденных уголовных дел;

• средний показатель количества уголовных дел, по которым производство приостановлено, составляет 43,5% и ярко отражает низкую степень профессионализма сотрудников правоохранительных органов в деятельности по раскрытию, расследованию и предупреждению указанных преступных посягательств.

С 1999 г. появилась еще одна проблема информационной безопасности – спам. Это анонимная массовая непрошеная рассылка. Сейчас около 30% всех электронных писем являются спамом. Наводнение спама приводит к ежегодным убыткам, оцененным до 20 млрд долл. Спам в пределах одной компании приводит к убыткам от 600 до 1000 долларов ежегодно, из расчета на одного пользователя.

Также широко распространяется сейчас промышленный шпионаж – устройство стоимостью всего 10$, в случае его удачного размещения может привести фирму к банкротству.

В наше время злоумышленники могут получить доступ не только к открытой информации, но и к информации, содержащей государственную и коммерческую тайну (в 2003 г. ФСБ пресечено более 900 попыток проникновения в информационные ресурсы органов государственной власти России).

1.2. Национальные интересы Российской Федерации в информационной сфере и их обеспечение

Современный этап развития общества характеризуется возрастающей ролью информационной сферы. Информационная сфера активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации. Национальная безопасность Российской Федерации существенным образом зависит от обеспечения информационной безопасности.

Под ***информационной безопасностью*** Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.

Интересы государства в информационной сфере заключаются в создании условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества.

На основе национальных интересов Российской Федерации в информационной сфере формируются стратегические и текущие задачи внутренней и внешней политики государства по обеспечению информационной безопасности.

Выделяются четыре основные составляющие национальных интересов Российской Федерации в информационной сфере.

Первая составляющая национальных интересов Российской Федерации в информационной сфере включает в себя соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.

Вторая составляющая национальных интересов Российской Федерации в информационной сфере включает в себя информационное обеспечение государственной политики Российской Федерации, связанное с доведением до российской и международной общественности достоверной информации о государственной политике Российской Федерации, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам.

Третья составляющая национальных интересов Российской Федерации в информационной сфере включает в себя развитие современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов.

Четвертая составляющая национальных интересов Российской Федерации в информационной сфере включает в себя защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России.

В этих целях необходимо:

- повысить безопасность информационных систем, включая сети связи, прежде всего безопасность первичных сетей связи и информационных систем органов государственной власти, финансово-кредитной и банковской сфер, сферы хозяйственной деятельности, а также систем и средств информатизации вооружения и военной техники, систем управления войсками и оружием, экологически опасными и экономически важными производствами;
- интенсифицировать развитие отечественного производства аппаратных и программных средств защиты информации и методов контроля за их эффективностью;
- обеспечить защиту сведений, составляющих государственную тайну;
- расширять международное сотрудничество Российской Федерации в области развития и безопасного использования информационных ресурсов, противодействия угрозе развязывания противоборства в информационной сфере.

1.3. Классификация компьютерных преступлений

Негативным последствием информатизации общества является появление так называемой компьютерной преступности. Сложность решения вопроса заключается в том, что диапазон противоправных действий, совершаемых с использованием средств компьютерной техники, чрезвычайно широк – от преступлений традиционного типа до требующих высокой математической и технической подготовки.

К разряду компьютерных следует отнести те преступления, у которых объектом преступного посягательства является информация, обрабатываемая и хранящаяся в компьютерных системах, а орудием посягательства служит компьютер. По этому пути пошло и российское законодательство.

С точки зрения уголовного законодательства, охраняется *компьютерная информация*, которая определяется как информация, зафиксированная на машинном носителе или передаваемая по телекоммуникационным каналам в форме, доступной восприятию ЭВМ. Вместо термина «компьютерная информация» можно использовать и термин «машинная информация», под которой подразумевается информация, которая запечатлена на машинном носителе, в памяти электронно-вычислительной машины, системе ЭВМ или их сети. В качестве предмета или орудия преступления, согласно законодательству, может выступать компьютерная информация, компьютер, компьютерная система или компьютерная сеть.

При рассмотрении вопросов о классификации компьютерных преступлений и их криминалистической характеристике целесообразно исходить из определения компьютерного преступления в широком смысле слова. В этом случае под компьютерным преступлением следует понимать предусмотренные законом общественноопасные деяния, совершаемые с использованием средств компьютерной техники. Правомерно также использовать термин «компьютерное преступление» в широком значении – как социологическую категорию, а не как понятие уголовного права.

Классификация компьютерных преступлений может быть проведена по различным основаниям. Так, например, можно условно подразделить все компьютерные преступления на две большие категории:

- преступления, связанные с вмешательством в работу компьютеров;
- преступления, использующие компьютеры как необходимые технические средства.

Выделяются следующие группы компьютерных преступлений:

- экономические преступления;
- преступления против личных прав и частной сферы;
- преступления против государственных и общественных интересов.

Экономические компьютерные преступления являются наиболее распространенными. Они совершаются по корыстным мотивам и включают в себя компьютерное мошенничество, кражу программ («компьютерное пиратство»), кражу услуг и машинного времени, экономический шпионаж.

Компьютерными преступлениями против личных прав и частной сферы являются незаконный сбор данных о лице, разглашение частной информации (например, банковской или врачебной тайны, информации о расходах и т.д.).

Компьютерные преступления против государственных и общественных интересов включают преступления, направленные против государственной и общественной безопасности (например, угрожающие обороноспособности государства, злоупотребления с автоматизированными системами голосования и т.д.).

Подходить к классификации компьютерных преступлений наиболее оправданно с позиций составов преступлений, которые могут быть отнесены к разряду компьютерных. Хотя состав компьютерных преступлений в настоящее время четко не определен, можно выделить ряд видов противоправных деяний, которые могут быть в него включены.

К основным видам преступлений, связанных с вмешательством в работу компьютеров, относятся:

1. Несанкционированный доступ в корыстных целях к информации, хранящейся в компьютере или информационно-вычислительной сети.

Несанкционированный доступ осуществляется, как правило, с использованием чужого имени, изменением физических адресов технических устройств, использованием информации, оставшейся после решения задач, модификацией программного и информационного обеспечения, хищением носителя информации, установкой аппаратуры записи, подключаемой к каналам передачи данных.

2. Разработка и распространение компьютерных вирусов.

Компьютерные вирусы обладают свойствами заражать программное обеспечение, базы данных и переходить через коммуникационные сети из одной системы в другую, распространяясь как вирусное заболевание.

3. Ввод в программное обеспечение «логических бомб».

«Логические бомбы» - это такие программы, которые срабатывают при выполнении определенных условий и частично или полностью выводят из строя программное обеспечение компьютерной системы.

4. Халатная небрежность при разработке, создании и эксплуатации программно-вычислительных комплексов и компьютерных сетей.

Особенностью компьютерных систем является то, что абсолютно безошибочных программ в принципе не бывает. Если проект

практически в любой области техники можно выполнить с огромным запасом надежности, то в области программирования такая надежность весьма условна, а в ряде случаев почти недостижима.

5. Подделка и фальсификация компьютерной информации.

Этот вид компьютерной преступности является одним из наиболее распространенных. Он является разновидностью несанкционированного доступа с той лишь разницей, что пользоваться им может сам разработчик, причем имеющий достаточно высокую квалификацию.

6. Хищение программного обеспечения.

Если «обычные» хищения подпадают под действие существующего уголовного закона, то проблема хищения программного обеспечения более сложна. Значительная часть программного обеспечения в России распространяется путем кражи и обмена краденым.

7. Несанкционированное копирование, изменение или уничтожение информации.

При неправомерном обращении в собственность машинная информация может не изыматься из фондов, а копироваться. Следовательно, машинная информация должна быть выделена как самостоятельный предмет уголовно-правовой охраны.

8. Несанкционированный просмотр или хищение информации из банков данных, баз данных и баз знаний.

В данном случае под базой данных следует понимать форму представления и организации данных, систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны с помощью ЭВМ.

Особенность компьютерных преступлений состоит и в том, что трудно найти другой вид преступления, после совершения которого его жертва не выказывает особой заинтересованности в поимке преступника, а сам преступник, будучи пойман, всячески рекламирует свою деятельность на поприще компьютерного взлома, не утаивая от представителей правоохранительных органов. Психологически этот парадокс вполне объясним.

Во-первых, жертва компьютерного преступления совершенно убеждена, что затраты на его раскрытие (включая потери, понесенные в результате утраты своей репутации) существенно превосходят уже причиненный ущерб.

Во-вторых, преступник приобретает широкую известность в деловых и криминальных кругах, что в дальнейшем позволяет ему с выгодой использовать приобретенный опыт.

1.4. Способы совершения компьютерных преступлений

Важнейшим и определяющим элементом криминалистической характеристики любого, в том числе и компьютерного, преступления является совокупность данных, характеризующих способ его совершения.

Под способом совершения преступления обычно понимают объективно и субъективно обусловленную систему поведения субъекта до, в момент и после совершения преступления, оставляющего различного рода характерные следы, позволяющие с помощью криминалистических приемов и средств получить представление о сути происшедшего, своеобразии преступного поведения правонарушителя, его отдельных личностных данных и, соответственно, определить наиболее оптимальные методы решения задач раскрытия преступления.

По способу совершения выделяют следующие группы компьютерных преступлений:

- воровство средств компьютерной техники;
- перехват информации;
- несанкционированный доступ;
- манипуляция данными и управляющими командами;
- комплексные методы.

К первой группе относятся традиционные способы совершения обычных видов преступлений, в которых действия преступника направлены на воровство чужого имущества. Характерной отличительной чертой данной группы способов совершения компьютерных преступлений будет тот факт, что в них средства компьютерной техники будут всегда выступать только в качестве предмета преступного посягательства.

Ко второй группе относятся способы совершения компьютерных преступлений, основанные на действиях преступника, направленных на получение данных и машинной информации посредством использования различных методов перехвата. К методам перехвата относятся:

- активный перехват;
- пассивный перехват;
- аудиоперехват;
- видеоперехват;
- просмотр мусора.

Активный перехват (interception) осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера, например линии принтера, или телефонному проводу канала связи, либо непосредственно через соответствующий порт персонального компьютера.

Пассивный (электромагнитный) перехват (electromagnetic pickup) основан на фиксации электромагнитных излучений, возникающих при функционировании многих средств компьютерной техники, включая и средства коммуникации (например, излучение электронно-лучевой трубки дисплея можно принимать с помощью специальных приборов на расстоянии до 1000 м).

Аудиоперехват, или снятие информации по виброакустическому каналу, является достаточно распространенным способом и имеет две разновидности. Первая заключается в установке подслушивающего устройства в аппаратуру средств обработки информации, вторая – в установке микрофона на инженерно-технические конструкции за пределами охраняемого помещения (стены, оконные рамы, двери и т.п.).

Видеоперехват осуществляется путем использования различной видеооптической техники.

Просмотр, или уборка «мусора» (scavening) представляет собой достаточно оригинальный способ перехвата информации. Преступником неправомерно используются технологические отходы информационного процесса, оставленные пользователем после работы с компьютерной техникой (например, удаленная с жестких дисков компьютера, а также съемных дисков информация может быть восстановлена и несанкционированно изъята с помощью специальных программных средств).

К третьей группе способов совершения компьютерных преступлений относятся действия преступника, направленные на получение несанкционированного доступа к информации.

К ним относятся следующие:

- «Компьютерный абордаж» (hacking) – несанкционированный доступ в компьютер или компьютерную сеть без права на то.

Этот способ используется хакерами для проникновения в чужие информационные сети.

- «За дураком» (piggybacking).

Этот способ используется преступниками путем подключения компьютерного терминала к каналу связи через коммуникационную аппаратуру в тот момент времени, когда сотрудник, отвечающий за

работу средства компьютерной техники, кратковременно покидает свое рабочее место, оставляя терминал в рабочем режиме.

- «За хвост» (between-the-lines entry).

При этом способе съема информации преступник подключается к линии связи законного пользователя и дожидается сигнала, обозначающего конец работы, перехватывает его на себя и осуществляет доступ к системе.

- «Неспешный выбор» (browsing).

При данном способе совершения преступления преступник осуществляет несанкционированный доступ к компьютерной системе путем нахождения уязвимых мест в ее защите.

- «Брешь» (trapdoor entry).

При данном способе преступником ищутся участки программ, имеющие ошибку или неудачную логику построения. Выявленные таким образом «бреши» могут использоваться преступником многократно, пока не будут обнаружены.

- «Люк» (trapdoor).

Данный способ является логическим продолжением предыдущего. В месте найденной «бреши» программа «разрывается», и туда дополнительно преступником вводится одна или несколько команд. Такой «люк» «открывается» по необходимости, а включенные команды автоматически выполняются.

К четвертой группе способов совершения компьютерных преступлений относятся действия преступников, связанные с использованием методов манипуляции данными и управляющими командами средств компьютерной техники. К этой группе относятся следующие способы совершения компьютерных преступлений:

- Написание программы, называемой «Троянский конь» (trojan horse).

Данный способ заключается в тайном введении в чужое программное обеспечение специально созданных программ, которые, попадая в информационно-вычислительные системы, начинают выполнять новые, не планировавшиеся законным владельцем действия, с одновременным сохранением прежних функций. В соответствии со ст. 273 Уголовного кодекса Российской Федерации под такой программой понимается «программа для ЭВМ, приводящая к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети». По существу «троянский конь» – это модернизация рассмотренного выше способа «люк» с той лишь разницей, что

люк «открывается» не при помощи непосредственных действий преступника, а автоматически, с использованием специально подготовленной для этих целей программы и без непосредственного участия самого преступника.

С помощью такого способа преступники обычно отчисляют на заранее открытый счет определенную сумму с каждой банковской операции. Возможен и вариант увеличения преступниками избыточных сумм на счетах при автоматическом пересчете рублевых остатков, связанных с переходом к коммерческому курсу соответствующей валюты.

Разновидностями такого способа совершения компьютерных преступлений является внедрение в программы «***логических бомб***» (logic bomb) и «***временных бомб***» (time bomb).

- Написание программы называемой «компьютерный вирус» (virus).

С уголовно-правовой точки зрения, согласно ст. 273 Уголовного кодекса РФ, под компьютерным вирусом следует понимать вредоносную программу для ЭВМ, способную самопроизвольно присоединяться к другим программам («заражать» их) и при запуске последних выполнять различные нежелательные действия: порчу файлов, искажение, стирание данных и информации, переполнение машинной памяти и создание помех в работе ЭВМ.

- Компьютерное мошенничество.

Данный вид компьютерных преступлений осуществляется способом «*подмены данных*» (*data digging*) или «*подмены кода*» (*code change*). Это наиболее простой и поэтому очень часто применяемый способ совершения преступления. Действия преступников в этом случае направлены на изменение или введение новых данных, и осуществляются они, как правило, при вводе-выводе информации.

- Незаконное копирование (тиражирование) программ с преодолением программных средств защиты предусматривает незаконное создание копии ключевой дискеты, модификацию кода системы защиты, моделирование обращения к ключевой дискете, снятие системы защиты из памяти ЭВМ и т.п.

Не секрет, что подавляющая часть программного обеспечения, используемого в России, является пиратскими копиями взломанных хакерами программ. В качестве примера незаконного тиражирования программ можно привести компьютерную базу российского законодательства «Консультант-плюс». Несмотря на постоянную работу специалистов фирмы по улучшению системы защиты, тысячи

нелегальных копий программы имеют хождение на территории России. Последняя, шестая версия «Консультанта» была «привязана» к дате создания компьютера, записанной в его постоянной памяти. Однако не прошло и двух недель после выхода этой версии, как хакерами была создана программа, эмулирующая нужную дату на любом компьютере.

Пятая группа способов – комплексные методы, которые включают в себя различные комбинации рассмотренных выше способов совершения компьютерных преступлений.

По международной классификации в отдельную группу принято выделять такие способы, как **компьютерный саботаж** с аппаратным или программным обеспечением, которые приводят к выводу из строя компьютерной системы. Наиболее значительные компьютерные преступления совершаются посредством порчи программного обеспечения, причем часто его совершают работники, недовольные своим служебным положением, отношением с руководством и т.д.

Существует ряд способов совершения компьютерных преступлений, которые сложно отнести к какой-либо группе. К таким способам относятся: асинхронная атака, моделирование, мистификация, маскарад и т.д.

Асинхронная атака (*Asynchronous attack*). Сложный способ, требующий хорошего знания операционной системы. Используя асинхронную природу функционирования большинства операционных систем, их заставляют работать при ложных условиях, из-за чего управление обработкой информации частично или полностью нарушается. Если лицо, совершающее «асинхронную атаку», достаточно профессионально, оно может использовать ситуацию, чтобы внести изменения в операционную систему или сориентировать ее на выполнение своих целей, причем извне эти изменения не будут заметны.

Моделирование (*Simulation*). Создается модель конкретной системы, в которую вводятся исходные данные и учитываются планируемые действия. На основании полученных результатов методом компьютерного перебора и сортировки выбираются возможные подходящие комбинации. Затем модель возвращается к исходной точке и выясняется, какие манипуляции с входными данными нужно проводить для получения на выходе желаемого результата. В принципе, «прокручивание» модели вперед-назад может происходить многократно, чтобы через несколько итераций добиться необ-

ходимого итога. После этого остается осуществить задуманное на практике.

Мистификация (*spoofing*). Возможна, например, в случаях, когда пользователь удаленного терминала ошибочно подключается к какой-либо системе, будучи абсолютно уверенным, что работает именно с той самой системой, с которой намеревался. Владелец системы, к которой произошло подключение, формируя правдоподобные отклики, может поддержать контакт в течение определенного времени и получать конфиденциальную информацию, в частности коды пользователя и т.д.

1.5. Пользователи и злоумышленники в Интернете

Интернет – это объединение в масштабе всей планеты группы сетей, которое использует единый протокол для передачи данных.

Известно, что изначально Интернет был лишь сетью, связывающей научные организации США, работавшие под руководством правительства. Сейчас Интернет – это всемирная паутина, объединяющая множество компьютеров. Все больше организаций присоединяются к Интернету для того, чтобы воспользоваться его преимуществами и ресурсами. Бизнесмены и государственные организации используют Интернет в самых различных целях – включая обмен электронной почтой, распространение информации среди заинтересованных лиц и проведение исследований. Да и обычных пользователей – частных лиц становиться все больше. Они общаются между собой, играют в различные сетевые игры, покупают товары в виртуальных магазинах и т.д.

С повышением компьютерной грамотности населения неизбежно растет число так называемых «злоумышленников» наряду с обычными, безобидными пользователями. Они, преследуя различные цели, нарушают работу обычных пользователей, нанося различного рода ущерб. Действия злоумышленников трудно предсказать и порой ее бывает трудно обнаружить и остановить. Многие организации уже понесли значительные финансовые потери из-за деятельности злоумышленников, некоторым организациям был нанесен урон их репутации, когда стало известно о проникновениях в их сети.

Возможности Интернета растут с каждым днем. Теперь можно

вообще не выходить из дома, так как современные средства коммуникации позволяют работать через Интернет, делать покупки, переводить деньги и так далее. Но существует и угроза потери, как данных, так и денег, так как злоумышленников, которые хотят ими воспользоваться, становится все больше.

Злоумышленников классифицируют на две большие группы: шпионы и луддиты.

Шпионы занимаются кражей информации, а луддиты взламывают сети и управляют ею, засылая туда вирусы.

Эти группы подразделяются на: хакеров, фракеров, кракеров, фишеров, скамеров, спамеров.

Хакеры

Слово хакер (hacker) проникло в русский язык из английского. Хакерами в XIX веке называли плохих игроков в гольф, своего рода дилетантов. Потом это понятие перекочевало в обыденную жизнь и стало использоваться чопорными англичанами для обозначения непрофессионалов в любых сферах деятельности.

Хакеров тоже можно разделить на четыре группы.

Первая группа. Случайные люди и политические активисты.

К первой группе компьютерных хулиганов относятся те, кто иногда занимаются взломом чужих программ. Большинство из таких хакеров – вполне приличные люди, профессиональные программисты, которые используют свои знания и умения для удовлетворения собственного любопытства или самоутверждения. К этой же группе относятся и хакеры, мотивы деятельности которых лежат в области политики. Многие взломщики, провозглашающие себя борцами за политические идеалы, на самом деле подобным образом реализуют свои несколько наивные представления о том, что, совершая мелкие гадости по отношению, например, к сайтам ненавистного им политического течения, они творят правосудие. Некоторые из них проникают на сайты конкурирующих политических организаций, другие помогают диссидентам, проживающим в условиях тоталитарных режимов, обмениваться информацией с внешним миром.

Вторая группа. Собственные сотрудники компании.

Персонал и доверенные лица, к которым относятся консультанты, эксперты или поставщики, представляют собой наибольшую угрозу для корпоративной системы компьютерной безопасности. Вовлеченные в сложные бизнес-отношения, эти лица могут иметь собственные мотивы для совершения компьютерных правонаруше-

ний, причем мотивы эти бывают весьма курьезного свойства. Например, взлом корпоративного сервера может быть совершен из стремления удовлетворить собственное любопытство относительно заработной платы коллег по работе или из-за обиды на руководство.

Третья группа. Кибер-хакеры.

Последнюю категорию хакеров составляют программисты высочайшего уровня, для которых компьютерный взлом стал профессией.

Американские власти панически боятся киберпреступников и тратят огромные деньги на борьбу с ними. Только по официальным данным, в прошлом году жертвами компьютерных взломщиков стали около 85% коммерческих компаний и правительственных организаций.

Еще в июле Генпрокуратура США создала десять новых подразделений для борьбы с киберпреступлениями.

В ФБР считают, что инструменты и методы, используемые постоянно совершенствующимися в своем мастерстве хакерами, нацелены на разрушение экономики США и являются частью замысла террористов. Террористы нанимают хакеров и фишеров для зарабатывания денег, установления контроля над интересующими их объектами, а также в целях пропаганды своих идей и деятельности.

Четвертая группа. Легальные хакеры.

Это те, которые абсолютно легально работают на различные компании, пытаются взломать их сайты, а если им это удается, то показывают разработчикам на «дыры» в системе. Но здесь есть определенная опасность.

С одной стороны, компания, нанявшая такого специалиста, рискует потерять конфиденциальную информацию, ведь никто не знает, как воспользуется взломанной информацией такой работник.

Но существует и обратная угроза. За таким делом могут поймать и самого взломщика. Так в 2003 г. произошло с русским хакером Алексеем Ивановым, который был приговорен в США к четырем годам тюрьмы и трехлетнему нахождению под наблюдением.

Фракеры

Фракеры – приверженцы электронного журнала Phrack, осуществляют взлом интрасети в познавательных целях для получения информации о топологии сетей, используемых в них программно-аппаратных средствах и информационных ресурсах, а также реализованных методах защиты. Эти сведения могут тем или иным способом (покупка, хищение и т.п.) попасть к заинтересованным в них

лицам, которые и осуществят НСД. На руку хулиганам играют сами же работники компаний. Так, директора компаний или же секретари из-за незнания правил безопасности могут предоставить вход в интрасеть компании фракеров. Фракеры действуют только в сетях, где доступ в Интернет осуществляется на основе телефонных линий.

Кракеры

Кракер – лицо, изучающее систему с целью ее взлома. Именно кракеры реализуют свои криминальные наклонности в похищении информации и написании вирусов, разрушающих ПО. Они применяют различные способы атак на компьютерную систему, используя принципы построения протоколов сетевого обмена. Кракеры разрабатывают специальное программное обеспечение, засылая его на взломанную машину. Основная задача кракера состоит в непосредственном осуществлении взлома системы с целью получения несанкционированного доступа к чужой информации – иначе говоря, для ее кражи, подмены или для объявления факта взлома. Кракер, по своей сути, ничем не отличается от обычного вора, взламывающего чужие квартиры и крадущего вещи. Он взламывает вычислительные системы и крадет чужую информацию.

Фишеры

Фишеры (от английского fisher – рыбак) – сравнительно недавно появившаяся разновидность Интернет-мошенников, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию: различные пароли, пин-коды, данные, используя фальшивые электронные адреса и поддельные веб-сайты и т.п.

Скамеры

Скамеры – это мошенники, рассылающие свои послания в надежде поймать на наживку наивных и жадных. Интернет-телефония становится все более популярной. На сегодня зарегистрировано уже довольно много случаев обращения мошенников к пользователям Skype-сервисом IP-телефонии, позволяющим пользователям связываться посредством компьютер-компьютер и компьютер-телефон.

Одним из первых схем обработки, использованной мошенниками в голосовом общении, – предложение клиенту выдать себя за наследника богатого клиента юридической компании, скончавшегося и не оставившего завещания. Сам мошенник при этом выступал в роли поверенного умершего богача и предлагал свои услуги человеку с якобы подходящими

для такой аферы именем и фамилией. Предполагалось, что это может позволить тому выдать себя за внезапно нашедшегося наследника, а вырученные таким образом деньги мошенник предлагал разделить пополам.

Естественно, от будущего наследничка требуется заполнить некоторое количество бумаг (для отвода глаз и дабы не возбуждать подозрений), а затем перевести деньги. После чего ни наследства, ни денег, ни мошенника клиент уже не увидит.

Спамеры

Спамеры – это те, от кого приходят в наши почтовые ящики не запрошенные массовые рассылки. Спамеры бывают разных категорий и весьма неоднородны. Рынок спамерских услуг – это действительно рынок, скорее даже индустрия. Индустрия эта довольно зрелая, поэтому она делится на разные слои. Можно выделить как минимум четыре-пять основных слоев:

Рассыльные службы. Это собственно и есть спамеры – те, кто рассылает спам. Это что-то вроде фирм или просто организованных групп весьма квалифицированных людей, часто с программистским прошлым (и настоящим). Эти фирмы имеют довольно совершенное программное обеспечение, которое умеет рассылать большие количества писем в единицу времени (до 100 писем в секунду, то есть 200 тысяч в час) и заметать следы. Они предлагают рассылку по миллионам адресов и берут за нее относительно небольшие деньги. Бизнес этот довольно выгодный – успешная российская спамерская контора может зарабатывать несколько десятков тысяч евро в месяц.

Собиратели баз данных. Этот вид игроков обслуживает нужды рассыльщиков и собирает для них почтовые адреса, которые объединяет в базы адресов. Они используют разнообразное программное обеспечение, которое умеет собирать адреса в Интернете, проверять их работоспособность, помещать в базу. При этом применяются разнообразные методы – от кражи адресов у провайдера до подбора адресов (с помощью различных эвристических алгоритмов и так называемых словарных атак).

Производители ПО. Это те, кто производит программное обеспечение для спамеров – софт для сбора адресов с сайтов и форумов (сетевые пауки), софт для массовой быстрой рассылки, софт для проверки существования и работоспособности адресов, и т.д.

Начинающие спамеры. Такой спамер пытается организовать свой бизнес рассылки, пользуясь техническими негодными средствами, – покупает карточку провайдера, рассылка идет через модем и т.п. Рас-

сылаемые таким способом письма составляют небольшую долю в общем количестве спамов – слишком много проблем (карточка быстро кончается, скорость рассылки очень низкая, база адресов устарела, провайдер может заметить и закрыть счет и т.д.). Такие спамеры обычно не очень хорошо заметают следы, от них в принципе можно ожидать рассылки письма с вирусом и т.п. Есть и другой вид спамера. Это чаще всего маркетинговые сотрудники обычных компаний, которые вдруг открыли для себя фантастические возможности рекламы электронной почты. Обычно адреса они берут просто с сайтов, честно указывают все свои координаты, обратный адрес, обычно настоящий, и т.д. Отрезвление происходит обычно быстро – провайдер замечает рассылку и отключает домен. Почта перестает ходить и приходится долго переписываться с провайдером, чтобы снова ее включить.

1.6. Причины уязвимости сети Интернет

Выделим причины уязвимости самой сети Интернета, что позволит понять уязвимость сетей и отдельных компьютеров, имеющих доступ к ней. Если рассматривать эти причины концептуально, не поясняя детально каждую из них в виду их тривиальности, то получим следующее:

1) дизайн Интернета, как открытой и децентрализованной сети с изначальным отсутствием политики безопасности: при разработке принципов функционирования Интернета основные усилия были направлены на достижение удобства обмена информацией, и многие сети спроектированы без механизмов контроля доступа со стороны Интернета;

2) уязвимость основных служб: базовым протоколом Интернета является набор протоколов TCP/IP, сервисные программы которого не гарантируют безопасности;

3) большая протяженность линий связи;

4) работа в Интернете основана на модели клиент/сервер, не лишенной определенных слабостей и конкретных лазеек в продуктах различных производителей; данная модель объединяет разнообразное программное и аппаратное обеспечение, которое может иметь «дыры» для проникновения злоумышленников или согласовываться в рамках одной сети, с точки зрения обеспечения информационной безопасности, не лучшим образом;

5) еще недостаточно организаций, занимающихся подготовкой профессионалов по защите в Интернете; хотя есть специальные фирмы, с исследованиями и рекомендациями которых можно прямо в Интернете ознакомиться, что делают, к сожалению, еще немногие;

6) внедрение различными компаниями собственного дизайна при создании Web-страниц (который может не соответствовать требованиям обеспечения определенного класса безопасности для Web-узла компании и скрывающейся далее, за ним сети) и распространение рекламной информации о своей продукции (реклама – хотя и наилучший двигатель торговли, но не гарантия приобретения самого защищенного продукта);

7) «утечка» технологий высокого уровня из секретных источников при вскрытии представленных в сети Web-узлов и сетей организаций, занимающихся разработкой этих технологий, и доступность информации о средствах защиты;

8) незашифрованность большей части передаваемой через Интернет информации, что дает возможность наблюдения за каналами передачи данных: электронная почта, пароли и передаваемые файлы могут быть легко перехвачены злоумышленником при помощи доступных программ;

9) работа в Интернете обслуживается большим числом сервисов, информационных служб и сетевых протоколов, знание правильности и тонкостей использования всех или хотя бы большинства сервисов, служб и протоколов одному человеку в лице администратора сети не реально;

10) сложность конфигурирования средств защиты – средства управления доступом зачастую сложны в настройке и контроле за ними, что влечет за собой неправильную конфигурацию таковых средств и приводит к несанкционированному доступу;

11) человеческий фактор в лице:

а) каждого отдельного пользователя, сидящего за компьютером и, возможно, не отличающегося высокими моральными принципами в смысле защиты интересов своей фирмы-работодателя и готового за соответствующую плату либо найти секретную информацию или предоставить доступ в сеть этой организации злоумышленникам, которые сами найдут в ней то, что их более всего интересует;

б) пользователей-«любителей», которые считают, что средства защиты им вообще не нужны, или неправильно сконфигурируют эти средства;

в) строго не определенного круга пользователей;

12) кажущаяся анонимность при работе в Интернете. Есть возможность обойти средства обнаружения отправителя той или иной информации или посетителя того или иного Web-узла с помощью использования виртуальных IP-адресов и промежуточных пересыльщиков – ремэйлеров – электронной почты. Специалисты компании InternetSecueitySystems считают, что в любой сети, основанной на протоколе TCP/IP, существует около 135 потенциальных каналов для НСД.

Контрольные вопросы

1. Особенности современных информационных технологий.
2. Когда появились первые преступления с использованием компьютерной техники в России?
3. Сколько уголовных дел по ст. 272 УК РФ («Неправомерный доступ к компьютерной информации») и ст.165 УК РФ («Причинение имущественного ущерба путем обмана и злоупотребления доверием») было возбуждено в 2003 году в России?
4. Какой ущерб нанесли компьютерные вирусы за последние 5 лет?
5. Что понимается под информационной безопасностью Российской Федерации?
6. Первая составляющая национальных интересов Российской Федерации в информационной сфере.
7. Вторая составляющая национальных интересов Российской Федерации в информационной сфере.
8. Третья составляющая национальных интересов Российской Федерации в информационной сфере.
9. Четвертая составляющая национальных интересов Российской Федерации в информационной сфере.
10. Классификация компьютерных преступлений.
11. Экономические компьютерные преступления.
12. Компьютерными преступлениями против личных прав и частной сферы.
13. Компьютерные преступления против государственных и общественных интересов.
14. Основные виды преступлений, связанных с вмешательством в работу компьютеров.
15. Способы совершения компьютерных преступлений.
16. Методы перехвата компьютерной информации.

17. Пользователи и злоумышленники в Интернете.
18. Кто такие хакеры?
19. Кто такие фракеры?
20. Кто такие кракеры?
21. Кто такие фишеры?
22. Кто такие скамеры?
23. Кто такие спамеры?
24. Причины уязвимости сети Интернет.
25. Защищаемая информация.
26. Защита информации.
27. Защита информации от утечки.
28. Защита информации от несанкционированного воздействия.
29. Защита информации от непреднамеренного воздействия.
30. Защита информации от разглашения.
31. Защита информации от несанкционированного доступа.
32. Защита информации от иностранной разведки.
33. Защита информации от иностранной технической разведки.
34. Защита информации от агентурной разведки.
35. Цель защиты информации.
36. Эффективность защиты информации.
37. Показатель эффективности защиты информации.
38. Нормы эффективности защиты информации.
39. Организация защиты информации.
40. Система защиты информации.
41. Мероприятие по защите информации.
42. Мероприятие по контролю эффективности защиты информации.
43. Техника защиты информации.
44. Объект защиты.
45. Способ защиты информации.
46. Категорирование защищаемой информации.
47. Метод контроля эффективности защиты информации это?
48. Контроль состояния защиты информации.
49. Средство защиты информации.
50. Средство контроля эффективности защиты информации.
51. Контроль организации защиты информации.
52. Контроль эффективности защиты информации.
53. Организационный контроль эффективности защиты информации.
54. Технический контроль эффективности защиты информации.
55. Информация.
56. Доступ к информации.

57. Субъект доступа к информации.
58. Носитель информации.
59. Собственник информации.
60. Владелец информации.
61. Пользователь (потребитель) информации.
62. Право доступа к информации.
63. Правило доступа к информации.
64. Орган защиты информации.
65. Информационные процессы.
66. Информационная система.
67. Информационные ресурсами.
68. Что понимают под утечкой информации.
69. Несанкционированный доступ.
70. Несанкционированное воздействие.
71. Что понимается под непреднамеренным воздействием на защищенную информацию.
72. Что понимается под эффективностью защиты информации.
73. Конфиденциальность информации.
74. Шифрование информации.
75. Уязвимость информации.

Тесты

1. В каком году в России появились первые преступления с использованием компьютерной техники (были похищены 125,5 тыс. долл. США во Внешэкономбанке)?

1. 1988;
2. 1991;
3. 1994;
4. 1997;
5. 2002.

2. Сколько уголовных дела по ст. ст. 272 и 165 УК РФ было возбуждено в 2003 г. в России?

1. 6;
2. 60;
3. 160;
4. 600;
5. 1600.

3. Какой общий ущерб по данным Института компьютерной безопасности, нанесли компьютерные вирусы за последние 5 лет (млрд долл. США)?

1. 4;
2. 34;
3. 54;
4. 74;
5. 94.

4. По данным журнала «Security Magazine», средний размер ущерба от компьютерного мошенничества составляет (долл. США):

1. 500 000;
2. 1 000 000;
3. 1 500 000;
4. 2 000 000;
5. 2 500 000.

5. По данным Главного информационного центра МВД России, количество компьютерных преступлений ежегодно увеличивается в (раза):

1. 2;
2. 2,5;
3. 3;
4. 3,5;
5. 4.

6. По данным Главного информационного центра МВД России, ежегодный размер материального ущерба от компьютерных преступлений составляет около (млн руб.):

1. 6;
2. 60;
3. 160;
4. 600;
5. 1600.

7. По данным Главного информационного центра МВД России, средний ущерб, причиняемый потерпевшему от 1 компьютерного преступления, равен (млн руб.):

1. 7;
2. 1,7;
3. 2,7;
4. 3,7;
5. 4,7.

8. Сколько процентов электронных писем являются спамом?

1. 10;
2. 30;
3. 50;
4. 70;
5. 90.

9. К каким ежегодным убыткам приводят спамы (млрд долл. США)?

1. 20;
2. 40;
3. 60;
4. 80;
5. 100.

10. В 2003 г. ФСБ пресечено попыток проникновения в информационные ресурсы органов государственной власти России около (раз):

1. 10;
2. 100;
3. 1 000;
4. 10 000;
5. 100 000.

11. Сколько выделяются основных составляющих национальных интересов Российской Федерации в информационной сфере?

1. 2;
2. 3;
3. 4;
4. 5;
5. 6.

12. Активный перехват информации это – перехват, который:

1. заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
2. основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
3. неправомерно использует технологические отходы информационного процесса;
4. осуществляется путем использования оптической техники;
5. осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

13. Пассивный перехват информации это – перехват, который:

1. заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
2. основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
3. неправомерно использует технологические отходы информационного процесса;
4. осуществляется путем использования оптической техники;
5. осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

14. Аудиоперехват перехват информации это – перехват, который:

1. заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
2. основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
3. неправомерно использует технологические отходы информационного процесса;
4. осуществляется путем использования оптической техники;
5. осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

15. Просмотр мусора это – перехват информации, который:

1. заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
2. основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
3. неправомерно использует технологические отходы информационного процесса;
4. осуществляется путем использования оптической техники;
5. осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

16. Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации, называется:

1. активный перехват;
2. пассивный перехват;

3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.

17. Перехват, который осуществляется путем использования оптической техники, называется:

1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.

18. Перехват, который основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций, называется:

1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.

19. Перехват, который осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера, называется:

1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.

20. Перехват, который неправомерно использует технологические отходы информационного процесса, называется:

1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.

21. Как называется способ несанкционированного доступа к информации, который заключается в несанкционированном доступе в компьютер или компьютерную сеть без права на то?

1. «За дураком»;
2. «Брешь»;

3. «Компьютерный абордаж»;
4. «За хвост»;
5. «Неспешный выбор».

22. Как называется способ несанкционированного доступа к информации, который заключается в подключении компьютерного терминала к каналу связи в тот момент времени, когда сотрудник кратковременно покидает свое рабочее место, оставляя терминал в рабочем режиме?

1. «За дураком»;
2. «Брешь»;
3. «Компьютерный абордаж»;
4. «За хвост»;
5. «Неспешный выбор».

23. Как называется способ несанкционированного доступа к информации, который заключается в подключении злоумышленника к линии связи законного пользователя и после сигнала, обозначающего конец работы, перехватывания его на себя, получая доступ к системе?

1. «За дураком»;
2. «Брешь»;
3. «Компьютерный абордаж»;
4. «За хвост»;
5. «Неспешный выбор».

24. Как называется способ несанкционированного доступа к информации, который заключается в отыскании участков программ, имеющих ошибку или неудачную логику построения?

1. «За дураком»;
2. «Брешь»;
3. «Компьютерный абордаж»;
4. «За хвост»;
5. «Неспешный выбор».

25. Как называется способ несанкционированного доступа к информации, который заключается в нахождении злоумышленником уязвимых мест в ее защите?

1. «За дураком»;
2. «Брешь»;
3. «Компьютерный абордаж»;
4. «За хвост»;
5. «Неспешный выбор».

26. Способ несанкционированного доступа к информации «За дураком» заключается:

1. в отыскании участков программ, имеющих ошибку или неудачную логику построения;
2. в подключении злоумышленника к линии связи законного пользователя и после сигнала, обозначающего конец работы, перехватывания его на себя, получая доступ к системе;
3. в подключении компьютерного терминала к каналу связи в тот момент времени, когда сотрудник, кратковременно покидает свое рабочее место, оставляя терминал в рабочем режиме;
4. в нахождении злоумышленником уязвимых мест в ее защите;
5. в несанкционированном доступе в компьютер или компьютерную сеть без права на то.

27. Способ несанкционированного доступа к информации «Брешь» заключается:

1. в отыскании участков программ, имеющих ошибку или неудачную логику построения;
2. в подключении злоумышленника к линии связи законного пользователя и после сигнала, обозначающего конец работы, перехватывания его на себя, получая доступ к системе;
3. в подключении компьютерного терминала к каналу связи в тот момент времени, когда сотрудник, кратковременно покидает свое рабочее место, оставляя терминал в рабочем режиме;
4. в нахождении злоумышленником уязвимых мест в ее защите;
5. в несанкционированном доступе в компьютер или компьютерную сеть без права на то.

28. Способ несанкционированного доступа к информации «Компьютерный абордаж» заключается:

1. в отыскании участков программ, имеющих ошибку или неудачную логику построения;
2. в подключении злоумышленника к линии связи законного пользователя и после сигнала, обозначающего конец работы, перехватывания его на себя, получая доступ к системе;
3. в подключении компьютерного терминала к каналу связи в тот момент времени, когда сотрудник кратковременно покидает свое рабочее место, оставляя терминал в рабочем режиме;
4. в нахождении злоумышленником уязвимых мест в ее защите;
5. в несанкционированном доступе в компьютер или компьютерную сеть без права на то.

29. Способ несанкционированного доступа к информации «За хвост» заключается:

1. в отыскании участков программ, имеющих ошибку или неудачную логику построения;
2. в подключении злоумышленника к линии связи законного пользователя и после сигнала, обозначающего конец работы, перехватывания его на себя, получая доступ к системе;
3. в подключении компьютерного терминала к каналу связи в тот момент времени, когда сотрудник кратковременно покидает свое рабочее место, оставляя терминал в рабочем режиме;
4. в нахождении злоумышленником уязвимых мест в ее защите;
5. в несанкционированном доступе в компьютер или компьютерную сеть без права на то.

30. Способ несанкционированного доступа к информации «Неспешный выбор» заключается:

1. в отыскании участков программ, имеющих ошибку или неудачную логику построения;
2. в подключении злоумышленника к линии связи законного пользователя и после сигнала, обозначающего конец работы, перехватывания его на себя, получая доступ к системе;
3. в подключении компьютерного терминала к каналу связи в тот момент времени, когда сотрудник, кратковременно покидает свое рабочее место, оставляя терминал в рабочем режиме;
4. в нахождении злоумышленником уязвимых мест в ее защите;
5. в несанкционированном доступе в компьютер или компьютерную сеть без права на то.

31. Хакер – это:

1. лицо, которое взламывает интрасеть в познавательных целях;
2. мошенник, рассылающий свои послания в надежде обмануть наивных и жадных;
3. лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов разрушающих ПО;
4. плохой игрок в гольф, дилетант;
5. мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию.

32. Фракер – это:

1. лицо, которое взламывает интрасеть в познавательных целях;
2. мошенник, рассылающий свои послания в надежде обмануть наивных и жадных;

3. лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов, разрушающих ПО;
4. плохой игрок в гольф, дилетант;
5. мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию.

33. Кракер – это:
1. лицо, которое взламывает интрасеть в познавательных целях;
2. мошенник, рассылающий свои послания в надежде обмануть наивных и жадных;
3. лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов, разрушающих ПО;
4. плохой игрок в гольф, дилетант;
5. мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию.

34. Фишер – это:
1. лицо, которое взламывает интрасеть в познавательных целях;
2. мошенник, рассылающий свои послания в надежде обмануть наивных и жадных;
3. лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов, разрушающих ПО;
4. плохой игрок в гольф, дилетант;
5. мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию.

35. Скамер – это:
1. лицо, которое взламывает интрасеть в познавательных целях;
2. мошенник, рассылающий свои послания в надежде обмануть наивных и жадных;
3. лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов, разрушающих ПО;
4. плохой игрок в гольф, дилетант;
5. Это мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию.

36. Спамер – это:

1. лицо, которое взламывает интрасеть в познавательных целях;
2. мошенник, рассылающий свои послания в надежде обмануть наивных и жадных;
3. лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов, разрушающих ПО;
4. тот, от кого приходят в наши почтовые ящики не запрошенные рассылки;
5. мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию.

37. Лицо, которое взламывает интрасеть в познавательных целях, – это:

1. скамер;
2. хакер;
3. фишер;
4. фракер;
5. кракер.

38. Мошенник, рассылающий свои послания в надежде обмануть наивных и жадных, – это:

1. скамер;
2. хакер;
3. фишер;
4. фракер;
5. кракер.

39. Лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов, разрушающих ПО, – это:

1. скамер;
2. хакер;
3. фишер;
4. фракер;
5. кракер.

40. Плохих игроков в гольф, дилетантов называли в XIX веке:

1. скамер;
2. хакер;
3. фишер;
4. фракер;
5. кракер.

41. Мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию, – это:

1. скамер;
2. хакер;
3. фишер;
4. фракер;
5. кракер.

42. Лицо, от которого в наши почтовые ящики приходят не запрошенные рассылки, – это:

1. скамер;
2. хакер;
3. спамер;
4. фракер;
5. кракер.

43. Защита информации – это:

1. процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
2. преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
3. получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
4. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
5. деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на нее.

44. Информационные процессы – это:

1. процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
2. преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
3. получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
4. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
5. деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на нее.

45. Шифрование информации – это:

1. процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
2. преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
3. получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
4. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
5. деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на нее.

46. Доступ к информации – это:

1. процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
2. преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
3. получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
4. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
5. деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на нее.

47. Защита информации от утечки – это деятельность по предотвращению:

1. получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;
2. воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;
3. воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
4. неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;

5. несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

48. Защита информации от несанкционированного воздействия – это деятельность по предотвращению:

1. получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;
2. воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;
3. воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
4. неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;
5. несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

49. Защита информации от непреднамеренного воздействия – это деятельность по предотвращению:

1. получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;
2. воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;
3. воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
4. неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;
5. несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

50. Защита информации от разглашения – это деятельность по предотвращению:

1. получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;
2. воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;
3. воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
4. неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;
5. несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

51. Защита информации от несанкционированного доступа – это деятельность по предотвращению:

1. получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;
2. воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;
3. воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
4. неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;
5. несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

52. Субъект доступа к информации – это:

1. физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов;

2. субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации;
3. субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника, в соответствии с установленными правами и правилами доступа к информации либо с их нарушением;
4. субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами;
5. участник правоотношений в информационных процессах.

53. Носитель информации – это:

1. физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов;
2. субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации;
3. субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника, в соответствии с установленными правами и правилами доступа к информации либо с их нарушением;
4. субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами;
5. участник правоотношений в информационных процессах.

54. Собственник информации – это:

1. физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов;
2. субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации;
3. субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника, в соответствии с установленными правами и правилами доступа к информации либо с их нарушением;

4. субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами;
5. участник правоотношений в информационных процессах.

55. Владелец информации – это:
1. физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов;
2. субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации;
3. субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника, в соответствии с установленными правами и правилами доступа к информации либо с их нарушением;
4. субъект, в полном объеме реализующий полномочия, пользования, распоряжения информацией в соответствии с законодательными актами;
5. участник правоотношений в информационных процессах.

56. Пользователь (потребитель) информации – это:
1. физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов;
2. субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации;
3. субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника, в соответствии с установленными правами и правилами доступа к информации либо с их нарушением;
4. субъект, в полном объеме реализующий полномочия, пользования, распоряжения информацией в соответствии с законодательными актами;
5. участник правоотношений в информационных процессах.

Тема 2.

Угрозы информации

Изучив тему 2, студент должен:
знать:

- закономерности возникновения угроз информационной безопасности;
- классификацию угроз информационной безопасности;
- пути и каналы утечки информации;
- виды удаленных атак на интрасеть;
- классические и современные методы взлома интрасетей.

акцентировать внимание на понятиях:

- угроза информационной безопасности, утечка информации, нарушение целостности информации, модификация информации, искажение информации, подделка информации, уничтожение информации, блокирование информации, побочное электромагнитное излучение, электромагнитная наводка, специальное электронное закладное устройство, внешнее воздействие на информационный ресурс.

Содержание темы (дидактические единицы и их характеристика):

Для успешной защиты имеющейся информации необходимо знать, каким угрозам она подвергается на всех этапах эксплуатации, а также какими путями злоумышленник проникает и взламывает компьютерную систему.

Цели и задачи изучения темы: Получение знаний о видах угроз, путях и каналах утечки информации, от кого они исходят и к чему приводят. Изучение видов атак и методов взлома интрасетей злоумышленниками.

Порядок изучения темы

Распределение бюджета времени по теме:

- количество часов, отведенных на практические занятия, из них в компьютерной аудитории – 4/4;
- количество часов, отведенных на самостоятельную работу, – 16.

Виды самостоятельной работы студентов:

- изучение учебного пособия «Информационная безопасность»;
- подготовка к участию в форуме по теме «Виды атак и методы взлома интрасетей»;
- изучение дополнительной литературы;
- выполнение тестовых заданий по теме.

Методические указания по изучению вопросов темы

При изучении учебных вопросов:

- изучить тему 2 по учебному пособию «Информационная безопасность»;
- принять участие в форуме по теме «Угрозы информации»;
- изучить дополнительные материалы

При изучении темы необходимо:

- *читать литературу*:

1. Информационная безопасность: Уч. Пособие. – М.: МЭСИ, 2007.
2. Герасименко В.А., Малюк А.А. Основы защиты информации, – М.: ППО «Известия», 1997. Гл. 1,2.
3. Мельников В.И. Защита информации в компьютерных системах. – М.: Финансы и статистика, 1997. – Разд. 1.
4. Милославская Н.Г., Толстой А.И. Интрасети: доступ в Internet, защита. – М.: ООО «ЮНИТИ-ДАНА», 2000., Гл. 1.
5. Проскурин В.Г., Крутов С.В. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах. – М.: Радио и связь, 2000.
6. Белкин П.Ю. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных. – М.: Радио и связь, 1999.

Вопросы темы

2.1. Виды угроз информационной безопасности РФ.
2.2. Источники угроз информационной безопасности РФ.
2.3. Угрозы информационной безопасности для АСОИ.
2.4. Удаленные атаки на интрасети.

2.1. Виды угроз информационной безопасности Российской Федерации

По своей общей направленности угрозы информационной безопасности Российской Федерации подразделяются на следующие виды:

1. Угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России. К ним относятся:

- принятие органами государственной власти правовых актов, ущемляющих конституционные права и свободы граждан в области духовной жизни и информационной деятельности;
- создание монополий на формирование, получение и распространение информации;
- противодействие, в том числе со стороны криминальных структур, реализации гражданами своих конституционных прав на личную и семейную тайну, тайну переписки, телефонных переговоров и иных сообщений;
- ограничение доступа к общественно необходимой информации;
- противоправное применение специальных средств воздействия на индивидуальное, групповое и общественное сознание;
- неисполнение органами государственной власти, организациями и гражданами требований законодательства, регулирующего отношения в информационной сфере;
- неправомерное ограничение доступа граждан к открытым информационным ресурсам органов государственной власти, архивным материалам и к другой открытой информации;
- дезорганизация и разрушение системы накопления и сохранения культурных ценностей, включая архивы;
- нарушение конституционных прав и свобод человека и гражданина в области массовой информации;
- вытеснение российских информационных агентств, средств массовой информации с внутреннего информационного рынка и усиление зависимости духовной, экономической и политической сфер общественной жизни России от зарубежных информационных структур;
- девальвация духовных ценностей, пропаганда образцов массовой культуры, основанных на культе насилия, на духовных и

нравственных ценностях, противоречащих ценностям, принятым в российском обществе;

- снижение духовного, нравственного и творческого потенциала населения России;
- манипулирование информацией (дезинформация, сокрытие или искажение информации).

2. Угрозы информационному обеспечению государственной политики Российской Федерации. К ним относятся:

- монополизация информационного рынка России, его отдельных секторов отечественными и зарубежными информационными структурами;
- блокирование деятельности государственных средств массовой информации по информированию российской и зарубежной аудитории;
- низкая эффективность информационного обеспечения государственной политики Российской Федерации вследствие дефицита квалифицированных кадров, отсутствия системы формирования и реализации государственной информационной политики.

3. Угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов. К ним относятся:

- противодействие доступу Российской Федерации к новейшим информационным технологиям, взаимовыгодному и равноправному участию российских производителей в мировом разделении труда в индустрии информационных услуг, средств информатизации, телекоммуникации и связи, информационных продуктов, а также создание условий для усиления технологической зависимости России в области современных информационных технологий;
- закупка органами государственной власти импортных средств информатизации, телекоммуникации и связи при наличии отечественных аналогов, не уступающих по своим характеристикам зарубежным образцам;
- вытеснение с отечественного рынка российских производителей средств информатизации, телекоммуникации и связи;
- увеличение оттока за рубеж специалистов и правообладателей интеллектуальной собственности.

4. Угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России. К ним относятся:

- противоправные сбор и использование информации;
- нарушения технологии обработки информации;
- внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;
- разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;
- уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;
- воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации;
- компрометация ключей и средств криптографической защиты информации;
- утечка информации по техническим каналам;
- внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти, предприятий, учреждений и организаций независимо от формы собственности;
- уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;
- перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации;
- использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии российской информационной инфраструктуры;
- несанкционированный доступ к информации, находящейся в банках и базах данных;
- нарушение законных ограничений на распространение информации.

2.2. Источники угроз информационной безопасности Российской Федерации

Источники угроз информационной безопасности Российской Федерации подразделяются на внешние и внутренние.

К внешним источникам относятся:

- деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов Российской Федерации в информационной сфере;
- стремление ряда стран к доминированию и ущемлению интересов России в мировом информационном пространстве, вытеснению ее с внешнего и внутреннего информационных рынков;
- обострение международной конкуренции за обладание информационными технологиями и ресурсами;
- деятельность международных террористических организаций;
- увеличение технологического отрыва ведущих держав мира и наращивание их возможностей по противодействию созданию конкурентоспособных российских информационных технологий;
- деятельность космических, воздушных, морских и наземных технических и иных средств (видов) разведки иностранных государств;
- разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним.

К внутренним источникам относятся:

- критическое состояние отечественных отраслей промышленности;
- неблагоприятная криминогенная обстановка, сопровождающаяся тенденциями сращивания государственных и криминальных структур в информационной сфере, получения криминальными структурами доступа к конфиденциальной информации, усиления влияния организованной преступности на жизнь общества, снижения степени защищенности законных интересов граждан, общества и государства в информационной сфере;

- недостаточная координация деятельности органов государственной власти по формированию и реализации единой государственной политики в области обеспечения информационной безопасности Российской Федерации;
- недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика;
- неразвитость институтов гражданского общества и недостаточный государственный контроль за развитием информационного рынка России;
- недостаточное финансирование мероприятий по обеспечению информационной безопасности Российской Федерации;
- недостаточная экономическая мощь государства;
- снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности;
- недостаточная активность органов государственной власти в информировании общества о своей деятельности, в разъяснении принимаемых решений, в формировании открытых государственных ресурсов и развитии системы доступа к ним граждан;
- отставание России от ведущих стран мира по уровню информатизации органов государственной власти в кредитно-финансовой сфере, промышленности, сельском хозяйстве, образовании, здравоохранении, сфере услуг и быта граждан.

2.3. Угрозы информационной безопасности для автоматизированных систем обработки информации (АСОИ)

Как показывает анализ, большинство современных автоматизированных систем обработки информации в общем случае представляет собой территориально распределенные системы интенсивно взаимодействующих (синхронизирующихся) между собой по данным (ресурсам) и управлению (событиям) локальных вычислительных сетей (ЛВС) и отдельных ЭВМ.

Перечислим особенности распределенных АСОИ:

- территориальная разнесенность компонентов системы и наличие интенсивного обмена информацией между ними;

- широкий спектр используемых способов представления, хранения и передачи информации;
- интеграция данных различного назначения, принадлежащих различным субъектам, в рамках единых баз данных и, наоборот, размещение необходимых некоторым субъектам данных в различных удаленных узлах сети;
- абстрагирование владельцев данных от физических структур и места размещения данных;
- использование режимов распределенной обработки данных;
- участие в процессе автоматизированной обработки информации большого количества пользователей и персонала различных категорий;
- непосредственный и одновременный доступ к ресурсам (в том числе и информационным) большого числа пользователей (субъектов) различных категорий;
- высокая степень разнородности используемых средств вычислительной техники и связи, а также их программного обеспечения;
- отсутствие специальной аппаратной поддержки средств защиты в большинстве типов технических средств, широко используемых в АСОИ.

Уязвимость основных структурно-функциональных элементов распределенных АСОИ

В общем случае АСОИ состоят из следующих основных структурно-функциональных элементов:

- рабочих станций – отдельных ЭВМ или удаленных терминалов сети, на которых реализуются автоматизированные рабочие места пользователей (абонентов, операторов);
- серверов или Host машин (служб файлов, печати, баз данных и т.п.), не выделенных (или выделенных, то есть не совмещенных с рабочими станциями) высокопроизводительных ЭВМ, предназначенных для реализации функций хранения, печати данных, обслуживания рабочих станций сети и т.п. действий;
- межсетевых мостов – элементов, обеспечивающих соединение нескольких сетей передачи данных, либо нескольких сегментов одной и той же сети, имеющих различные протоколы взаимодействия (шлюзов, центров коммутации пакетов, коммуникационных ЭВМ);
- каналов связи (локальных, телефонных, с узлами коммутации и т.д.).

Рабочие станции являются наиболее доступными компонентами сетей и именно с них могут быть предприняты наиболее многочисленные попытки совершения несанкционированных действий. С рабочих станций осуществляются управление процессами обработки информации, запуск программ, ввод и корректировка данных, на дисках рабочих станций могут размещаться важные данные и программы обработки. На видеомониторы и печатающие устройства рабочих станций выводится информация при работе пользователей (операторов), выполняющих различные функции и имеющих разные полномочия по доступу к данным и другим ресурсам системы. Именно поэтому рабочие станции должны быть надежно защищены от доступа посторонних лиц и содержать средства разграничения доступа к ресурсам со стороны законных пользователей, имеющих разные полномочия. Кроме того, средства защиты должны предотвращать нарушения нормальной настройки рабочих станций и режимов их функционирования, вызванные неумышленным вмешательством неопытных (невнимательных) пользователей.

В особой защите нуждаются такие привлекательные для злоумышленников элементы сетей, как серверы (Host-машины) и мосты. Первые – как концентраторы больших объемов информации, вторые – как элементы, в которых осуществляется преобразование (возможно через открытую, нешифрованную форму представления) данных при согласовании протоколов обмена в различных участках сети.

Благоприятным для повышения безопасности серверов и мостов обстоятельством является, как правило, наличие возможностей по их надежной защите физическими средствами и организационными мерами в силу их выделенности, позволяющей сократить до минимума число лиц из персонала сети, имеющих непосредственный доступ к ним. Иными словами, непосредственные случайные воздействия персонала и преднамеренные воздействия злоумышленников на выделенные серверы и мосты можно считать маловероятными. В то же время надо ожидать массированной атаки на серверы и мосты с использованием средств удаленного доступа. Здесь злоумышленники, прежде всего, могут искать возможности повлиять на работу различных подсистем серверов и мостов, используя недостатки протоколов обмена и средств разграничения удаленного доступа к ресурсам и системным таблицам. Использоваться могут все возможности и средства, от стандартных (без модификации компонентов) до подключения специальных аппаратных средств (кана-

лы, как правило, слабо защищены от подключения) и применения высококлассных программ для преодоления системы защиты.

Конечно, сказанное выше не означает, что не будет попыток внедрения аппаратных и программных закладок в сами мосты и серверы, открывающих дополнительные широкие возможности по несанкционированному удаленному доступу. Закладки могут быть внедрены как с удаленных станций (посредством вирусов или иным способом), так и непосредственно в аппаратуру и программы серверов при их ремонте, обслуживании, модернизации, переходе на новые версии программного обеспечения, смене оборудования.

Каналы и средства связи также нуждаются в защите. В силу большой пространственной протяженности линий связи (через неконтролируемую или слабо контролируемую территорию) практически всегда существует возможность подключения к ним, либо вмешательства в процесс передачи данных. Возможные при этом угрозы подробно изложены ниже.

Основные виды угроз безопасности субъектов информационных отношений

Основными видами угроз безопасности АСОИ (угроз интересам субъектов информационных отношений) являются:

- стихийные бедствия и аварии (наводнение, ураган, землетрясение, пожар и т.п.);
- сбои и отказы оборудования (технических средств) АСОИ;
- последствия ошибок проектирования и разработки компонентов АСОИ (аппаратных средств, технологии обработки информации, программ, структур данных и т.п.);
- ошибки эксплуатации (пользователей, операторов и другого персонала);
- преднамеренные действия нарушителей и злоумышленников (обиженных лиц из числа персонала, преступников, шпионов, диверсантов и т.п.).

Классификация угроз безопасности информации

Все множество потенциальных угроз информации по природе их возникновения разделяется на два класса: естественные (объективные) и искусственные (субъективные) (рис. 2.1).

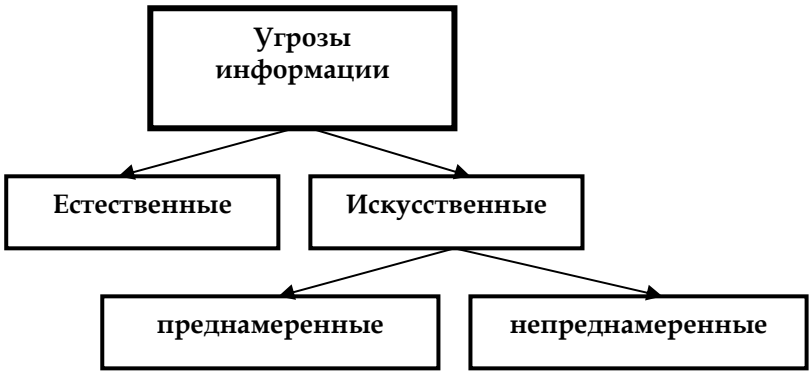


Рис. 2.1. **Угрозы информации**

Естественные угрозы – это угрозы, вызванные воздействиями на АСОИ и ее элементы объективных физических процессов или стихийных природных явлений, не зависящих от человека.

Искусственные угрозы – это угрозы АСОИ, вызванные деятельностью человека. Среди них, исходя из мотивации действий, можно выделить непреднамеренные и преднамеренные.

Непреднамеренные угрозы (неумышленные, случайные) – вызванные ошибками при:

- проектировании АСОИ и ее элементов;
- разработке программного обеспечения;
- действиях персонала;

Преднамеренные (умышленные) угрозы, связанные с корыстными устремлениями людей (злоумышленников).

Источники угроз по отношению к АСОИ могут быть внешними или внутренними (компоненты самой АСОИ – ее аппаратура, программы, персонал).

Основные непреднамеренные искусственные угрозы

Основные непреднамеренные искусственные угрозы АСОИ (действия, совершаемые людьми случайно, по незнанию, невнимательности или халатности без злого умысла):

- неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программ-

ных, информационных ресурсов системы (неумышленная порча оборудования, удаление, искажение файлов с важной информацией или программ, в том числе системных и т.п.);

- неправомерное отключение оборудования или изменение режимов работы устройств и программ;
- неумышленная порча носителей информации;
- запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или осуществляющих необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т.п.);
- нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения сотрудником своих служебных обязанностей), с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);
- заражение компьютера вирусами;
- неосторожные действия, приводящие к разглашению конфиденциальной информации или делающие ее общедоступной;
- разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);
- проектирование архитектуры системы, технологии обработки данных, разработка прикладных программ, с возможностями, представляющими опасность для работоспособности системы и безопасности информации;
- игнорирование организационных ограничений (установленных правил) при работе в системе;
- вход в систему в обход средств защиты (загрузка посторонней операционной системы со сменных магнитных носителей и т.п.);
- некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности;
- пересылка данных по ошибочному адресу абонента (устройства);
- ввод ошибочных данных;
- неумышленное повреждение каналов связи.

Основные преднамеренные искусственные угрозы

Основные возможные пути умышленной дезорганизации работы АСОИ, проникновения в систему и несанкционированного доступа к информации:

- физическое разрушение системы (путем взрыва, поджога и т.п.) или вывод из строя всех или отдельных наиболее важных компонентов компьютерной системы (устройств, носителей важной системной информации, лиц из числа персонала и т.п.);
- отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т.п.);
- действия по дезорганизации функционирования системы (изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.);
- внедрение агентов в число персонала системы (в том числе в административную группу, отвечающую за безопасность);
- вербовка (путем подкупа, шантажа и т.п.) персонала или отдельных пользователей, имеющих необходимые полномочия;
- применение подслушивающих устройств, дистанционная фото- и видеосъемка и т.п.;
- перехват побочных электромагнитных, акустических и других излучений устройств и линий связи, а также наводок активных излучений на вспомогательные технические средства, непосредственно не участвующие в обработке информации (телефонные линии, сети питания, отопления и т.п.);
- перехват данных, передаваемых по каналам связи, и их анализ с целью выяснения протоколов обмена, правил вхождения в связь и авторизации пользователя и последующих попыток их имитации для проникновения в систему;
- хищение носителей информации (различных съемных носителей, микросхем памяти, запоминающих устройств и компьютеров в целом);
- несанкционированное копирование носителей информации;
- хищение производственных отходов (распечаток, записей, списанных носителей информации и т.п.);
- чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
- незаконное получение паролей и других реквизитов разграничения доступа (агентурным путем, используя халатность пользо-

вателей, путем подбора, путем имитации интерфейса системы и т.д.) с последующей маскировкой под зарегистрированного пользователя («маскарад»);

- несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики, такие как номер рабочей станции в сети, физический адрес, адрес в системе связи, аппаратный блок кодирования и т.п.;
- вскрытие шифров криптозащиты информации;
- внедрение аппаратных спецвложений, программных «закладок» и «вирусов» («троянский конь» и «жучки»), то есть таких участков программ, которые не нужны для осуществления заявленных функций, но позволяют преодолевать систему защиты, скрытно и незаконно осуществлять доступ к системным ресурсам с целью регистрации и передачи критической информации или дезорганизации функционирования системы;
- незаконное подключение к линиям связи с целью работы «между строк», с использованием пауз в действиях законного пользователя от его имени с последующим вводом ложных сообщений или модификацией передаваемых сообщений;
- незаконное подключение к линиям связи с целью прямой подмены законного пользователя путем его физического отключения после входа в систему и успешной аутентификации с последующим вводом дезинформации и навязыванием ложных сообщений.

Чаще всего для достижения поставленной цели злоумышленник использует не один, а совокупность перечисленных выше путей.

Классификация каналов проникновения в систему и утечки информации

Все каналы проникновения в систему и утечки информации разделяют на прямые и косвенные.

Под ***косвенными*** понимают такие каналы, использование которых не требует проникновения в помещения, где расположены компоненты системы.

Для использования ***прямых*** каналов такое проникновение необходимо. Прямые каналы могут использоваться без внесения изменений в компоненты системы или с изменениями компонентов.

По типу основного средства, используемого для реализации угрозы, все возможные каналы можно условно разделить на три группы, где таковыми средствами являются: человек, программа или аппаратура.

Классификация видов нарушений работоспособности систем и несанкционированного доступа к информации по объектам воздействия и способам нанесения ущерба безопасности приведена в табл. 2.

Таблица 2.1

Виды нарушений работоспособности систем и несанкционированного доступа к информации

Способы нанесения ущерба	**Объекты воздействий**			
	Оборудование	**Программы**	**Данные**	**Персонал**
Раскрытие (утечка) информации	Хищение носителей информации, подключение к линии связи, несанкционированное использование ресурсов	Несанкционированное копирование перехват	Хищение, копирование, перехват	Передача сведений о защите, разглашение, халатность
Потеря целостности информации	Подключение, модификация, спец.вложения, изменение режимов работы, несанкционированное использование ресурсов	Внедрение «троянских коней» и «жучков»	Искажение, модификация	Вербовка персонала, «маскарад»
Нарушение работоспособности автоматизированной системы	Изменение режимов функционирования, вывод из строя, хищение, разрушение	Искажение, удаление, подмена	Искажение, удаление, навязывание ложных данных	Уход, физическое устранение
Незаконное тиражирование (воспроизведение) информации	Изготовление аналогов без лицензий	Использование незаконных копий	Публикация без ведома авторов	

По способу получения информации потенциальные каналы доступа можно разделить на:

- физический;
- электромагнитный (перехват излучений);
- информационный (программно-математический).

При контактном НСД (физическом, программно-математическом) возможные угрозы информации реализуются путем доступа к элементам АСОИ, к носителям информации, к самой вводимой и выводимой информации (и результатам), к программному обеспечению (в том числе к операционным системам), а также путем подключения к линиям связи.

При бесконтактном доступе (например, по электромагнитному каналу) возможные угрозы информации реализуются перехватом излучений аппаратуры АС, в том числе наводимых в токопроводящих коммуникациях и цепях питания, перехватом информации в линиях связи, вводом в линии связи ложной информации, визуальным наблюдением (фотографированием) устройств отображения информации, прослушиванием переговоров персонала АСОИ и пользователей.

Преступления, в том числе и компьютерные, совершаются людьми. Пользователи системы и ее персонал, с одной стороны, являются составной частью, необходимым элементом АСОИ. С другой стороны, они же являются основной причиной и движущей силой нарушений и преступлений.

Неформальная модель нарушителя в АСОИ

Нарушитель – это лицо, предпринявшее попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства.

Злоумышленником будем называть нарушителя, намеренно идущего на нарушение из корыстных побуждений.

Неформальная модель нарушителя отражает его практические и теоретические возможности, априорные знания, время и место действия и т.п. Для достижения своих целей нарушитель должен приложить некоторые усилия, затратить определенные ресурсы.

При разработке модели нарушителя определяются предположения:

- о категориях лиц, к которым может принадлежать нарушитель;
- о мотивах действий нарушителя (цели);
- о квалификации нарушителя и его технической оснащенности;
- о характере возможных действий нарушителей.

По отношению к АСОИ нарушители могут быть внутренними (из числа персонала системы) или внешними (посторонними лицами).

Внутренним нарушителем может быть лицо из следующих категорий персонала:

- пользователи (операторы) системы;
- персонал, обслуживающий технические средства (инженеры, техники);
- сотрудники отделов разработки и сопровождения ПО (прикладные и системные программисты);
- технический персонал, обслуживающий здания (уборщики, электрики, сантехники и другие сотрудники, имеющие доступ в здания и помещения, где расположены компоненты АСОИ);
- сотрудники службы безопасности АСОИ;
- руководители различных уровней.

Посторонние лица, которые могут быть нарушителями:

- клиенты (представители других организаций, физические лица);
- посетители (приглашенные по какому-либо поводу);
- представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации (энерго-, водо-, теплоснабжения и т.п.);
- представители конкурирующих организаций (иностранных спецслужб) или лица, действующие по их заданию;
- лица, случайно или умышленно нарушившие пропускной режим (без цели нарушить безопасность АС);
- любые лица, находящиеся внутри контролируемой территории.

Можно выделить три основных мотива нарушений: безответственность, самоутверждение и корыстный интерес.

При нарушениях, вызванных безответственностью, пользователь целенаправленно или случайно производит какие-либо разрушающие действия, не связанные со злым умыслом. В большинстве случаев это следствие некомпетентности или небрежности.

Некоторые пользователи считают получение доступа к АСОИ успехом самоутверждения либо в собственных глазах, либо в глазах коллег.

Нарушение безопасности АСОИ может быть вызвано и корыстным интересом пользователя системы. В этом случае он будет целенаправленно пытаться преодолеть систему защиты для доступа к

хранимой, передаваемой и обрабатываемой в АСОИ информации. Даже если АСОИ имеет средства, делающие такое проникновение чрезвычайно сложным, полностью защитить ее от проникновения практически невозможно.

Всех нарушителей можно классифицировать следующим образом.

По уровню знаний об АСОИ:

- знает функциональные особенности АСОИ, основные закономерности формирования в ней массивов данных и потоков запросов к ним, умеет пользоваться штатными средствами;
- обладает высоким уровнем знаний и опытом работы с техническими средствами системы и их обслуживания;
- обладает высоким уровнем знаний в области программирования и вычислительной техники, проектирования и эксплуатации автоматизированных информационных систем;
- знает структуру, функции и механизм действия средств защиты, их сильные и слабые стороны.

По уровню возможностей (используемым методам и средствам):

- применяющий агентурные методы получения сведений;
- применяющий пассивные средства (технические средства перехвата без модификации компонентов системы);
- использующий только штатные средства и недостатки систем защиты для ее преодоления (несанкционированные действия с использованием разрешенных средств), а также компактные съемные носители информации, которые могут быть скрытно пронесены через посты охраны;
- применяющий методы и средства активного воздействия (модификация и подключение дополнительных технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ).

По времени действия:

- в процессе функционирования АСОИ;
- в период неактивности компонентов системы (в нерабочее время, во время плановых перерывов в ее работе, перерывов для обслуживания и ремонта и т.п.);
- в любом случае.

По месту действия:

- без доступа на контролируемую территорию организации;
- с контролируемой территории без доступа в здания и сооружения;
- внутри помещений, но без доступа к техническим средствам АСОИ;
- с рабочих мест конечных пользователей (операторов) АСОИ;
- с доступом в зону данных (баз данных, архивов и т.п.);
- с доступом в зону управления средствами обеспечения безопасности АСОИ.

Определение конкретных значений характеристик возможных нарушителей в значительной степени субъективно. Модель нарушителя, построенная с учетом особенностей конкретной предметной области и технологии обработки информации, может быть представлена перечислением нескольких вариантов его облика.

2.4. Удаленные атаки на интрасети

Цель предпринимаемых злоумышленниками атак на компьютеры из интрасетей, подключенных к Интернету, состоит в получении доступа к их информационным и сетевым ресурсам. Примером первого типа ресурсов могут быть базы данных, файл-серверы и т.п. Ко второму типу ресурсов относятся различные сетевые сервисы, например, Интернет, электронная почта, телеконференции и т.д.

Принципиальным отличием атак, осуществляемых злоумышленниками в открытых сетях, является фактор расстояния от ПК, выбранного в качестве жертвы, или «прослушиваемого» канала связи до местоположения злоумышленника. Этот фактор нашел выражение в определении подобного вида атак как «удаленных».

Под ***удаленной атакой*** принято понимать несанкционированное информационное воздействие на распределенную вычислительную систему, программно осуществляемое по каналам связи.

Для удаленных атак можно выделить наиболее общие схемы их осуществления. Такие удаленные атаки получили название типовых.

Тогда типовая удаленная атака – это удаленное несанкционированное информационное воздействие, программно осуществляемое по каналам связи и характерное для любой распределенной вычислительной системы.

Объектом удаленных атак могут стать следующие виды сетевых устройств:

- оконечные устройства;
- каналы связи;
- промежуточные устройства: ретрансляторы, шлюзы, модемы и т.п.

Рассмотрим классификацию удаленных атак по следующим шести основным критериям:

1. ***по характеру воздействия*** удаленные атаки делятся на пассивные и активные (примером первого типа атак является, например, прослушивание каналов связи и перехват вводимой с клавиатуры информации; примером второго типа является атака «третий посередине», когда злоумышленник может, например, подменять данные информационного обмена между двумя пользователями Интернета и/или интрасети или между пользователем и запрашиваемым им сетевым сервисом, пересылаемые в обоих направлениях)
2. ***по цели воздействия***, т.е. в зависимости от нарушения трех основных возможных свойств информации и информационных ресурсов – их конфиденциальности, целостности и доступности, плюс нарушение доступности всей системы или ее отдельных служб (пример атаки – «отказ в обслуживании);
3. ***по условию начала осуществления воздействия*** атака может быть безусловной (предпринимается злоумышленником в любом случае), или может активизироваться либо при посылке определенного запроса от атакуемого объекта, либо при наступлении ожидаемого события на атакуемом объекте;
4. ***по наличию обратной связи с атакуемым объектом*** различают атаки с обратной связью или без обратной связи (такая атака называется однонаправленной);
5. ***по расположению субъекта атаки относительно атакуемого объекта*** атаки бывают внутрисегментными (средства взлома сети или, например, прослушивания каналов связи должны располагаться в том же сегменте сети, который интересует злоумышленника) или межсегментными (в этом случае дальность расстояния от жертвы до злоумышленника не имеет значения);
6. ***по уровню эталонной модели взаимосвязи открытых систем OSI Международной организации стандартизации (ISO),*** на котором осуществляется воздействие. Атака может реализовываться на всех семи уровнях – физическом, канальном, сетевом, транспортном,

сеансовом, представительном и прикладном. Средства обеспечения безопасности интрасетей на основе такой модели регламентируются стандартом ISO7492-2. Эти же рекомендации могут применяться и для разработки, создания аналогичных механизмов в Интернет-сетях, так как группа протоколов TCP/IP соответствует уровням 1-4 модели, а прикладной уровень в сетях Интернет соответствует верхним уровням (5-7).

Среди вышеперечисленных УА можно выделить пять основных и наиболее часто предпринимаемых в настоящее время типовых удаленных атак:

1. *Анализ сетевого трафика* (или прослушивание канала связи с помощью специальных средств – снифферов). Эта атака позволяет:

- изучить логику работы сети – получить соответствие событий, происходящих в системе, и команд, пересылаемых при этом хостами, в момент появления данных событий (в дальнейшем это позволит злоумышленнику на основе задания соответствующих команд получить, например, привилегированные права на действия в системе или расширить свои полномочия в ней);
- перехватить поток передаваемых данных, которыми обмениваются компоненты сетевой ОС – для извлечения секретной или идентификационной информации (например, паролей пользователей), ее подмены, модификации и т.п.

2. *Подмена доверенного объекта или субъекта распределенной вычислительной сети* и передача по каналам связи сообщений от его имени с присвоением его прав доступа.

Такая атака эффективно реализуется в системах, где применяются нестойкие алгоритмы идентификации/аутентификации хостов, пользователей и т.д. Под доверенным объектом будем понимать станцию, легально подключенную к серверу (в более общем смысле «доверенная» система – это система, которая достигает специфического уровня контроля за доступом к информации, обеспечивая механизм предотвращения (или определения) неавторизованного доступа).

3. *Ложный объект распределенной вычислительной сети.* Он внедряется двумя способами:

- навязыванием ложного маршрута из-за недостатков в алгоритмах маршрутизации (т.е. проблем идентификации сетевых управляющих устройств), в результате чего можно попасть в сеть

жертвы, где с помощью определенных средств можно «вскрыть» ее компьютер;

- использованием недостатков алгоритмов удаленного поиска (SAP(NetWare), и DNS (Internet)…).

Эта атака позволяет воздействовать на перехваченную информацию следующим образом:

- проводить селекцию потока информации;
- модифицировать информацию;
- подменять информацию.

4. *Отказ в обслуживании.* Атака может быть предпринята, если нет средств аутентификации адреса отправителя и с хоста на атакуемый хост можно передавать бесконечное число анонимных запросов на подключение от имени других хостов. В этом способе проникновения используется возможность фрагментирования пакетов, содержащаяся в спецификации IP. Нападающий передает слишком много фрагментов пакетов, которые должны быть смонтированы принимающей системой. Если общий объем фрагментов превышает максимально допустимый размер пакета, то система «зависает» или даже выходит из строя.

Результатом осуществления данной атаки может стать:

- нарушение работоспособности соответствующей службы предоставления удаленного доступа на атакуемый хост;
- передача с одного адреса такого количества запросов на подключение к атакуемому хосту, какое максимально может «вместить» трафик (атака – направленный «шторм запросов»), что влечет за собой переполнение очереди запросов и отказ одной из сетевых служб или полная остановка ПК из-за невозможности системы заниматься ничем другим, кроме обработки запросов.

5. *Удаленный контроль над станцией в сети.* Атака заключается в запуске на атакуемом компьютере программы «сетевого шпиона», основная цель которой – получение удаленного контроля над станцией в сети. Схематично основные этапы работы сетевого шпиона выглядят следующим образом:

- инсталляция в памяти;
- ожидание запроса с удаленного хоста, на котором запущена головная сервер-программа и обмен с ней сообщениями о готовности;
- передача перехваченной информации на головную сервер-программу или предоставление ей контроля над атакуемым компьютером.

Контрольные вопросы

1. Виды угроз информационной безопасности Российской Федерации.
2. Угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности.
3. Угрозы информационному обеспечению государственной политики Российской Федерации.
4. Угрозы развитию отечественной индустрии информации.
5. Угрозы безопасности информационных и телекоммуникационных средств и систем.
6. Источники угроз информационной безопасности Российской Федерации.
7. Внешние источники информационной безопасности Российской Федерации.
8. Внутренние источники информационной безопасности Российской Федерации.
9. Угрозы информационной безопасности для автоматизированных систем обработки информации (АСОИ).
10. Уязвимость основных структурно-функциональных элементов распределенных АСОИ.
11. Основные виды угроз безопасности субъектов информационных отношений.
12. Классификация угроз безопасности информации.
13. Естественные угрозы информации.
14. Искусственные угрозы информации.
15. Непреднамеренные угрозы информации.
16. Преднамеренные угрозы информации.
17. Основные непреднамеренные искусственные угрозы.
18. Основные преднамеренные искусственные угрозы.
19. Классификация каналов проникновения в систему и утечки информации.
20. Неформальная модель нарушителя в АС.
21. Удаленные атаки на интрасети.
22. Что принято понимать под удаленной атакой.
23. Классификация удаленных атак.

Тесты

1. Естественные угрозы безопасности информации вызваны:

1. деятельностью человека;
2. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
3. воздействиями объективных физических процессов или стихийных природных явлений, не зависящих от человека;
4. корыстными устремлениями злоумышленников;
5. ошибками при действиях персонала.

2. Искусственные угрозы безопасности информации вызваны:

1. деятельностью человека;
2. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
3. воздействиями объективных физических процессов или стихийных природных явлений, не зависящих от человека;
4. корыстными устремлениями злоумышленников;
5. ошибками при действиях персонала.

3. К основным непреднамеренным искусственным угрозам АСОИ относится:

1. физическое разрушение системы путем взрыва, поджога и т.п.;
2. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;
3. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
4. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
5. неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы.

4. К основным непреднамеренным искусственным угрозам АСОИ относится:

1. физическое разрушение системы путем взрыва, поджога и т.п.;
2. неправомерное отключение оборудования или изменение режимов работы устройств и программ;
3. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
4. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
5. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи.

5. К основным непреднамеренным искусственным угрозам АСОИ относится:

1. физическое разрушение системы путем взрыва, поджога и т.п.;
2. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
3. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
4. неумышленная порча носителей информации;
5. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи.

6. К основным непреднамеренным искусственным угрозам АСОИ относится:

1. запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы;
2. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
3. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
4. физическое разрушение системы путем взрыва, поджога и т.п.;
5. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи.

7. К основным непреднамеренным искусственным угрозам АСОИ относится:

1. физическое разрушение системы путем взрыва, поджога и т.п.;
2. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
3. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
4. нелегальное внедрение и использование неучтенных программ игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения служебных обязанностей;
5. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи.

8. К основным непреднамеренным искусственным угрозам АСОИ относится:

1. физическое разрушение системы путем взрыва, поджога и т.п.;
2. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
3. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;

4. неосторожные действия, приводящие к разглашению конфиденциальной информации, или делающие ее общедоступной;
5. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи.

9. К основным непреднамеренным искусственным угрозам АСОИ относится:

1. физическое разрушение системы путем взрыва, поджога и т.п.;
2. разглашение, передача или утрата атрибутов разграничения доступа;
3. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
4. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
5. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи.

10. К основным непреднамеренным искусственным угрозам АСОИ относится:

1. физическое разрушение системы путем взрыва, поджога и т.п.;
2. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;
3. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
4. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
5. проектирование архитектуры системы, с возможностями, представляющими опасность для работоспособности системы и безопасности информации.

11. К основным непреднамеренным искусственным угрозам АСОИ относится:

1. игнорирование организационных ограничений при работе в системе;
2. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;
3. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
4. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
5. физическое разрушение системы путем взрыва, поджога и т.п.

12. К основным непреднамеренным искусственным угрозам АСОИ относится:

1. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
2. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;
3. вход в систему в обход средств защиты;
4. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
5. физическое разрушение системы путем взрыва, поджога и т.п.

13. К основным непреднамеренным искусственным угрозам АСОИ относится:

1. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
2. некомпетентное использование, настройка или отключение средств защиты;
3. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;
4. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
5. физическое разрушение системы путем взрыва, поджога и т.п.

14. К основным непреднамеренным искусственным угрозам АСОИ относится:

1. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
2. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
3. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;
4. пересылка данных по ошибочному адресу абонента;
5. физическое разрушение системы путем взрыва, поджога и т.п.

15. К основным непреднамеренным искусственным угрозам АСОИ относится:

1. ввод ошибочных данных;
2. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
3. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;
4. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
5. физическое разрушение системы путем взрыва, поджога и т.п.

16. К основным непреднамеренным искусственным угрозам АСОИ относится:

1. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;
2. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
3. неумышленное повреждение каналов связи;
4. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
5. физическое разрушение системы путем взрыва, поджога и т.п.

17. К основным преднамеренным искусственным угрозам АСОИ относится:

1. неправомерное отключение оборудования или изменение режимов работы устройств и программ;
2. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);
3. физическое разрушение системы путем взрыва, поджога и т.п.;
4. игнорирование организационных ограничений (установленных правил) при работе в системе;
5. пересылка данных по ошибочному адресу абонента.

18. К основным преднамеренным искусственным угрозам АСОИ относится:

1. отключение или вывод из строя систем электропитания, охлаждения и вентиляции, линий связи и т.п.;
2. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);
3. неправомерное отключение оборудования или изменение режимов работы устройств и программ;
4. игнорирование организационных ограничений (установленных правил) при работе в системе;
5. пересылка данных по ошибочному адресу абонента.

19. К основным преднамеренным искусственным угрозам АСОИ относится:

1. пересылка данных по ошибочному адресу абонента;
2. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);

3. неправомерное отключение оборудования или изменение режимов работы устройств и программ;
4. игнорирование организационных ограничений (установленных правил) при работе в системе;
5. действия по дезорганизации функционирования системы (изменение режимов работы, забастовка, саботаж персонала и т.п.).

20. К основным преднамеренным искусственным угрозам АСОИ относится:
1. пересылка данных по ошибочному адресу абонента;
2. внедрение агентов в число персонала системы, в том числе в административную группу, отвечающую за безопасность;
3. неправомерное отключение оборудования или изменение режимов работы устройств и программ;
4. игнорирование организационных ограничений (установленных правил) при работе в системе;
5. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).

21. К основным преднамеренным искусственным угрозам АСОИ относится:
1. пересылка данных по ошибочному адресу абонента;
2. игнорирование организационных ограничений (установленных правил) при работе в системе;
3. неправомерное отключение оборудования или изменение режимов работы устройств и программ;
4. вербовка персонала или отдельных пользователей, имеющих необходимые полномочия;
5. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).

22. К основным преднамеренным искусственным угрозам АСОИ относится:
1. пересылка данных по ошибочному адресу абонента;
2. игнорирование организационных ограничений (установленных правил) при работе в системе;
3. применение подслушивающих устройств, дистанционная фото- и видеосъемка и т.п.;
4. неправомерное отключение оборудования или изменение режимов работы устройств и программ;

5. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).

23. К основным преднамеренным искусственным угрозам АСОИ относится:

1. пересылка данных по ошибочному адресу абонента;
2. игнорирование организационных ограничений (установленных правил) при работе в системе;
3. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;
4. неправомерное отключение оборудования или изменение режимов работы устройств и программ;
5. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).

24. К основным преднамеренным искусственным угрозам АСОИ относится:

1. перехват данных, передаваемых по каналам связи;
2. игнорирование организационных ограничений (установленных правил) при работе в системе;
3. пересылка данных по ошибочному адресу абонента;
4. неправомерное отключение оборудования или изменение режимов работы устройств и программ;
5. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).

25. К основным преднамеренным искусственным угрозам АСОИ относится:

1. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);
2. игнорирование организационных ограничений (установленных правил) при работе в системе;
3. пересылка данных по ошибочному адресу абонента;
4. неправомерное отключение оборудования или изменение режимов работы устройств и программ;
5. хищение носителей информации.

26. К основным преднамеренным искусственным угрозам АСОИ относится:

1. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);
2. игнорирование организационных ограничений (установленных правил) при работе в системе;
3. несанкционированное копирование носителей информации;
4. неправомерное отключение оборудования или изменение режимов работы устройств и программ;
5. пересылка данных по ошибочному адресу абонента.

27. К основным преднамеренным искусственным угрозам АСОИ относится:

1. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);
2. хищение производственных отходов (распечаток, записей, списанных носителей информации и т.п.);
3. игнорирование организационных ограничений (установленных правил) при работе в системе;
4. неправомерное отключение оборудования или изменение режимов работы устройств и программ;
5. пересылка данных по ошибочному адресу абонента.

28. К основным преднамеренным искусственным угрозам АСОИ относится:

1. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
2. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);
3. игнорирование организационных ограничений (установленных правил) при работе в системе;
4. неправомерное отключение оборудования или изменение режимов работы устройств и программ;
5. пересылка данных по ошибочному адресу абонента.

29. К основным преднамеренным искусственным угрозам АСОИ относится:

1. неправомерное отключение оборудования или изменение режимов работы устройств и программ;

2. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);
3. игнорирование организационных ограничений (установленных правил) при работе в системе;
4. незаконное получение паролей и других реквизитов разграничения доступа;
5. пересылка данных по ошибочному адресу абонента.

30. К основным преднамеренным искусственным угрозам АСОИ относится:
1. неправомерное отключение оборудования или изменение режимов работы устройств и программ;
2. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);
3. игнорирование организационных ограничений (установленных правил) при работе в системе;
4. пересылка данных по ошибочному адресу абонента;
5. несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики.

31. К основным преднамеренным искусственным угрозам АСОИ относится:
1. неправомерное отключение оборудования или изменение режимов работы устройств и программ;
2. вскрытие шифров криптозащиты информации;
3. игнорирование организационных ограничений (установленных правил) при работе в системе;
4. пересылка данных по ошибочному адресу абонента;
5. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).

32. К основным преднамеренным искусственным угрозам АСОИ относится:
1. неправомерное отключение оборудования или изменение режимов работы устройств и программ;
2. пересылка данных по ошибочному адресу абонента;
3. игнорирование организационных ограничений (установленных правил) при работе в системе;

4. внедрение аппаратных спецвложений, программных «закладок» и «вирусов»;
5. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).

33. К основным преднамеренным искусственным угрозам АСОИ относится:

1. неправомерное отключение оборудования или изменение режимов работы устройств и программ;
2. незаконное подключение к линиям связи с целью работы «между строк»;
3. игнорирование организационных ограничений (установленных правил) при работе в системе;
4. пересылка данных по ошибочному адресу абонента;
5. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).

34. К основным преднамеренным искусственным угрозам АСОИ относится:

1. неправомерное отключение оборудования или изменение режимов работы устройств и программ;
2. игнорирование организационных ограничений (установленных правил) при работе в системе;
3. незаконное подключение к линиям связи с целью подмены законного пользователя путем его отключения после входа в систему;
4. пересылка данных по ошибочному адресу абонента;
5. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).

35. К внутренним нарушителям информационной безопасности относятся:

1. клиенты;
2. пользователи системы;
3. посетители;
4. любые лица, находящиеся внутри контролируемой территории;
5. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации.

36. К внутренним нарушителям информационной безопасности относятся:

1. клиенты;
2. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
3. посетители;
4. любые лица, находящиеся внутри контролируемой территории;
5. персонал, обслуживающий технические средства.

37. К внутренним нарушителям информационной безопасности относятся:

1. сотрудники отделов разработки и сопровождения ПО;
2. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
3. посетители;
4. любые лица, находящиеся внутри контролируемой территории;
5. клиенты.

38. К внутренним нарушителям информационной безопасности относятся:

1. посетители;
2. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
3. технический персонал, обслуживающий здание;
4. любые лица, находящиеся внутри контролируемой территории;
5. клиенты.

39. К внутренним нарушителям информационной безопасности относятся:

1. посетители;
2. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
3. любые лица, находящиеся внутри контролируемой территории;
4. сотрудники службы безопасности;
5. клиенты.

40. К внутренним нарушителям информационной безопасности относятся:

1. посетители;
2. руководители различных уровней;

3. любые лица, находящиеся внутри контролируемой территории;
4. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
5. клиенты.

41. К посторонним нарушителям информационной безопасности относятся:
1. пользователи;
2. персонал, обслуживающий технические средства;
3. клиенты;
4. технический персонал, обслуживающий здание;
5. сотрудники службы безопасности.

42. К посторонним нарушителям информационной безопасности относятся:
1. пользователи;
2. персонал, обслуживающий технические средства;
3. технический персонал, обслуживающий здание;
4. посетители;
5. сотрудники службы безопасности.

43. К посторонним нарушителям информационной безопасности относятся:
1. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
2. персонал, обслуживающий технические средства;
3. технический персонал, обслуживающий здание;
4. пользователи;
5. сотрудники службы безопасности.

44. К посторонним нарушителям информационной безопасности относятся:
1. сотрудники службы безопасности;
2. персонал, обслуживающий технические средства;
3. технический персонал, обслуживающий здание;
4. пользователи;
5. представители конкурирующих организаций.

45. К посторонним нарушителям информационной безопасности относятся:
1. сотрудники службы безопасности;
2. лица, нарушившие пропускной режим;

3. технический персонал, обслуживающий здание;
4. пользователи;
5. персонал, обслуживающий технические средства.

46. По характеру воздействия удаленные атаки делятся:

1. на условные и безусловные;
2. на атаки с обратной связью и без обратной связи;
3. на внутрисегментные и межсегментные;
4. на пассивные и активные;
5. на атаки, которые могут реализовываться на всех семи уровнях – физическом, канальном, сетевом, транспортном, сеансовом, представительном и прикладном.

47. По цели воздействия удаленные атаки делятся:

1. на условные и безусловные;
2. на атаки с обратной связью и без обратной связи;
3. на внутрисегментные и межсегментные;
4. на пассивные и активные;
5. на атаки в зависимости от нарушения конфиденциальности, целостности и доступности.

48. По условию начала осуществления воздействия удаленные атаки делятся:

1. на условные и безусловные;
2. на атаки с обратной связью и без обратной связи;
3. на внутрисегментные и межсегментные;
4. на пассивные и активные;
5. на атаки в зависимости от нарушения конфиденциальности, целостности и доступности.

49. По наличию обратной связи с атакуемым объектом удаленные атаки делятся:

1. на условные и безусловные;
2. на атаки с обратной связью и без обратной связи;
3. на внутрисегментные и межсегментные;
4. на пассивные и активные;
5. на атаки в зависимости от нарушения конфиденциальности, целостности и доступности.

50. По расположению субъекта атаки относительно атакуемого объекта удаленные атаки делятся:

1. на условные и безусловные;

2. на атаки с обратной связью и без обратной связи;
3. на внутрисегментные и межсегментные;
4. на пассивные и активные;
5. на атаки в зависимости от нарушения конфиденциальности, целостности и доступности.

51. По уровню эталонной модели взаимосвязи открытых систем OSI Международной организации стандартизации (ISO) удаленные атаки делятся:

1. на условные и безусловные;
2. на атаки с обратной связью и без обратной связи;
3. на внутрисегментные и межсегментные;
4. на пассивные и активные;
5. на атаки, которые могут реализовываться на всех семи уровнях.

52. Атака, которая позволяет изучить логику работы сети:

1. подмена доверенного объекта или субъекта распределенной вычислительной сети;
2. ложный объект распределенной вычислительной сети;
3. анализ сетевого трафика;
4. отказ в обслуживании;
5. удаленный контроль над станцией в сети.

53. Атака, позволяющая перехватить поток передаваемых данных, которыми обмениваются компоненты сетевой ОС:

1. подмена доверенного объекта или субъекта распределенной вычислительной сети;
2. ложный объект распределенной вычислительной сети;
3. анализ сетевого трафика;
4. отказ в обслуживании;
5. удаленный контроль над станцией в сети.

54. Атака, эффективно реализующаяся в системах, где применяются нестойкие алгоритмы идентификации/аутентификации хостов, пользователей:

1. подмена доверенного объекта или субъекта распределенной вычислительной сети;
2. ложный объект распределенной вычислительной сети;
3. анализ сетевого трафика;
4. отказ в обслуживании;
5. удаленный контроль над станцией в сети.

55. Атака, которая заключается в навязывании ложного маршрута из-за недостатков в алгоритмах маршрутизации:

1. подмена доверенного объекта или субъекта распределенной вычислительной сети;
2. ложный объект распределенной вычислительной сети;
3. анализ сетевого трафика;
4. отказ в обслуживании;
5. удаленный контроль над станцией в сети.

56. Атака, которая использует недостатки алгоритмов удаленного поиска (SAP(NetWare), и DNS (Internet)…):

1. подмена доверенного объекта или субъекта распределенной вычислительной сети;
2. ложный объект распределенной вычислительной сети;
3. анализ сетевого трафика;
4. отказ в обслуживании;
5. удаленный контроль над станцией в сети.

57. Атака, которая позволяет воздействовать на перехваченную информацию (проводить селекцию потока информации):

1. подмена доверенного объекта или субъекта распределенной вычислительной сети;
2. ложный объект распределенной вычислительной сети;
3. анализ сетевого трафика;
4. отказ в обслуживании;
5. удаленный контроль над станцией в сети.

58. Атака, которая позволяет воздействовать на перехваченную информацию (модифицировать информацию):

1. подмена доверенного объекта или субъекта распределенной вычислительной сети;
2. ложный объект распределенной вычислительной сети;
3. анализ сетевого трафика;
4. отказ в обслуживании;
5. удаленный контроль над станцией в сети.

59. Атака, которая позволяет воздействовать на перехваченную информацию (подменять информацию):

1. подмена доверенного объекта или субъекта распределенной вычислительной сети;
2. ложный объект распределенной вычислительной сети;
3. анализ сетевого трафика;

4. отказ в обслуживании;
5. удаленный контроль над станцией в сети.

60. Атака, результатом осуществления которой может стать нарушение работоспособности соответствующей службы предоставления удаленного доступа на атакуемый хост:

1. подмена доверенного объекта или субъекта распределенной вычислительной сети;
2. ложный объект распределенной вычислительной сети;
3. анализ сетевого трафика;
4. отказ в обслуживании;
5. удаленный контроль над станцией в сети.

61. Атака, которая может быть предпринята, если нет средств аутентификации адреса отправителя и с хоста на атакуемый хост можно передавать бесконечное число анонимных запросов на подключение от имени других хостов:

1. подмена доверенного объекта или субъекта распределенной вычислительной сети;
2. ложный объект распределенной вычислительной сети;
3. анализ сетевого трафика;
4. отказ в обслуживании;
5. удаленный контроль над станцией в сети.

62. Атака, которая заключается в передаче с одного адреса такого количества запросов на подключение к атакуемому хосту, какое максимально может «вместить» трафик:

1. подмена доверенного объекта или субъекта распределенной вычислительной сети;
2. ложный объект распределенной вычислительной сети;
3. анализ сетевого трафика;
4. отказ в обслуживании;
5. удаленный контроль над станцией в сети.

63. Атака, которая заключается в запуске на атакуемом компьютере программы «сетевого шпиона»:

1. подмена доверенного объекта или субъекта распределенной вычислительной сети;
2. ложный объект распределенной вычислительной сети;
3. анализ сетевого трафика;
4. отказ в обслуживании;
5. удаленный контроль над станцией в сети.

64. Атака, которая заключается в запуске на атакуемом компьютере программы «сетевого шпиона»:

1. подмена доверенного объекта или субъекта распределенной вычислительной сети;
2. ложный объект распределенной вычислительной сети;
3. анализ сетевого трафика;
4. отказ в обслуживании;
5. удаленный контроль над станцией в сети.

Тема 3.

Вредоносные программы

Изучив тему 3, студент должен:
знать:

- какие программы называются «компьютерными вирусами» и чем они отличаются от других вредных программ;
- классификацию «компьютерных вирусов», и какую угрозу они представляют для безопасности информации;
- алгоритмы работы «компьютерных вирусов» и пути их внедрения в систему;
- по индивидуальным признакам различать «компьютерные вирусы» различных классов;

акцентировать внимание на понятиях:

- «компьютерные вирусы», свойства «компьютерных вирусов», вредные программы, резидентность, стелс, самошифрование, полиморфичность, overwriting-вирусы, parasitig-вирусы, companion-вирусы, link-вирусы, файловые черви, макровирусы, сетевые вирусы, «троянскин кони», логические бомбы

Содержание темы (дидактические единицы и их характеристика):

Какие имеются вредоносные программы, как они классифицируются. Алгоритмы работы «компьютерных вирусов» и их деструктивные возможности.

Цели и задачи изучения темы: Получение знаний о существующих «компьютерных вирусах» и об алгоритмах их работы.

Порядок изучения темы

Распределение бюджета времени по теме:

- количество часов отведенных на практические занятия, из них в компьютерной аудитории – 4/4;
- количество часов, отведенных на самостоятельную работу – 16.

Виды самостоятельной работы студентов:

- изучение учебного пособия «Информационная безопасность»;
- подготовка к участию в форуме по теме «Компьютерные вирусы»;
- изучение дополнительной литературы;
- выполнение тестовых заданий по теме.

Методические указания по изучению вопросов темы

При изучении учебных вопросов:

- изучить тему 3 по учебному пособию «Информационная безопасность»;
- принять участие в форуме по теме «Вредоносные программы»;
- изучить дополнительные материалы;

При изучении темы необходимо:

- *читать литературу*:

1. Информационная безопасность: Уч. Пособие. – М.: МЭСИ, 2007.
2. Касперский Е.В. Компьютерные вирусы: что это такое и как с ними бороться. – М.: СК Пресс, 1998.
3. Фролов А.В., Фролов Г.В. Осторожно: компьютерные вирусы. – М.: Диалог-МИФИ, 1996.

- *посетить сайты:* www.viruslist.com, www.subscribe.ru, www.refer.ru, www.virus.komi.ru.

Вопросы темы

3.1. Условия существования вредоносных программ.
3.2. Классические компьютерные вирусы.
3.3. Сетевые черви.
3.4. Троянские программы.
3.5. Спам.
3.6. Хакерские утилиты и прочие вредоносные программы.
3.7. Кто и почему создает вредоносные программы.

К вредоносным программам относятся: классические файловые вирусы, сетевые черви, троянские программы, спам, хакерские утилиты и прочие программы, наносящие заведомый вред компьютеру, на котором они запускаются на выполнение, или другим компьютерам в сети.

3.1. Условия существования вредоносных программ

Операционная система или приложение может подвергнуться вирусному нападению в том случае, если она имеет возможность запустить программу, не являющуюся частью самой системы. Данному условию удовлетворяют все популярные операционные системы, многие офисные приложения, графические редакторы, системы проектирования и прочие программные комплексы, имеющие встроенные скриптовые языки.

Компьютерные вирусы, черви, троянские программы существуют для десятков операционных систем и приложений. В то же время существует огромное количество других операционных систем и приложений, для которых вредоносные программы пока не обнаружены.

Причиной появления вредоносных программ в конкретной операционной системе или приложении является одновременное выполнение следующих условий:

- популярность, широкое распространение данной системы;
- наличие разнообразной и достаточно полной документации по системе;
- незащищенность системы или существование известных уязвимостей в системе безопасности.

Каждое перечисленное условие является необходимым, а выполнение всех трех условий одновременно является достаточным для появления разнообразных вредоносных программ.

Условие популярности системы необходимо для того, чтобы она заинтересовала компьютерных хулиганов или хакеров. Если производитель системы добился ее массового распространения, то очевидно, что рано или поздно хакеры и вирусописатели попытаются использовать ее в своих интересах.

Напрашивается естественный вывод: чем популярнее операционная система или приложение, тем чаще она будет являться

жертвой вирусной атаки. Практика это подтверждает – распределение количества вредного программного обеспечения для Windows и Linux практически совпадает с долями рынка, которые занимают эти операционные системы.

Наличие полной документации необходимо для существования вирусов по естественной причине – создание программ (включая вирусные) невозможно без технического описания использования сервисов операционной системы и правил написания приложений. У большинства мобильных телефонов, например, подобная информация закрыта – ни компании-производители программных продуктов, ни хакеры не имеют возможности разрабатывать программы для данных устройств. У некоторых телефонов есть документация по разработке приложений – и, как следствие, появляются и вредоносные программы, разработанные специально для телефонов данного типа.

Под ***защищенностью*** системы понимаются архитектурные решения, которые не позволяют новому (неизвестному) приложению получить полный или достаточно широкий доступ к файлам на диске (включая другие приложения) и потенциально опасным сервисам системы. Подобное ограничение фактически блокирует любую вирусную активность, но при этом, естественно, накладывает существенные ограничения на возможности обычных программ.

3.2. Классические компьютерные вирусы

К данной категории относятся программы, распространяющие свои копии по ресурсам локального компьютера с целью:

- последующего запуска своего кода при каких-либо действиях пользователя;
- дальнейшего внедрения в другие ресурсы компьютера.

В отличие от червей вирусы не используют сетевых сервисов для проникновения на другие компьютеры. Копия вируса попадает на удаленные компьютеры только в том случае, если зараженный объект по каким-либо не зависящим от функционала вируса причинам оказывается активизированным на другом компьютере, например:

- при заражении доступных дисков вирус проник в файлы, расположенные на сетевом ресурсе;

- вирус скопировал себя на съемный носитель или заразил файлы на нем;
- пользователь отослал электронное письмо с зараженным вложением.

Некоторые вирусы содержат в себе свойства других разновидностей вредоносного программного обеспечения, например бэкдор-процедуру или троянскую компоненту уничтожения информации на диске.

Классификация классических вирусов

Типы компьютерных вирусов различаются между собой по следующим основным признакам:

1. Среда обитания;
2. Способ заражения.

Под «средой обитания» понимаются системные области компьютера, операционные системы или приложения, в компоненты (файлы) которых внедряется код вируса. Под «способом заражения» понимаются различные методы внедрения вирусного кода в заражаемые объекты.

Среда обитания

По среде обитания вирусы можно разделить на:

- файловые;
- загрузочные;
- макровирусы;
- скриптовые.

Файловые вирусы при своем размножении тем или иным способом используют файловую систему какой-либо (или каких-либо) ОС. Они:

- различными способами внедряются в исполняемые файлы (наиболее распространенный тип вирусов);
- создают файлы-двойники (компаньон-вирусы);
- создают свои копии в различных каталогах;
- используют особенности организации файловой системы (link-вирусы).

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

активный boot-сектор. Данный тип вирусов был достаточно распространен в 1990-х гг., но практически исчез с переходом на 32-битные операционные системы и отказом от использования дискет как основного способа обмена информацией. Теоретически возможно появление загрузочных вирусов, заражающих CD-диски и USB-флешек, но на текущий момент такие вирусы не обнаружены.

Многие табличные и графические редакторы, системы проектирования, текстовые процессоры имеют свои макро-языки для автоматизации выполнения повторяющихся действий. Эти макро-языки часто имеют сложную структуру и развитый набор команд. Макро-вирусы являются программами на макро-языках, встроенных в такие системы обработки данных. Для своего размножения вирусы этого класса используют возможности макро-языков и при их помощи переносят себя из одного зараженного файла (документа или таблицы) в другие.

Способы заражения

Файловые вирусы

По способу заражения файлов вирусы делятся на:

- перезаписывающие вирусы (overwriting);
- паразитические вирусы (parasitic);
- вирусы-компаньоны (companion);
- вирусы-ссылки (link);
- вирусы, заражающие объектные модули (OBJ);
- вирусы, заражающие библиотеки компиляторов (LIB);
- вирусы, заражающие исходные тексты программ.

Overwriting

Данный метод заражения является наиболее простым: вирус записывает свой код вместо кода заражаемого файла, уничтожая его содержимое. Естественно, что при этом файл перестает работать и не восстанавливается. Такие вирусы очень быстро обнаруживают себя, так как операционная система и приложения довольно быстро перестают работать.

Parasitic

К паразитическим относятся все файловые вирусы, которые при распространении своих копий обязательно изменяют содержимое файлов, оставляя сами файлы при этом полностью или частично работоспособными.

Основными типами таких вирусов являются вирусы, записывающиеся в начало файлов (prepending), в конец файлов (appending) и в середину файлов (inserting). В свою очередь, внедрение вирусов в середину файлов происходит различными методами – путем переноса части файла в его конец или копирования своего кода в заведомо неиспользуемые данные файла (cavity-вирусы).

Внедрение вируса в начало файла

Известны два способа внедрения паразитического файлового вируса в начало файла. Первый способ заключается в том, что вирус переписывает начало заражаемого файла в его конец, а сам копируется в освободившееся место (рис 3.1). При заражении файла вторым способом вирус дописывает заражаемый файл к своему телу (рис 3.2).

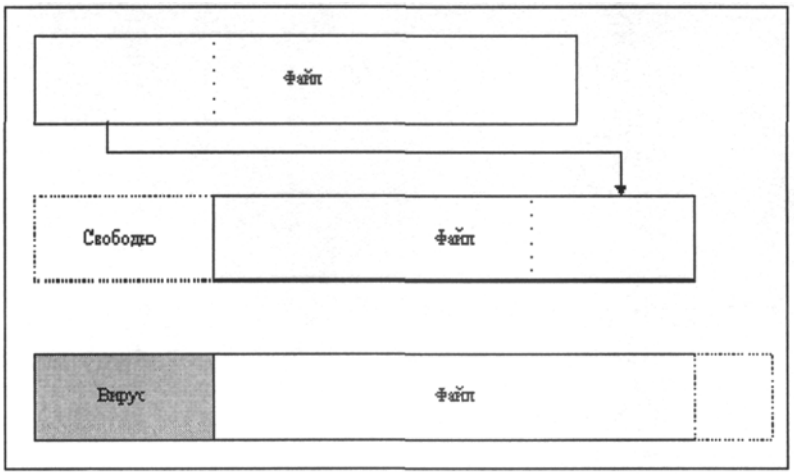


Рис. 3.1. **Внедрение вируса в начало файла первым способом**

Таким образом, при запуске зараженного файла первым управление получает код вируса. При этом вирусы, чтобы сохранить работоспособность программы, либо лечат зараженный файл, повторно запускают его, ждут окончания его работы и снова записываются в его начало (иногда для этого используется временный файл, в который записывается обезвреженный файл), либо восстанавливают код программы в памяти компьютера и настраивают необходимые адреса в ее теле (т. е. дублируют работу ОС).

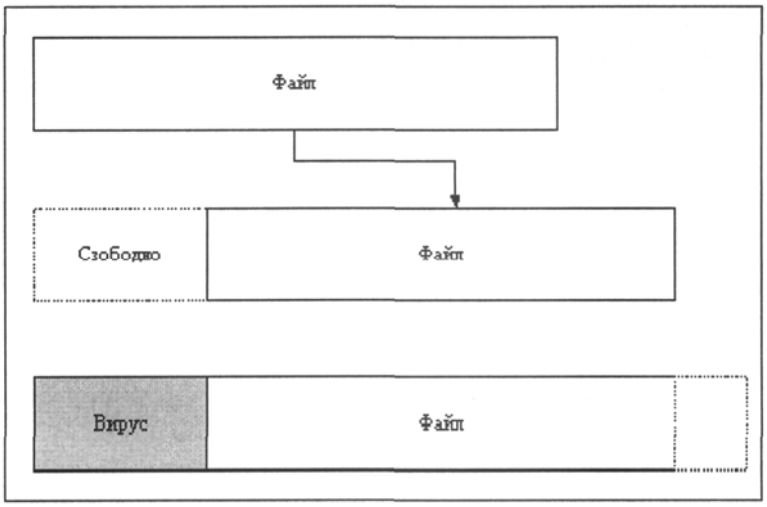


Рис. 3.2. **Внедрение вируса в начало файла вторым способом**

Внедрение вируса в конец файла

Наиболее распространенным способом внедрения вируса в файл является дописывание вируса в его конец (рис. 3.3).

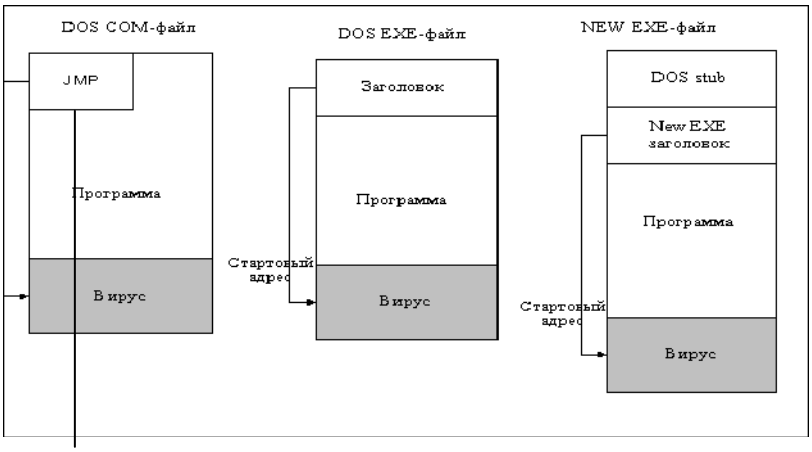


Рис. 3.3. **Внедрение вируса в конец файла**

При этом вирус изменяет начало файла таким образом, что первыми выполняемыми командами программы, содержащейся в файле, являются команды вируса.

Для того чтобы получить управление при старте файла, вирус корректирует стартовый адрес программы (адрес точки входа). Для этого вирус производит необходимые изменения в заголовке файла.

Внедрение вируса в середину файла

Существует несколько методов внедрения вируса в середину файла. В наиболее простом из них вирус переносит часть файла в его конец или «раздвигает» файл и записывает свой код в освободившееся пространство. Этот способ во многом аналогичен методам, перечисленным выше. Некоторые вирусы при этом компрессируют переносимый блок файла так, что длина файла при заражении не изменяется.

Вторым является метод «cavity», при котором вирус записывается в заведомо неиспользуемые области файла. Вирус может быть скопирован в незадействованные области заголовок EXE-файла, в «дыры» между секциями EXE-файлов или в область текстовых сообщений популярных компиляторов. Существуют вирусы, заражающие только те файлы, которые содержат блоки, заполненные каким-либо постоянным байтом, при этом вирус записывает свой код вместо такого блока.

Кроме того, копирование вируса в середину файла может произойти в результате ошибки вируса, в этом случае файл может быть необратимо испорчен.

Вирусы без точки входа

Отдельно следует отметить довольно незначительную группу вирусов, не имеющих «точки входа» (EPO-вирусы – Entry Point Obscuring viruses). К ним относятся вирусы, не изменяющие адрес точки старта в заголовке EXE-файлов. Такие вирусы записывают команду перехода на свой код в какое-либо место в середину файла и получают управление не непосредственно при запуске зараженного файла, а при вызове процедуры, содержащей код передачи управления на тело вируса. Причем выполняться эта процедура может крайне редко (например, при выводе сообщения о какой-либо специфической ошибке). В результате вирус может долгие годы «спать» внутри файла и выскочить на свободу только при некоторых ограниченных условиях.

Перед тем, как записать в середину файла команду перехода на свой код, вирусу необходимо выбрать «правильный» адрес в файле – иначе зараженный файл может оказаться испорченным. Известны несколько способов, с помощью которых вирусы определяют такие адреса внутри файлов, например, поиск в файле последовательности стандартного кода заголовков процедур языков программирования (C/Pascal), дизассемблирование кода файла или замена адресов импортируемых функций.

Companion

К категории «companion» относятся вирусы, не изменяющие заражаемых файлов. Алгоритм работы этих вирусов состоит в том, что для заражаемого файла создается файл-двойник, причем при запуске зараженного файла управление получает именно этот двойник, т. е. вирус.

К вирусам данного типа относятся те из них, которые при заражении переименовывают файл в какое-либо другое имя, запоминают его (для последующего запуска файла-хозяина) и записывают свой код на диск под именем заражаемого файла. Например, файл NOTEPAD.EXE переименовывается в NOTEPAD.EXD, а вирус записывается под именем NOTEPAD.EXE. При запуске управление получает код вируса, который затем запускает оригинальный NOTEPAD.

Возможно существование и других типов вирусов-компаньонов, использующих иные оригинальные идеи или особенности других операционных систем. Например, PATH-компаньоны, которые размещают свои копии в основном катагоге Windows, используя тот факт, что этот каталог является первым в списке PATH, и файлы для запуска Windows, в первую очередь, будет искать именно в нем. Данными способом самозапуска пользуются также многие компьютерные черви и троянские программы.

Прочие способы заражения

Существуют вирусы, которые никоим образом не связывают свое присутствие с каким-либо выполняемым файлом. При размножении они всего лишь копируют свой код в какие-либо каталоги дисков в надежде, что эти новые копии будут когда-либо запущены пользователем. Иногда эти вирусы дают своим копиям «специальные» имена, чтобы подтолкнуть пользователя на запуск своей копии – например, INSTALL.EXE или WINSTART.BAT.

Некоторые вирусы записывают свои копии в архивы (ARJ, ZIP, RAR). Другие записывают команду запуска зараженного файла в BAT-файлы.

Link-вирусы также не изменяют физического содержимого файлов, однако при запуске зараженного файла «заставляют» ОС выполнить свой код. Этой цели они достигают модификацией необходимых полей файловой системы.

Загрузочные вирусы

Известные на текущий момент загрузочные вирусы заражают загрузочный (boot) сектор гибкого диска и boot-сектор или Master Boot Record (MBR) винчестера. Принцип действия загрузочных вирусов основан на алгоритмах запуска операционной системы при включении или перезагрузке компьютера – после необходимых тестов установленного оборудования (памяти, дисков и т.д.) программа системной загрузки считывает первый физический сектор загрузочного диска (A:, C: или CD-ROM в зависимости от параметров, установленных в BIOS Setup) и передает на него управление.

При заражении дисков загрузочные вирусы «подставляют» свой код вместо какой-либо программы, получающей управление при загрузке системы. Принцип заражения, таким образом, одинаков во всех описанных выше способах: вирус «заставляет» систему при ее перезапуске считать в память и отдать управление не оригинальному коду загрузчика, но коду вируса.

Заражение дискет производится единственным известным способом – вирус записывает свой код вместо оригинального кода boot-сектора дискеты. Винчестер заражается тремя возможными способами – вирус записывается либо вместо кода MBR, либо вместо кода boot-сектора загрузочного диска (обычно диска C:), либо модифицирует адрес активного boot-сектора в таблице разделов диска (Disk Partition Table), расположенной в MBR винчестера.

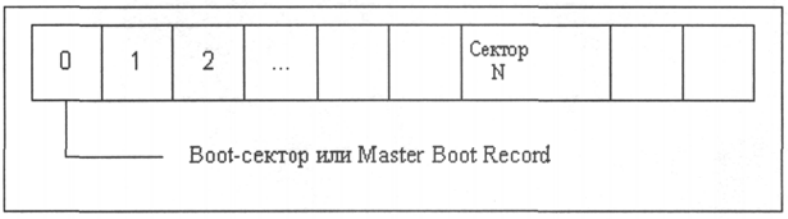


Рис. 3.4. **Незараженный диск**

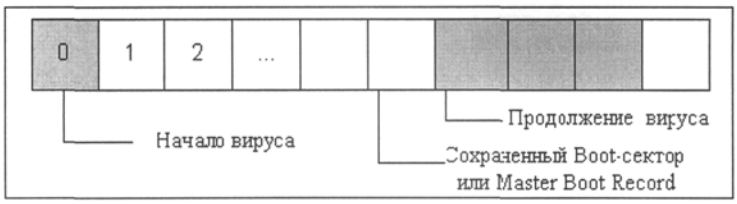


Рис. 3.5. **Зараженный диск (подмена boot/MBR)**

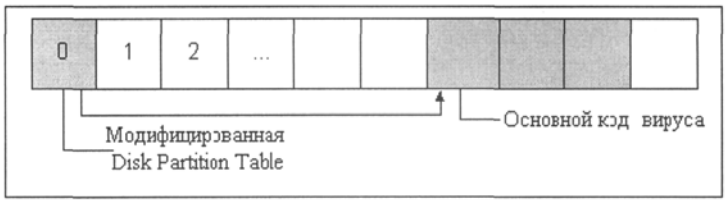


Рис. 3.6. **Зараженный диск (подмена активного boot-сектора в Disk Partition Table)**

При инфицировании диска вирус в большинстве случаев переносит оригинальный boot-сектор (или MBR) в какой-либо другой сектор диска (например, в первый свободный). Если длина вируса больше длины сектора, то в заражаемый сектор помещается первая часть вируса, остальные части размещаются в других секторах (например, в первых свободных).

Макровирусы

Наибольшее распространение получили макровирусы для Microsoft Office (Word, Excel и PowerPoint), хранящих информацию в формате OLE2 (Object Linking and Embedding). Вирусы в прочих приложениях достаточно редки.

Физическое расположение вируса внутри файла MS Office зависит от его формата, который в случае продуктов Microsoft чрезвычайно сложен – каждый файл-документ: Word, Office или таблица Excel – представляют собой последовательность блоков данных (каждый из которых также имеет свой формат), объединенных между собой при помощи большого количества служебных данных. По причине такой сложности форматов файлов Word, Excel и Office представить расположение макровируса в файле можно лишь схематично:

Рис. 3.7. **Расположение макровируса в файле**

При работе с документами и таблицами MS Office выполняет различные действия: открывает документ, сохраняет, печатает, закрывает и т.д. При этом MS Word, например, ищет и выполняет соответствующие «встроенные макросы» – при сохранении файла по команде File/Save вызывается макрос FileSave, при сохранении по команде File/SaveAs – FileSaveAs, при печати документов – FilePrint и т.д., если, конечно, таковые макросы определены.

Существует также несколько «автомакросов», автоматически вызываемых при различных условиях. Например, при открытии документа MS Word проверяет его на наличие макроса AutoOpen. Если такой макрос присутствует, то Word выполняет его. При закрытии

документа Word выполняет макрос AutoClose, при запуске Word вызывается макрос AutoExec, при завершении работы – AutoExit, при создании нового документа – AutoNew. Автоматически (т.е. без участия пользователя) выполняются также макросы/функции, ассоциированные с какой-либо клавишей либо моментом времени или датой, т.е. MS Word/Excel вызывают макрос/функцию при нажатии на какую-либо конкретную клавишу (или комбинацию клавиш) либо при достижении какого-либо момента времени.

Макровирусы, поражающие файлы MS Office, как правило, пользуются одним из перечисленных выше приемов – в вирусе либо присутствует авто-макрос (авто-функция), либо переопределен один из стандартных системных макросов (ассоциированный с каким-либо пунктом меню), либо макрос вируса вызывается автоматически при нажатии на какую-либо клавишу или комбинацию клавиш. Получив управление, макровирус переносит свой код в другие файлы, обычно в файлы, которые редактируются в данный момент. Реже макровирусы самостоятельно ищут другие файлы на диске.

Скрипт-вирусы

Следует отметить также скрипт-вирусы, являющиеся подгруппой файловых вирусов. Данные вирусы, написаны на различных скрипт-языках (VBS, JS, BAT, PHP и т.д.). Они либо заражают другие скрипт-программы (командные и служебные файлы MS Windows или Linux), либо являются частями многокомпонентных вирусов. Также, данные вирусы могут заражать файлы других форматов (например, HTML), если в них возможно выполнение скриптов.

3.3. Сетевые черви

К данной категории относятся программы, распространяющие свои копии по локальным и/или глобальным сетям с целью:

- проникновения на удаленные компьютеры;
- запуска своей копии на удаленном компьютере;
- дальнейшего распространения на другие компьютеры в сети.

Для своего распространения сетевые черви используют разнообразные компьютерные и мобильные сети: электронную почту, системы обмена мгновенными сообщениями, файлообменные (P2P) и IRC-сети, LAN, сети обмена данными между мобильными устройствами (телефонами, карманными компьютерами) и т. д.

Большинство известных червей распространяется в виде файлов: вложение в электронное письмо, ссылка на зараженный файл на каком-либо веб- или FTP-ресурсе в ICQ- и IRC-сообщениях, файл в каталоге обмена P2P и т. д.

Некоторые черви (так называемые «бесфайловые» или «пакетные» черви) распространяются в виде сетевых пакетов, проникают непосредственно в память компьютера и активизируют свой код.

Для проникновения на удаленные компьютеры и запуска своей копии черви используют различные методы: социальный инжиниринг (например, текст электронного письма, призывающий открыть вложенный файл), недочеты в конфигурации сети (например, копирование на диск, открытый на полный доступ), ошибки в службах безопасности операционных систем и приложений.

Некоторые черви обладают также свойствами других разновидностей вредоносного программного обеспечения. Например, некоторые черви содержат троянские функции или способны заражать выполняемые файлы на локальном диске, т. е. имеют свойство троянской программы и/или компьютерного вируса.

Классификация сетевых червей

Основным признаком, по которому типы червей различаются между собой, является способ распространения червя – каким способом он передает свою копию на удаленные компьютеры. Другими признаками различия червей между собой являются способы запуска копии червя на заражаемом компьютере, методы внедрения в систему, а также полиморфизм, «стелс» и прочие характеристики, присущие и другим типам вредоносного программного обеспечения (вирусам и троянским программам).

Email-Worm – почтовые черви

К данной категории червей относятся те из них, которые для своего распространения используют электронную почту. При этом червь отсылает либо свою копию в виде вложения в электронное письмо, либо ссылку на свой файл, расположенный на каком-либо сетевом ресурсе (например, URL на зараженный файл, расположенный на взломанном или хакерском веб-сайте).

В первом случае код червя активизируется при открытии (запуске) зараженного вложения, во втором – при открытии ссылки на зараженный файл. В обоих случаях эффект одинаков – активизируется код червя.

Для отправки зараженных сообщений почтовые черви используют различные способы. Наиболее распространены:

- прямое подключение к SMTP-серверу, используя встроенную в код червя почтовую библиотеку;
- использование сервисов MS Outlook;
- использование функций Windows MAPI.

Различные методы используются почтовыми червями для поиска почтовых адресов, на которые будут рассылаться зараженные письма. Почтовые черви:

- рассылают себя по всем адресам, обнаруженным в адресной книге MS Outlook;
- считывает адреса из адресной базы WAB;
- сканируют «подходящие» файлы на диске и выделяет в них строки, являющиеся адресами электронной почты;
- отсылают себя по всем адресам, обнаруженным в письмах в почтовом ящике (при этом некоторые почтовые черви «отвечают» на обнаруженные в ящике письма).

Многие черви используют сразу несколько из перечисленных методов. Встречаются также и другие способы поиска адресов электронной почты.

IM-Worm – черви, использующие Интернет-пейджеры

Известные компьютерные черви данного типа используют единственный способ распространения – рассылку на обнаруженные контакты (из контакт-листа) сообщений, содержащих URL, на файл, расположенный на каком-либо веб-сервере. Данный прием практически полностью повторяет аналогичный способ рассылки, использующийся почтовыми червями.

IRC-Worm – черви в IRC-каналах

У данного типа червей, как и у почтовых червей, существуют два способа распространения червя по IRC-каналам, повторяющие способы, описанные выше. Первый заключается в отсылке URL-ссылки на копию червя. Второй способ – отсылка зараженного файла какому-либо пользователю сети. При этом атакуемый пользователь должен подтвердить прием файла, затем сохранить его на диск и открыть (запустить на выполнение).

Net-Worm – прочие сетевые черви

Существуют прочие способы заражения удаленных компьютеров, например:

- копирование червя на сетевые ресурсы;
- проникновение червя на компьютер через уязвимости в операционных системах и приложениях;
- проникновение в сетевые ресурсы публичного использования;
- паразитирование на других вредоносных программах.

Первый способ заключается в том, что червь ищет удаленные компьютеры и копирует себя в каталоги, открытые на чтение и запись (если такие обнаружены). При этом черви данного типа или перебирают доступные сетевые каталоги, используя функции операционной системы, и/или случайным образом ищут компьютеры в глобальной сети, подключаются к ним и пытаются открыть их диски на полный доступ.

Для проникновения вторым способом черви ищут в сети компьютеры, на которых используется программное обеспечение, содержащее критические уязвимости. Для заражения уязвимых компьютеров червь посылает специально оформленный сетевой пакет или запрос (эксплойт уязвимости), в результате чего код (или часть кода) червя проникает на компьютер-жертву. Если сетевой пакет содержит только часть кода червя, он затем скачивает основной файл и запускает его на исполнение.

Отдельную категорию составляют черви, использующие для своего распространения веб- и FTP-серверы. Заражение происходит в два этапа. Сначала червь проникает в компьютер-сервер и необходимым образом модифицирует служебные файлы сервера (например, статические веб-страницы). Затем червь «ждет» посетителей, которые запрашивают информацию с зараженного сервера (например, открывают зараженную веб-страницу), и таким образом проникает на другие компьютеры в сети.

Существуют сетевые черви, паразитирующие на других червях и/или троянских программах удаленного администрирования (бэкдорах). Данные черви используют тот факт, что многие бэкдоры позволяют по определенной команде скачивать указанный файл и запускать его на локальном диске. То же возможно с некоторыми червями, содержащими бэкдор-процедуры. Для заражения удаленных компьютеров данные черви ищут другие компьютеры в сети и посылают на них команду скачивания и запуска своей копии. Если атакуемый компьютер оказывается уже зараженным «подходящей»

троянской программой, червь проникает в него и активизирует свою копию.

Следует отметить, что многие компьютерные черви используют более одного способа распространения своих копий по сетям, два и более методов атаки удаленных компьютеров.

P2P-Worm – черви для файлообменных сетей

Механизм работы большинства подобных червей достаточно прост – для внедрения в P2P-сеть червю достаточно скопировать себя в каталог обмена файлами, который обычно расположен на локальной машине. Всю остальную работу по распространению вируса P2P-сеть берет на себя – при поиске файлов в сети она сообщит удаленным пользователям о данном файле и предоставит весь необходимый сервис для скачивания файла с зараженного компьютера.

Существуют более сложные P2P-черви, которые имитируют сетевой протокол конкретной файлообменной системы и на поисковые запросы отвечают положительно – при этом червь предлагает для скачивания свою копию.

3.4. Троянские программы

В данную категорию входят программы, осуществляющие различные несанкционированные пользователем действия: сбор информации и ее передачу злоумышленнику, ее разрушение или злонамеренную модификацию, нарушение работоспособности компьютера, использование ресурсов компьютера.

Отдельные категории троянских программ наносят ущерб удаленным компьютерам и сетям, не нарушая работоспособность зараженного компьютера (например, троянские программы, разработанные для массированных DOS-атак на удаленные ресурсы сети).

Классификация троянских программ

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 троянская программа устанавливает себя в системе и затем следит за ней, при этом пользователю не выдается никаких сообщений о действиях ее в системе. Более того, ссылка на троянскую программу может отсутствовать в списке активных приложений. В результате пользователь может 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 вредоносных программ, 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 троянские программы от червей тот факт, что они распространяются по сети не самопроизвольно (как черви), а только по специальной команде.

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 троянской программы электронному адресу или адресам.

Существуют PSW-троянцы, которые сообщают и другую информацию о зараженном компьютере, например, информацию о системе (например, размер памяти и дискового пространства, версию операционной системы, тип используемого почтового клиента, IP-адрес и т. п.). Некоторые троянские программы 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 вредоносных программ

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

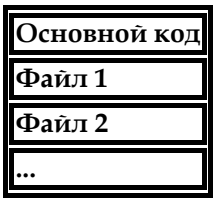
Информация об именах и расположении загружаемых программ содержится в коде и данных троянской программы или скачивается ей с управляющего Интернет-ресурса (обычно с веб-страницы).

Trojan-Dropper – инсталляторы 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 выделяет из своего файла остальные компоненты (файл 1, файл 2, ...), записывает их на диск и открывает их (запускает на выполнение).

Обычно один (или более) компонентов являются троянскими программами, и как минимум один компонент является обманом: программой-шуткой, игрой, картинкой или чем-то подобным. Обман должен 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 каком-либо файле 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 относятся многоцелевые троянские программы, например, те из них, которые одновременно шпионят за пользователем и предоставляют proxy-сервис удаленному злоумышленнику.

Rootkit – сокрытие присутствия в операционной системе

Понятие rootkit пришло к нам из UNIX. Первоначально это понятие использовалось для обозначения набора инструментов, применяемых для получения прав root.

Так как инструменты типа rootkit на сегодняшний день имеются и на других ОС (в том числе, на Windows), то следует признать подобное определение rootkit морально устаревшим и не отвечающим реальному положению дел.

Таким образом, rootkit – программный код или техника, направленная на сокрытие присутствия в системе заданных объектов (процессов, файлов, ключей реестра и т.д.).

ArcBomb – «бомбы» в архивах

Представляют собой архивы, специально оформленные таким образом, чтобы вызывать нештатное поведение архиваторов при попытке разархивировать данные – зависание или существенное замедление работы компьютера или заполнение диска большим количеством пустых данных. Особенно опасны архивные «бомбы» для файловых и почтовых серверов, если на сервере используется какая-либо система автоматической обработки входящей информации, – архивная «бомба» может просто остановить работу сервера.

Встречаются три типа подобных «бомб»: некорректный заголовок архива, повторяющиеся данные и одинаковые файлы в архиве.

Некорректный заголовок архива или испорченные данные в архиве могут привести к сбою в работе конкретного архиватора или алгоритма разархивирования при разборе содержимого архива.

Значительных размеров файл, содержащий повторяющиеся данные, позволяет заархивировать такой файл в архив небольшого размера (например, 5ГБ данных упаковываются в 200КБ RAR или в 480КБ ZIP-архив).

Огромное количество одинаковых файлов в архиве также практически не сказывается на размере архива при использовании специальных методов (например, существуют приемы упаковки 10^{100} одинаковых файлов в 30КБ RAR или 230КБ ZIP-архив).

Trojan-Notifier – оповещение об успешной атаке

Троянцы данного типа предназначены для сообщения 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.

3.5. Спам

Английское слово Spam произошло от словосочетания spiced ham – «ветчина со специями». Это название родилось в стенах американской компании Hormel, которая запатентовала его как торговую марку. История началась в 30-е гг., когда у компании скопился огромный запас второсортного мяса, и Hormel начала массированную маркетинговую кампанию по сбыту своих залежей. Новоиспеченный спам удалось в большом количестве продать американской армии, которая не смогла справиться с ним в одиночку и поспешила поделиться со странами-союзниками. Запасов хватило до конца сороковых, в послевоенной Англии спам являлся одним из немногих продуктов питания.

Если говорить о спаме как о массовой непрошенной рассылке по электронной почте, то его история берет свое начало 5 марта 1994 г. В этот день американская юридическая компания Canter and Siegel отправила по нескольким конференциям Usenet рекламную информацию о лотерее US Green Car.

Год от года объем спамерских рассылок растет, развиваются технологии рассылки спама, спам меняет свою тематику, стиль обращения к пользователям.

В последнее время характер спама становится все более криминальным, спамерские письма все чаще маскируются под служебные сообщения известных Интернет-сервисов и общественных организаций.

К основным видам спама относятся:

- влияние на котировки акций;
- фишинг;
- черный пиар;
- нигерийские письма;
- источник слухов;
- пустые письма.

Влияние на котировки акций

В настоящее время происходит стремительный рост количества рассылок предложений по инвестициям и игре на фондовой бирже. Этот спам предлагает информацию о динамике акций той или иной компании на фондовой бирже. Часто информация подается как «инсайдерская», случайно попавшая к данному отправителю письма. Фактически это попытка повлиять на предпочтения инвесторов и курс акций.

Фишинг

Фишинг (ловля на удочку) – это распространение поддельных сообщений от имени банков или финансовых компаний. Целью такого сообщения является сбор логинов, паролей и пин-кодов пользователей.

Обычно такой спам содержит текст с предупреждением об обнаруженных дырах в безопасности денежных операций «онлайн», в качестве меры предосторожности предлагается зайти на сайт и подтвердить/сменить пароль доступа к счету или пин-код банковской карты.

Естественно, ссылки в таком письме ведут не на настоящие банковские сайты, а на поддельные (спамерские) сайты. Ворованные коды/пароли можно использовать как для доступа к счету, так и для оплаты покупок в Интернет-магазинах. К настоящему времени спамеры перешли на новые технологии, и теперь фишинг-сообщения могут содержать «шпионский» скрипт, который перехватывает коды и/или пароли при вводе их на официальном банковском сайте и пересылает спамеру. Для активации скрипта достаточно просто открыть сообщение.

Пример типичного фишинг-сообщения.

> From: CityBank
> To: Иванов Иван Иванович
> Subject: Уведомление о получении платежа
> Уважаемый клиент!
> На Ваш текущий счет был получен перевод в иностранной валюте на сумму, превышающую USD 2.000. В соответствии с пользовательским соглашением CitiBankR, Вам необходимо подтвердить этот перевод для его успешного зачисления на Ваш счет. Для подтверждения платежа просим Вас зайти в программу управления Вашим счетом CitiBankR и следовать предложенным инструкциям.
> Если подтверждение не будет получено в течение 48 часов, платеж будет возвращен отправителю.
> Для входа в программу CitiBankR, нажмите сюда >>
> С уважением,
> Служба CitiBankR

Черный пиар

Это акция, цель которой – опорочить ту или иную фирму, компанию, политического кандидата и т.п. Эти рассылки имеют «негативный» характер, т.е. они агитируют не «за», а «против» (в письмах даются причины, почему не надо голосовать за того или иного кандидата).

Нигерийские письма

«Нигерийскими письмами» называют спам, написанный от имени реальных или вымышленных лиц, обычно – граждан стран с нестабильной экономической ситуацией, воспринимаемых публикой как рассадник коррупции. Первый зафиксированный спам такого типа рассылался от имени вымышленных нигерийских чиновников, именно поэтому он и получил название «нигерийских писем».

Автор такого письма обычно утверждает, что он располагает миллионами долларов, но они приобретены не совсем законными способами или же хранятся в обход закона. Например, это украденные иностранные инвестиции или гранты ООН. Дальше автор письма объясняет, что по этой причине он не может более держать деньги на счету в нигерийском банке, и что ему срочно требуется счет в зарубежном банке, куда можно перечислить «грязные» деньги. В качестве вознаграждения за помощь предлагается от 10% до 30% от заявленной в письме суммы. Идея мошенничества заключа-

ется в том, что доверчивый пользователь предоставит автору письма доступ к своему счету. Нетрудно предугадать результат – все деньги с этого счета будут сняты и уйдут в неизвестном направлении.

Источник слухов

Нежелательная корреспонденция бывает разных видов. Пользователи Рунета привыкли считать спамом сообщения, несущие более или менее ярко выраженную рекламную компоненту, но спам более разнообразен, чем это кажется на первый взгляд.

Организаторы данной рассылки инициируют первые несколько писем, содержащих эмоционально нагруженные сведения о потенциальной опасности (например, сведения о заражении питьевых источников, готовящемся теракте и т.п.) или просьбы о помощи жертвам стихийных бедствий.

Пользователи склонны доверчиво относиться к таким письмам и рассылают их копии дальше по спискам адресов в своих адресных книгах. По массовости такие пересылки оказываются вполне сопоставимыми со средней спамерской рассылкой, и уступают они только в скорости распространения.

Пример такого письма.

Здравствуйте

Сообщаемая мной информация – не слух, а официальная информация, разосланная ФСБ телеграммами по администрациям больниц, поликлиник, скорой помощи Москвы и Московской области (это стандартная процедура в случае угрозы вреда здоровью массе людей, т.к. данные службы должны быть в первую очередь в курсе). Информация получена от моего родственника, который как раз и работает в "скорой". Кроме того, соответствующие объявления уже развешены во многих лечебных учереждениях.

Информация:

«По имеющейся у спецслужб информации в настоящее время планируется террористическая акция по отравлению питьевой воды в Москве или в Московской области, биологическое (например, сальмонэлиоз) или химическое (например, цианид). К сожалению, точной информации по месту и характеру отравления нет. Но необходимо уделить особое внимание всем случаям отравлений, особенно массовым».

Меры предосторожности:

Пить только кипяченую воду (ни в коем случае сырую), желательно предварительно пропущенную через очищающие фильтры.

Предупредить всех.

Пустые письма

С 2003 г. у спамеров сложилась практика периодически проводить рассылки содержательно «пустых», т.е. нерекламных сообщений. Иногда это действительно пустые письма (нет контента), иногда письма с единственным словом «привет» или «тест», довольно часто рассылки содержат бессмысленные последовательности символов.

Такие рассылки преследуют сразу несколько целей. С одной стороны, это обычное тестирование нового или модифицированного спамерского программного обеспечения и т. п. С другой стороны, «пустые» рассылки довольно легко проходят антиспам-фильтры (не содержат спамерского контента), вызывая у пользователей понятное раздражение и скепсис по отношению к фильтрации спама.

Они также создают большую дополнительную нагрузку на каналы связи, что может выражаться в существенном снижении скорости обмена электронной корреспонденцией на время прохождения спамерской рассылки.

3.6. Хакерские утилиты и прочие вредоносные программы

К данной категории относятся:

- утилиты автоматизации создания вирусов, червей и троянских программ (конструкторы);
- программные библиотеки, разработанные для создания вредоносных программ;
- хакерские утилиты скрытия кода зараженных файлов от антивирусной проверки (шифровальщики файлов);
- «злые шутки», затрудняющие работу с компьютером;
- программы, сообщающие пользователю заведомо ложную информацию о своих действиях в системе;
- прочие программы, тем или иным способом намеренно наносящие прямой или косвенный ущерб данному или удаленным компьютерам.

Классификация прочих вредоносных программ

К прочим вредоносным относятся разнообразные программы, котрые не представляют угрозы непосредственно компьютеру, на котором исполняются, а разработаны для создания других вирусов

или троянских программ, организации DOS-атак на удаленные сервера, взлома других компьютеров и т. п.

DOS, DDOS – сетевые атаки

Программы данного типа реализуют атаки на удаленные сервера, посылая на них многочисленные запросы, что приводит к отказу в обслуживании, если ресурсы атакуемого сервера недостаточны для обработки всех поступающих запросов (DOS = Denial of Service).

DOS-программы реализуют атаку с одного компьютера с ведома пользователя. DDOS-программы (Distributed DOS) реализуют распределенные атаки с разных компьютеров, причем без ведома пользователя зараженного компьютера. Для этого DDOS-программа засылается любым способом на компьютер «жертв-посредников» и после запуска в зависимости от текущей даты или по команде от «хозяина» начинает DOS-атаку на указанный сервер в сети.

Некоторые компьютерные черви содержат в себе DOS-процедуры, атакующие сайты, которые по каким-либо причинам «невзлюбил» автор червя. Так, червь Codered 20 августа 2001 г. организовал успешную атаку на официальный сайт Президента США, а червь Mydoom.a 1 февраля 2004 г. «выключил» сайт SCO, производителя дистрибутивов UNIX.

Exploit, HackTool – взломщики удаленных компьютеров.

Хакерские утилиты данного класса предназначены для проникновения в удаленные компьютеры с целью дальнейшего управления ими (используя методы троянских программ типа «backdoor») или для внедрения во взломанную систему других вредоносных программ.

Хакерские утилиты типа «exploit» при этом используют уязвимости в операционных системах или приложениях, установленных на атакуемом компьютере.

Flooder – «замусоривание» сети

Данные хакерские утилиты используются для бесполезных сообщений каналов Интернета – IRC-каналов, компьютерных пейджинговых сетей, электронной почты и т. д.

Constructor – конструкторы вирусов и троянских программ

Конструкторы вирусов и троянских программ – это утилиты, предназначенные для изготовления новых компьютерных вирусов и троянских программ. 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, наличие или отсутствие самошифровки, противодействие отладчику, внутренние текстовые строки, выбрать эффекты, сопровождающие работу вируса, и т. п. Прочие конструкторы не имеют интерфейса и считывают информацию о типе вируса из конфигурационного файла.

Nuker – фатальные сетевые атаки

Утилиты, отправляющие специально оформленные запросы на атакуемые компьютеры в сети, в результате чего атакуемая система прекращает работу. Используют уязвимости в программном обеспечении и операционных системах, в результате чего сетевой запрос специального вида вызывает критическую ошибку в атакуемом приложении.

Bad-Joke, Hoax – злые шутки, введение пользователя в заблуждение

К ним относятся программы, которые не причиняют компьютеру какого-либо прямого вреда, однако выводят сообщения о том, что такой вред уже причинен, либо будет причинен при каких-либо условиях, либо предупреждают пользователя о несуществующей опасности. К «злым шуткам» относятся, например, 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. – в зависимости от чувства юмора автора такой программы.

FileCryptor, PolyCryptor – скрытие от антивирусных программ

Хакерские утилиты, использующиеся для шифрования других вредоносных программ с целью скрытия их содержимого от антивирусной проверки.

PolyEngine – полиморфные генераторы

Полиморфные генераторы 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 их авторами без ограничений в виде файла-архива. Основным файлом в архиве любого генератора является объектный модуль, содержащий этот генератор. Во всех встречавшихся генераторах этот модуль содержит внешнюю (external) функцию – вызов программы генератора.

VirTool

Утилиты, предназначенные для облегчения написания компьютерных вирусов и для их изучения в хакерских целях.

3.7. Кто и почему создает вредоносные программы

Основная масса вирусов и троянских программ в прошлом создавалась студентами и школьниками, которые только что изучили язык программирования, хотели попробовать свои силы, но не смогли найти для них более достойного применения. Отраден тот факт, что значительная часть подобных вирусов их авторами не распространялась и вирусы через некоторое время умирали сами вместе с дисками, на которых хранились. Такие вирусы писались и пишутся по сей день только для самоутверждения их авторов.

Вторую группу создателей вирусов также составляют молодые люди (чаще всего – студенты), которые еще не полностью овладели искусством программирования. Единственная причина, толкающая их на написание вирусов, – это комплекс неполноценности, который компенсируется компьютерным хулиганством. Жизнь подобных вирусописателей стала заметно проще с развитием Интернета и появлением многочисленных веб-сайтов, ориентированных на обучение написанию компьютерных вирусов. На подобных веб-ресурсах можно найти подробные рекомендации по методам проникновения в систему, приемам скрытия от антивирусных программ, способам дальнейшего распространения вируса. Часто здесь же можно найти готовые исходные тексты, в которые надо всего лишь внести минимальные «авторские» изменения и откомпилировать рекомендуемым способом.

«Хулиганские» вирусы в последние годы становятся все менее и менее актуальными – за исключением тех случаев, когда такие

вредоносные программы вызвали глобальные сетевые и почтовые эпидемии. На текущий момент доля подобных вирусов и троянских программ занимает не более 10%, заносимого в антивирусные базы данных. Оставшиеся 90% гораздо более опасны, чем просто вирусы.

Став старше и опытнее, многие из подобных вирусописателей попадают в третью, наиболее опасную группу, которая создает и запускает в мир профессиональные вирусы. Эти тщательно продуманные и отлаженные программы создаются профессиональными, часто очень талантливыми программистами. Такие вирусы нередко используют достаточно оригинальные алгоритмы проникновения в системные области данных, ошибки в системах безопасности операционных сред, социальный инжиниринг и прочие хитрости.

Отдельно стоит четвертая группа авторов вирусов – исследователи, довольно сообразительные программисты, которые занимаются изобретением принципиально новых методов заражения, скрытия, противодействия антивирусам и т. д. Они же придумывают способы внедрения в новые операционные системы. Эти программисты пишут вирусы не ради собственно вирусов, а скорее ради исследования. Часто авторы подобных вирусов не распространяют свои творения, однако активно пропагандируют свои идеи через многочисленные Интернет-ресурсы, посвященные созданию вирусов. При этом опасность, исходящая от таких «исследовательских» вирусов, тоже весьма велика – попав в руки «профессионалов» из предыдущей группы, эти идеи очень быстро появляются в новых вирусах.

Мелкое воровство

С появлением и популяризацией платных Интернет-сервисов (почта, WWW, хостинг) компьютерный андеграунд начинает проявлять повышенный интерес к получению доступа в сеть за чужой счет, т. е. посредством кражи чьего-либо логина и пароля (или нескольких логинов/паролей с различных пораженных компьютеров) путем применения специально разработанных троянских программ.

В начале 1997 г. зафиксированы первые случаи создания и распространения троянских программ, ворующих пароли доступа к системе AOL. В 1998 г., с распространением Интернет-услуг в Европе и России, аналогичные троянские программы появляются и для других Интернет-сервисов. До сих пор троянцы, ворующие пароли к dial-up, пароли к AOL, коды доступа к другим сервисам, составляют заметную часть ежедневных «поступлений» в лаборатории антивирусных компаний всего мира.

Троянские программы данного типа, как и вирусы, обычно создаются молодыми людьми, у которых нет средств для оплаты Интернет-услуг. Характерен тот факт, что по мере удешевления Интернет-сервисов уменьшается и удельное количество таких троянских программ.

«Мелкими воришками» также создаются троянские программы других типов: ворующие регистрационные данные и ключевые файлы различных программных продуктов (часто – сетевых игр), использующие ресурсы зараженных компьютеров в интересах своего «хозяина» и т. п.

Криминальный бизнес

Наиболее опасную категорию вирусописателей составляют хакеры-одиночки или группы хакеров, которые осознанно или неосознанно создают вредоносные программы с единственной целью: получить чужие деньги (рекламируя что-либо или просто воруя их), ресурсы зараженного компьютера (опять-таки, ради денег – для обслуживания спам-бизнеса или организации DOS-атак с целью дальнейшего шантажа).

Обслуживание рекламного и спам-бизнеса – один из основных видов деятельности таких хакеров. Для рассылки спама ими создаются специализированные троянские proxy-серверы, которые затем внедряются в десятки тысяч компьютеров. Затем такая сеть «зомби-машин» поступает на черный Интернет-рынок, где приобретается спамерами. Для внедрения в операционную систему и дальнейшего обновления принудительной рекламы создаются утилиты, использующие откровенно хакерские методы: незаметную инсталляцию в систему, разнообразные маскировки (чтобы затруднить удаление рекламного софта), противодействие антивирусным программам.

Вторым видом деятельности подобных вирусописателей является создание, распространение и обслуживание троянских программ-шпионов, направленных на воровство денежных средств с персональных (а если повезет – то и с корпоративных) «электронных кошельков» или с обслуживаемых через Интернет банковских счетов. Троянские программы данного типа собирают информацию о кодах доступа к счетам и пересылают ее своему «хозяину».

Третьим видом криминальной деятельности этой группы является Интернет-рэкет, т. е. организация массированной DOS-атаки на один или несколько Интернет-ресурсов с последующим требованием денежного вознаграждения за прекращение атаки. Обычно

под удар попадают Интернет-магазины, букмекерские конторы – т. е. компании, бизнес которых напрямую зависит от работоспособности веб-сайта компании.

Вирусы, созданные этой категорией вирусописателей, становятся причиной многочисленных вирусных эпидемий, инициированных для массового распространения и установки описанных выше троянских компонент.

Контрольные вопросы

1. Какие программы являются вредоносными.
2. Условия существования вредоносных программ.
3. Причины появления вредных программ.
4. Классические компьютерные вирусы.
5. Классификация классических вирусов.
6. Способы заражения компьютерными вирусами.
7. Внедрение вируса в начало файла.
8. Внедрение вируса в конец файла.
9. Внедрение вируса в середину файла.
10. Вирусы без точки входа.
11. Загрузочные вирусы.
12. Макровирусы.
13. Сетевые черви.
14. Классификация сетевых червей.
15. Email-Worm – почтовые черви.
16. IM-Worm – черви, использующие Интернет-пейджеры.
17. IRC-Worm – черви в IRC-каналах.
18. Net-Worm – прочие сетевые черви.
19. P2P-Worm – черви для файлообменных сетей.
20. Троянские программы.
21. Классификация троянских программ.
22. Backdoor – троянские утилиты удаленного администрирования.
23. Trojan-PSW – воровство паролей.
24. Trojan-Clicker – Интернет-кликеры.
25. Trojan-Downloader – доставка вредоносных программ.
26. Trojan-Dropper – инсталляторы вредоносных программ.
27. Trojan-Proxy – троянские прокси-сервера.
28. Trojan-Spy – шпионские программы.
29. Trojan – прочие троянские программы.

30. Rootkit – сокрытие присутствия в операционной системе.
31. ArcBomb – «бомбы» в архивах.
32. Trojan-Notifier – оповещение об успешной атаке.
33. Спам.
34. Основные виды спама.
35. Хакерские утилиты и прочие вредоносные программы.
36. Основные виды хакерских утилит и прочих вредоносных программ.
37. DOS, DDOS – сетевые атаки.
38. Exploit, HackTool – взломщики удаленных компьютеров.
39. Flooder – «замусоривание» сети.
40. Constructor – конструкторы вирусов и троянских программ.
41. Nuker – фатальные сетевые атаки.
42. Bad-Joke, Hoax – злые шутки, введение пользователя в заблуждение.
43. FileCryptor, PolyCryptor – скрытие от антивирусных программ.
44. PolyEngine – полиморфные генераторы.
45. Кто и почему создает вредоносные программы.

Тесты

1. По среде обитания классические вирусы разделяются:

1. на паразитические;
2. на компаньоны;
3. на файловые;
4. на ссылки;
5. на перезаписывающие.

2. По среде обитания классические вирусы разделяются:

1. на загрузочные;
2. на компаньоны;
3. на паразитические;
4. на ссылки;
5. на перезаписывающие.

3. По среде обитания классические вирусы разделяются:

1. на ссылки;
2. на компаньоны;
3. на паразитические;

4. на макровирусы;
5. на перезаписывающие.

4. По среде обитания классические вирусы разделяются:
1. на ссылки;
2. на компаньоны;
3. на скриптовые;
4. на паразитические;
5. на перезаписывающие.

5. По способу заражения классические вирусы разделяются:
1. на файловые;
2. на загрузочные;
3. на макровирусы;
4. на скриптовые;
5. на перезаписывающие.

6. По способу заражения классические вирусы разделяются:
1. на файловые;
2. на паразитические;
3. на макровирусы;
4. на скриптовые;
5. на загрузочные.

7. По способу заражения классические вирусы разделяются:
1. на компаньоны;
2. на файловые;
3. на макровирусы;
4. на скриптовые;
5. на загрузочные.

8. По способу заражения классические вирусы разделяются:
1. на скриптовые;
2. на файловые;
3. на макровирусы;
4. на ссылки;
5. на загрузочные.

9. Сетевой червь отсылает либо свою копию в виде вложения в электронное письмо, либо ссылку на свой файл, расположенный на каком-либо сетевом ресурсе:

1. IM-Worm;
2. IRC-Worm;
3. Net-Worm;
4. P2P-Worm;
5. Email-Worm.

10. Сетевые черви используют способ распространения – рассылку на обнаруженные контакты (из контакт-листа) сообщений, содержащих URL, на файл, расположенный на каком-либо веб-сервере:

1. IM-Worm;
2. IRC-Worm;
3. Net-Worm;
4. P2P-Worm;
5. Email-Worm.

11. Сетевые черви распространяются двумя способами по IRC-каналам. Первый заключается в отсылке URL-ссылки на копию червя. Второй способ – отсылка зараженного файла какому-либо пользователю сети. При этом атакуемый пользователь должен подтвердить прием файла, затем сохранить его на диск и открыть:

1. IM-Worm;
2. IRC-Worm;
3. Net-Worm;
4. P2P-Worm;
5. Email-Worm.

12. Сетевой червь ищет удаленные компьютеры и копирует себя в каталоги, открытые на чтение и запись, при этом червь или перебирает доступные сетевые каталоги, используя функции операционной системы, и/или случайным образом ищет компьютеры в глобальной сети, подключается к ним и пытается открыть их диски на полный доступ:

1. IM-Worm;
2. IRC-Worm;
3. Net-Worm;
4. P2P-Worm;
5. Email-Worm.

13. Сетевые черви ищут в сети компьютеры, на которых используется программное обеспечение, содержащее уязвимости. Для заражения уязвимых компьютеров червь посылает специально оформленный сетевой пакет или запрос, в результате чего код червя проникает на компьютер-жертву:

1. IM-Worm;
2. IRC-Worm;
3. Net-Worm;
4. P2P-Worm;
5. Email-Worm.

14. Для внедрения в сеть сетевому червю достаточно скопировать себя в каталог обмена файлами, который обычно расположен на локальном компьютере. Всю остальную работу по распространению вируса сеть берет на себя – при поиске файлов в сети она сообщит удаленным пользователям о данном файле и предоставит весь необходимый сервис для скачивания файла с зараженного компьютера:

1. IM-Worm;
2. IRC-Worm;
3. Net-Worm;
4. P2P-Worm;
5. Email-Worm.

15. Сетевой червь имитирует сетевой протокол конкретной файлообменной системы и на поисковые запросы отвечает положительно – при этом червь предлагает для скачивания свою копию:

1. IM-Worm;
2. IRC-Worm;
3. Net-Worm;
4. P2P-Worm;
5. Email-Worm.

16. Троянские утилиты удаленного администрирования:

1. Trojan-PSW;
2. Trojan-Clicker;
3. Backdoor;
4. Trojan-Downloader;
5. Trojan-Dropper.

17. Троянские программы для воровства паролей:
1. Trojan-PSW;
2. Trojan-Clicker;
3. Trojan-Proxy;
4. Trojan-Downloader;
5. Trojan-Dropper.

18. Троянские программы для доставки вредоносных программ:
1. Trojan-PSW;
2. Trojan-Clicker;
3. Trojan-Proxy;
4. Trojan-Downloader;
5. Trojan-Dropper.

19. Троянские программы инсталляторы вредоносных программ:
1. Trojan-PSW;
2. Trojan-Clicker;
3. Trojan-Proxy;
4. Trojan-Downloader;
5. Trojan-Dropper.

20. Троянские шпионские программы:
1. Trojan-PSW;
2. Trojan-Spy;
3. Trojan-Proxy;
4. Trojan-Downloader;
5. Trojan-Dropper.

21. Троянские программы, применяемые для организации несанкционированных обращений к Интернет-ресурсам:
1. Trojan-PSW;
2. Trojan-Spy;
3. Trojan-Clicker;
4. Trojan-Downloader;
5. Trojan-Dropper.

22. Троянские программы, скрытно осуществляющие анонимный доступ к различным Интернет-ресурсам, обычно используются для рассылки спама:
1. Trojan-PSW;
2. Trojan-Spy;

3. Trojan-Proxy;
4. Trojan-Downloader;
5. Trojan-Dropper.

23. Троянские программы, предназначенные для оповещение об успешной атаке:

1. Trojan-PSW;
2. Trojan-Spy;
3. Trojan-Proxy;
4. Trojan-Notifier;
5. Trojan-Dropper.

24. Спам распространяет поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей:

1. черный пиар;
2. фишинг;
3. нигерийские письма;
4. источник слухов;
5. пустые письма.

25. Спам, который имеет цель опорочить ту или иную фирму, компанию, политического кандидата и т.п:

1. черный пиар;
2. фишинг;
3. нигерийские письма;
4. источник слухов;
5. пустые письма.

26. Спам, написанный от имени реальных или вымышленных лиц, обычно граждан стран с нестабильной экономической ситуацией, воспринимаемых публикой как рассадник коррупции:

1. черный пиар;
2. фишинг;
3. нигерийские письма;
4. источник слухов;
5. пустые письма.

27. Спам инициирует письма, содержащие сведения о потенциальной опасности или просьбы о помощи жертвам стихийных бедствий:

1. черный пиар;

2. фишинг;
3. нигерийские письма;
4. источник слухов;
5. пустые письма.

28. Спам периодически проводит рассылки нерекламных сообщений:

1. черный пиар;
2. фишинг;
3. нигерийские письма;
4. источник слухов;
5. пустые письма.

Тема 4.

Защита от компьютерных вирусов

Изучив тему 4, студент должен:
знать:

- откуда проникают в компьютерную систему «компьютерные вирусы»;
- правила защиты от «компьютерных вирусов»;

уметь:

- выбрать антивирусную программу;
- правильно использовать антивирусную программу;
- восстанавливать пораженные «компьютерными вирусами» объекты.

акцентировать внимание на понятиях:

- антивирусная программа, сканеры, CRC-сканеры, мониторы, иммунизаторы.

Содержание темы (дидактические единицы и их характеристика):

Основные правила защиты от «компьютерных вирусов». Обзор антивирусных программ. Методика использования антивирусных программ. Восстановление пораженных «компьютерными вирусами» объектов.

Цели и задачи изучения темы: Получение знаний о правилах защиты от «компьютерных вирусов». Получение навыков в выборе антивирусных программ. Получение навыков по восстановлению пораженных «компьютерными вирусами» объектов.

Порядок изучения темы

Распределение бюджета времени по теме:

- количество часов, отведенных на практические занятия, из них в компьютерной аудитории – 4/4;
- количество часов, отведенных на самостоятельную работу, – 16.

Виды самостоятельной работы студентов:

− изучение учебного пособия «Информационная безопасность»;
− подготовка к участию в форуме по теме «Антивирусные программы»;
− изучение дополнительной литературы;
− выполнение тестовых заданий по теме.

Методические указания по изучению вопросов темы

При изучении учебных вопросов:

- изучить тему 4 по учебному пособию «Информационная безопасность»;
- принять участие в форуме по теме «Защита от компьютерных вирусов»;
- изучить дополнительные материалы.

При изучении темы необходимо:

- *читать литературу*:

1. Информационная безопасность: Уч. Пособие. – М.: МЭСИ, 2007.
2. Касперский Е.В. Компьютерные вирусы: что это такое и как с ними бороться. – М.: СК Пресс, 1998.
3. Фролов А.В., Фролов Г.В. Осторожно: компьютерные вирусы. – М.: Диалог-МИФИ, 1996.

- *посетить сайты:* www.viruslist.com, www.subscribe.ru, www.new.russian.net.ru, www.dials.ru.

Вопросы темы

4.1. Признаки заражения компьютера.
4.2. Источники компьютерных вирусов.
4.3. Основные правила защиты.
4.4. Антивирусные программы.

4.1. Признаки заражения компьютера

Непрофессионалу сложно обнаружить присутствие вирусов на компьютере, поскольку они умело маскируются среди обычных файлов. Рассмотрим признаки заражения компьютера, а также способы восстановления данных после вирусной атаки и меры по предотвращению их поражения вредоносными программами.

Можно отметить ряд признаков, свидетельствующих о заражении компьютера вредоносными программами:

- вывод на экран непредусмотренных сообщений или изображений;
- подача непредусмотренных звуковых сигналов;
- неожиданное открытие и закрытие лотка CD-ROM-устройства;
- произвольный, без вашего участия, запуск на компьютере каких-либо программ;
- при наличии на вашем компьютере межсетевого экрана, появление предупреждений о попытке какой-либо из программ вашего компьютера выйти в Интернет, хотя вы это не инициировали.

Если вы замечаете, что с компьютером происходит подобное, то с большой степенью вероятности можно предположить, что ваш компьютер поражен вирусом.

Кроме того, есть некоторые характерные признаки поражения вирусом через электронную почту:

- друзьям или знакомым приходят сообщения от вас, которые вы не отправляли;
- в почтовом ящике находится большое количество сообщений без обратного адреса и заголовка.

Следует отметить, что не всегда такие признаки вызываются присутствием вирусов. Иногда они могут быть следствием других причин. Например, в случае с почтой зараженные сообщения могут рассылаться с вашим обратным адресом, но не с вашего компьютера.

Имеются косвенные признаки заражения компьютера:

- частые зависания и сбои в работе компьютера;
- медленная работа компьютера при запуске программ;
- невозможность загрузки операционной системы;
- исчезновение файлов и каталогов или искажение их содержимого;

- частое обращение к жесткому диску (часто мигает лампочка на системном блоке);
- Интернет-браузер «зависает» или ведет себя неожиданным образом (например, окно программы невозможно закрыть).

В 90% случаев наличие косвенных признаков вызвано сбоем в аппаратном или программном обеспечении. Несмотря на то, что подобные симптомы с малой вероятностью свидетельствуют о заражении, при их появлении рекомендуется провести полную проверку вашего компьютера установленной на нем антивирусной программой.

Действия при появлении признаков заражения вредоносной программой.

Если вы заметили, что ваш компьютер ведет себя «подозрительно»:

1. Не поддаваться панике.
2. Отключите компьютер от Интернета.
3. Отключите компьютер от локальной сети.
4. Если признак заражения состоит в том, что вы не можете загрузиться с жесткого диска компьютера (компьютер выдает ошибку, когда вы его включаете), попробуйте загрузиться в режиме защиты от сбоев или с диска аварийной загрузки Windows, который вы создавали при установке операционной системы на компьютер.
5. Прежде чем предпринимать какие-либо действия, сохраните результаты вашей работы на внешний съемный носитель.
6. Установите полную версию антивирусной программы.
7. Получите последние обновления антивирусных баз.
8. Установите рекомендуемый уровень настроек антивирусной программы.
9. Запустите полную проверку компьютера антивирусной программой.

4.2. Источники компьютерных вирусов

Компьютерные вирусы могут проникнуть в компьютер из следующих источников:

- глобальные сети – электронная почта;
- электронные конференции;

- локальные сети;
- пиратское программное обеспечение;
- компьютеры общего пользования;
- ремонтные службы.

Глобальные сети – электронная почта

Основным источником вирусов на сегодняшний день является глобальная сеть Интернет. Наибольшее число заражений вирусом происходит при обмене письмами в форматах Word/Office. Пользователь зараженного макровирусом редактора, сам того не подозревая, рассылает зараженные письма адресатам, а они, в свою очередь, отправляют новые зараженные письма и т. д.

Предположим, что пользователь ведет переписку с пятью адресатами, каждый из которых также переписывается с пятью адресатами. После посылки зараженного письма все пять компьютеров, получивших его, оказываются зараженными (рис. 4.1).

Затем с каждого вновь зараженного компьютера отправляется еще пять писем. Одно уходит назад на уже зараженный компьютер, а четыре – новым адресатам (рис. 4.2).

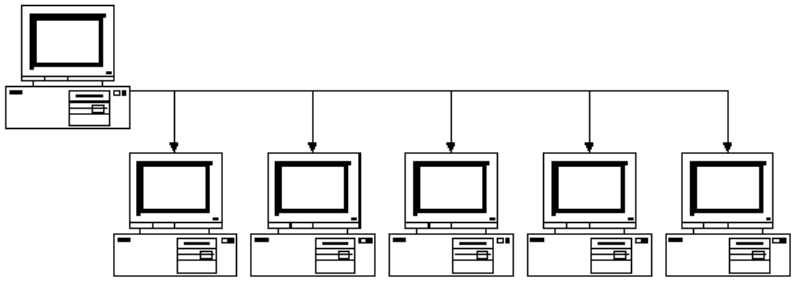


Рис. 4.1. **Заражение первых пяти компьютеров**

Таким образом, на втором уровне рассылки заражено уже 1+5+20=26 компьютеров (рис. 4.2). Если адресаты сети обмениваются письмами раз в день, то к концу рабочей недели (за 5 дней) зараженными окажутся как минимум 1+5+20+80+320=426 компьютеров. Нетрудно подсчитать, что за 10 дней заразится более ста тысяч компьютеров! Причем каждый день их количество будет учетверяться.

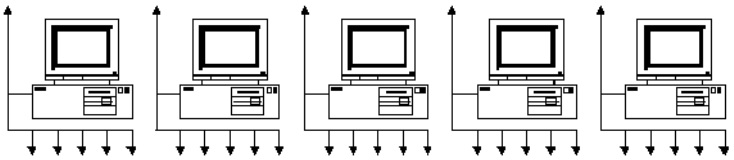


Рис. 4.2. **Второй уровень заражения**

Описанный случай распространения вируса является наиболее часто регистрируемым антивирусными компаниями. Нередки случаи, когда зараженный файл-документ или таблица Excel по причине недосмотра попадает в списки рассылки коммерческой информации какой-либо крупной компании – в этом случае страдают не пять, а сотни или даже тысячи абонентов таких рассылок, которые затем разошлют зараженные файлы десяткам тысячам своих абонентов.

Электронные конференции

Файл-серверы общего пользования и электронные конференции также служат одним из основных источников распространения вирусов. Зараженные файлы рассылаются по нескольким конференциям одновременно, и эти файлы маскируются под новые версии какого-либо ПО (иногда под новые версии антивирусов).

В случае массовой рассылки вируса пораженными практически одновременно могут оказаться тысячи компьютеров.

Локальные сети

Третий путь быстрого заражения – локальные сети. Если не принимать необходимых мер защиты, то зараженная рабочая станция при входе в сеть заражает один или несколько служебных файлов на сервере (рис. 4.3).

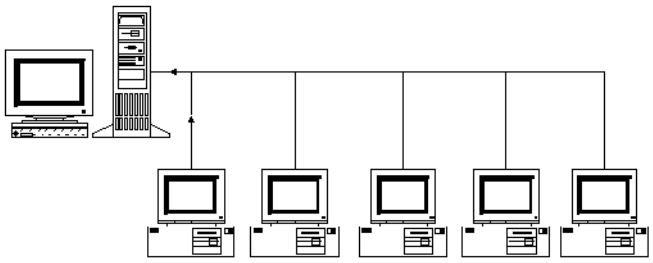


Рис. 4.3. **Заражение служебных файлов на сервере**

На следующий день пользователи при входе в сеть запускают зараженные файлы с сервера и таким образом вирус получает доступ на незараженные компьютеры.

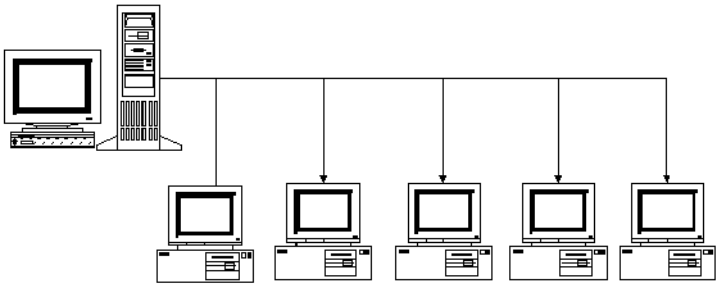


Рис. 4.4. **Заражение на компьютере**

Пиратское программное обеспечение

Нелегальные копии программного обеспечения являются одной из основных зон риска. Часто пиратские копии на содержат файлы, зараженные самыми разнообразными типами вирусов.

Компьютеры общего пользования

Опасность представляют компьютеры, установленные в учебных заведениях. Студент может принести на своем съемном диске компьютерный вирус и заразить учебный компьютер. Этот вирус разнесется по всем учебным компьютерам локальной сети. При скачивании данных с учебного компьютера локальной сети вирусом будут заражены съемные диски других студентов, которые заразят свои домашние компьютеры и компьютеры своих товарищей.

По такой цепочке компьютерные вирусы могут попасть в компьютерную сеть фирмы, где работают родители.

Ремонтные службы

Вполне реально заражение компьютера вирусом при его ремонте или профилактическом осмотре. Ремонтники – тоже люди, и некоторым из них свойственно наплевательское отношение к элементарным правилам компьютерной безопасности. Однажды забыв закрыть защиту от записи на одном из своих гибких дисков, такой ремонтник довольно быстро разнесет заразу по машинам своей клиентуры и, скорее всего, потеряет ее (клиентуру).

4.3. Основные правила защиты

Правило первое. Крайне осторожно относитесь к документам Word/Excel, которые получаете из глобальных сетей. Перед тем как запустить файл на выполнение или открыть документ/таблицу, обязательно проверьте их на наличие вирусов.

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

Значительно уменьшается риск заражения компьютерной сети при использовании компьютеров без съемных носителей информации.

Желательно также, перед тем как запустить новое ПО, попробовать его на компьютере, не подключенном к общей локальной сети.

Правило третье. Лучше покупать дистрибутивные копии программного обеспечения у официальных продавцов, чем бесплатно или почти бесплатно копировать их из других источников или покупать пиратские копии.

Как следствие из этого правила вытекает необходимость хранения дистрибутивных копий ПО (в том числе копий операционной системы), причем копии желательно хранить на защищенных от записи съемных дисках.

Пользуйтесь только хорошо зарекомендовавшими себя источниками программ и прочих файлов.

Правило четвертое. Периодически сохраняйте файлы, с которыми ведется работа, на внешнем носителе, т. е. делайте резервные копии. Затраты на копирование файлов, содержащих исходные тексты программ, базы данных, документацию, значительно меньше затрат на восстановление этих файлов при проявлении вирусом агрессивных свойств или при сбое компьютера.

4.4. Антивирусные программы

Количество и разнообразие вирусов велико, и чтобы их быстро и эффективно обнаружить, антивирусная программа должна отвечать следующим параметрам.

Стабильность и надежность работы. Этот параметр, без сомнения, является определяющим – даже самый лучший антивирус окажется совершенно бесполезным, если он не сможет нормально функционировать на компьютере, если в результате какого-либо сбоя в работе программы процесс проверки компьютера не пройдет до конца. Тогда всегда есть вероятность того, что какие-то зараженные файлы остались незамеченными.

Размеры вирусной базы программы. С учетом постоянного появления новых вирусов база данных должна регулярно обновляться. Сюда же следует отнести и возможность программы определять разнообразные типы вирусов, и умение работать с файлами различных типов (архивы, документы). Немаловажным также является наличие резидентного монитора, осуществляющего проверку всех новых файлов «на лету» (то есть автоматически, по мере их записи на диск).

Скорость работы программы, наличие дополнительных возможностей типа алгоритмов определения даже неизвестных программе вирусов (эвристическое сканирование). Сюда же следует отнести возможность восстанавливать зараженные файлы, не стирая их с жесткого диска, а только удалив из них вирусы. Немаловажным является также процент ложных срабатываний программы (ошибочное определение вируса).

Многоплатформенность (наличие версий программы под различные операционные системы. Антивирусная программа для крупной организации просто обязана поддерживать все распространенные операционные системы. Кроме того, при работе в сети немаловажным является наличие серверных функций, предназначенных для административной работы, а также возможность работы с различными видами серверов.

Виды антивирусных программ

На сегодняшний день перечень доступных антивирусных программ весьма обширен. Они различаются как по цене (от весьма дорогих до абсолютно бесплатных), так и по своим функциональным возможностям. Наиболее мощные (и, как правило, наиболее дорогие) антивирусные программы представляют собой на самом деле пакеты специализированных утилит, способных при совместном их использовании поставить заслон практически любому виду вредоносных программ.

Типовой перечень функций, которые способны выполнять антивирусные программы:

- сканирование памяти и содержимого дисков по расписанию;

- сканирование памяти компьютера, а также записываемых и читаемых файлов в реальном режиме времени с помощью резидентного модуля;
- выборочное сканирование файлов с измененными атрибутами;
- распознавание поведения, характерного для компьютерных вирусов;
- блокировка и/или удаление выявленных вирусов;
- восстановление зараженных информационных объектов;
- принудительная проверка подключенных к корпоративной сети компьютеров;
- удаленное обновление антивирусного программного обеспечения и баз данных с информацией о вирусах, в том числе автоматическое обновление баз данных по вирусам через Интернет;
- фильтрация трафика Интернета на предмет выявления вирусов в передаваемых программах и документах;
- выявление потенциально опасных Java-апплетов и модулей ActiveX;
- ведение протоколов, содержащих информацию о событиях, касающихся антивирусной защиты.

К наиболее мощным и популярным на сегодняшний день в России антивирусным пакетам относятся:

- Doctor Web (в документации часто именуется более кратко – Dr Web) – программа российской компании;
- Антивирус Касперского (в документации именуется более кратко – AVP) – разработка еще одной российской фирмы
- Norton AntiVirus корпорации Symantec;
- McAfee VirusScan компании Network Associates;
- Panda Antivirus.
- Nod32 Antivirus.

Популярность перечисленных выше пакетов обусловлена прежде всего тем, что в них реализован комплексный подход к борьбе с вредоносными программами. То есть, установив такой пакет, вы избавляетесь от необходимости использовать какие-либо дополнительные антивирусные средства.

Последние версии антивирусных пакетов содержат в своем составе также и средства борьбы с вредоносными программами, проникающими из сети (в первую очередь из Интернета). Так какие же,

собственно, существуют технологии выявления и нейтрализации компьютерных вирусов?

Специалисты в области антивирусной технологии выделяют пять типов антивирусов: сканеры, мониторы, ревизоры изменений, иммунизаторы и поведенческие блокираторы.

Сканер.

Принцип работы антивирусного сканера состоит в том, что он просматривает файлы, оперативную память и загрузочные секторы дисков на предмет наличия вирусных масок, то есть уникального программного кода вируса. Вирусные маски (описания) известных вирусов содержатся в антивирусной базе данных сканера, и если он встречает программный код, совпадающий с одним из этих описаний, то он выдает сообщение об обнаружении соответствующего вируса.

Программы-детекторы

Программы-детекторы обеспечивают поиск и обнаружение вирусов в оперативной памяти, на внешних носителях, и при обнаружении выдают соответствующее сообщение. Различают детекторы универсальные и специализированные. Универсальные детекторы в своей работе используют проверку неизменности файлов путем подсчета и сравнения с эталоном контрольной суммы. Недостаток универсальных детекторов связан с невозможностью определения причин искажения файлов. Специализированные детекторы выполняют поиск известных вирусов по их сигнатуре (повторяющемуся участку кода). Недостаток таких детекторов состоит в том, что они неспособны обнаруживать все известные вирусы.

Детектор, позволяющий обнаруживать несколько вирусов, называют *полидетектором*.

Недостатком таких антивирусных программ является то, что они могут находить только те вирусы, которые известны разработчикам таких программ.

Программы-доктора (фаги)

Программы-доктора не только находят зараженные вирусами файлы, но и «лечат» их, т.е. удаляют из файла тело программы вируса, возвращая файлы в исходное состояние. В начале своей работы фаги ищут вирусы в оперативной памяти, уничтожая их, и только затем переходят к «лечению» файлов. Среди фагов выделяют *полифаги*, т.е. программы-доктора, предназначенные для поиска и уничтожения большого количества вирусов.

Учитывая, что постоянно появляются новые вирусы, программы-детекторы и программы-доктора быстро устаревают, и требуется регулярное обновление их версий.

Программы-ревизоры

Программы-ревизоры относятся к самым надежным средствам защиты от вирусов. Ревизоры запоминают исходное состояние программ, каталогов и системных областей диска тогда, когда компьютер не заражен вирусом, а затем периодически или по желанию пользователя сравнивают текущее состояние с исходным. Обнаруженные изменения выводятся на экран видеомонитора. Как правило, сравнение состояний производят сразу после загрузки операционной системы. При сравнении проверяются длина файла, код циклического контроля (контрольная сумма файла), дата и время модификации, другие параметры.

Программы-ревизоры имеют достаточно развитые алгоритмы, обнаруживают стелс-вирусы и могут даже отличить изменения версии проверяемой программы от изменений, внесенных вирусом.

Программы-фильтры (сторожа)

Программы-фильтры представляют собой небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов. Такими действиями могут являться:

- попытки коррекции файлов с расширениями COM и EXE;
- изменение атрибутов файлов;
- прямая запись на диск по абсолютному адресу;
- запись в загрузочные сектора диска;
- загрузка резидентной программы.

При попытке какой-либо программы произвести указанные действия «сторож» посылает пользователю сообщение и предлагает запретить или разрешить соответствующее действие. Программы-фильтры весьма полезны, так как способны обнаружить вирус на самой ранней стадии его существования до размножения. Однако они не «лечат» файлы и диски. Для уничтожения вирусов требуется применить другие программы, например фаги. К недостаткам программ-сторожей можно отнести их «назойливость» (например, они постоянно выдают предупреждение о любой попытке копирования исполняемого файла), а также возможные конфликты с другим программным обеспечением.

Вакцины (иммунизаторы)

Вакцины – это резидентные программы, предотвращающие заражение файлов. Вакцины применяют, если отсутствуют программы-доктора, «лечащие» этот вирус. Вакцинация возможна только от известных вирусов. Вакцина модифицирует программу или диск таким образом, чтобы это не отражалось на их работе, а вирус будет воспринимать их зараженными и поэтому не внедрится. В настоящее время программы-вакцины имеют ограниченное применение.

Существенным недостатком таких программ является их ограниченные возможности по предотвращению заражения от большого числа разнообразных вирусов.

Вопросы

1. Признаки заражения компьютера.
2. Косвенные признаки заражения компьютера.
3. Действия при появлении признаков заражения вредоносной программой.
4. Источники компьютерных вирусов.
5. Глобальные сети и электронная почта как источник компьютерных вирусов.
6. Электронные конференции как источник компьютерных вирусов.
7. Локальные сети как источник компьютерных вирусов.
8. Пиратское программное обеспечение как источник компьютерных вирусов.
9. Компьютеры общего пользования как источник компьютерных вирусов.
10. Ремонтные службы как источник компьютерных вирусов.
11. Основные правила защиты от компьютерных вирусов.
12. Антивирусные программы.
13. Виды антивирусных программ.
14. Типовой перечень функций, которые способны выполнять антивирусные программы.
15. Назовите мощные и популярные на сегодняшний день в России антивирусные пакеты.
16. Принцип работы антивирусного сканера.
17. Принцип работы антивирусных программ-детекторов.

18. Принцип работы антивирусных программ-докторов (фагов).
19. Принцип работы антивирусных программ-ревизоров.
20. Принцип работы антивирусных программ-фильтров (сторожей).
21. Принцип работы вакцинаторов (иммунизаторов).

Тесты

1. Антивирус просматривает файлы, оперативную память и загрузочные секторы дисков на предмет наличия вирусных масок:

1. детектор;
2. доктор;
3. сканер;
4. ревизор;
5. сторож.

2. Антивирус обеспечивает поиск вирусов в оперативной памяти, на внешних носителях путем подсчета и сравнения с эталоном контрольной суммы:

1. детектор;
2. доктор;
3. сканер;
4. ревизор;
5. сторож.

3. Антивирус не только находит зараженные вирусами файлы, но и «лечит» их, т.е. удаляет из файла тело программы вируса, возвращая файлы в исходное состояние:

1. детектор;
2. доктор;
3. сканер;
4. ревизор;
5. сторож.

4. Антивирус запоминает исходное состояние программ, каталогов и системных областей диска, когда компьютер не заражен вирусом, а затем периодически или по команде пользователя сравнивает текущее состояние с исходным:

1. детектор;
2. доктор;

3. сканер;
4. ревизор;
5. сторож.

5. Антивирус представляет собой небольшую резидентную программу, предназначенную для обнаружения подозрительных действий при работе компьютера, характерных для вирусов:

1. детектор;
2. доктор;
3. сканер;
4. ревизор;
5. сторож.

6. Антивирус модифицирует программу или диск таким образом, чтобы вирус воспринимал их зараженными и поэтому не внедрялся:

1. детектор;
2. доктор;
3. сканер;
4. ревизор;
5. иммунизатор.

7. Антивирусный сканер:

1. обеспечивает поиск вирусов путем подсчета и сравнения с эталоном контрольной суммы;
2. находит зараженные вирусами файлы, «лечит» их, т.е. удаляет из файла тело вируса, возвращая файлы в исходное состояние;
3. запоминает исходное состояние, когда компьютер не заражен вирусом, затем периодически сравнивает текущее состояние с исходным;
4. просматривает файлы, оперативную память и загрузочные секторы дисков на предмет наличия вирусных масок;
5. обнаруживает подозрительные действия при работе компьютера, характерные для вирусов.

8. Антивирусный детектор:

1. обеспечивает поиск вирусов путем подсчета и сравнения с эталоном контрольной суммы;
2. находит зараженные вирусами файлы, «лечит» их, т.е. удаляет из файла тело вируса, возвращая файлы в исходное состояние;
3. запоминает исходное состояние, когда компьютер не заражен вирусом, затем периодически сравнивает текущее состояние с исходным;

4. просматривает файлы, оперативную память и загрузочные секторы дисков на предмет наличия вирусных масок;
5. обнаруживает подозрительные действия при работе компьютера, характерные для вирусов.

9. Антивирусный доктор:

1. обеспечивает поиск вирусов путем подсчета и сравнения с эталоном контрольной суммы;
2. находит зараженные вирусами файлы и удаляет из файла тело вируса, возвращая файлы в исходное состояние;
3. запоминает исходное состояние, когда компьютер не заражен вирусом, затем периодически сравнивает текущее состояние с исходным;
4. просматривает файлы, оперативную память и загрузочные секторы дисков на предмет наличия вирусных масок;
5. обнаруживает подозрительные действия при работе компьютера, характерные для вирусов.

10. Антивирусный ревизор:

1. обеспечивает поиск вирусов путем подсчета и сравнения с эталоном контрольной суммы;
2. находит зараженные вирусами файлы и удаляет из файла тело вируса, возвращая файлы в исходное состояние;
3. запоминает исходное состояние, когда компьютер не заражен вирусом, затем периодически сравнивает текущее состояние с исходным;
4. просматривает файлы, оперативную память и загрузочные секторы дисков на предмет наличия вирусных масок;
5. обнаруживает подозрительные действия при работе компьютера, характерные для вирусов.

11. Антивирусный сторож:

1. обеспечивает поиск вирусов путем подсчета и сравнения с эталоном контрольной суммы;
2. находит зараженные вирусами файлы и удаляет из файла тело вируса, возвращая файлы в исходное состояние;
3. запоминает исходное состояние, когда компьютер не заражен вирусом, затем периодически сравнивает текущее состояние с исходным;

4. просматривает файлы, оперативную память и загрузочные секторы дисков на предмет наличия вирусных масок;
5. обнаруживает подозрительные действия при работе компьютера, характерные для вирусов.

12. Антивирусный иммунизатор:

1. обеспечивает поиск вирусов путем подсчета и сравнения с эталоном контрольной суммы;
2. находит зараженные вирусами файлы и удаляет из файла тело вируса, возвращая файлы в исходное состояние;
3. модифицирует программу или диск таким образом, чтобы вирус воспринимал их зараженными и поэтому не внедрялся;
4. просматривает файлы, оперативную память и загрузочные секторы дисков на предмет наличия вирусных масок;
5. обнаруживает подозрительные действия при работе компьютера, характерные для вирусов.

Тема 5.

Методы и средства защиты компьютерной информации

Изучив тему 5, студент должен:
знать:

- методы защиты информации
- как организовать информационную безопасность в организации;

уметь:

- применять методы защиты информации

акцентировать внимание на понятиях:

- ограничение доступа, разграничение доступа, разделение доступа, криптографическое преобразование информации, контроль и учет доступа, законодательные меры.

Содержание темы (дидактические единицы и их характеристика):

Рассматриваются методы защиты информации: ограничение доступа, разграничение доступа, разделение доступа, криптографическое преобразование информации, контроль и учет доступа, законодательные меры, обеспечение информационной безопасности в Интернете.

Цели и задачи изучения темы: Получение знаний о методах защиты информации. Получение знаний и навыков по обеспечению информационной безопасности организации при ее подключении к Интернет.

Порядок изучения темы

Распределение бюджета времени по теме:

- количество часов отведенных на практические занятия, из них в компьютерной аудитории – 8/8;
- количество часов, отведенных на самостоятельную работу – 32.

Виды самостоятельной работы студентов:

− изучение учебного пособия «Информационная безопасность»;
− подготовка к участию в форуме по теме «Методы защиты информации»;
− изучение дополнительной литературы;
− выполнение тестовых заданий по теме.

Методические указания по изучению вопросов темы

При изучении учебных вопросов:

- изучить тему 5 по учебному пособию «Информационная безопасность»;
- принять участие в форуме по теме «Методы защиты информации»;
- изучить дополнительные материалы.

При изучении темы необходимо:

- *читать литературу*:

1. «Информационная безопасность: Уч. Пособие. – М.: МЭСИ, 2007.
2. Герасименко В.А., Малюк А.А. Основы защиты информации, – М.: ППО «Известия», 1997. Гл. 1,2.
3. Мельников В.И. Защита информации в компьютерных системах. – М.: Финансы и статистика, 1997. – Разд. 1.
4. Милославская Н.Г., Толстой А.И. Интрасети: доступ в Internet, защита. – М.: ООО «ЮНИТИ-ДАНА», 2000., Гл. 1.
5. Проскурин В.Г., Крутов С.В. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах. – М.: Радио и связь, 2000.
6. Белкин П.Ю. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных. – М.: Радио и связь, 1999.

- *посетить сайты:* www.compulenta.ru, www.isecurity.ru, www.oxpaha.ru, www.cyberterrorism report.ru.

Вопросы темы

5.1. Методы обеспечения информационной безопасности РФ.
5.2. Ограничение доступа.
5.3. Контроль доступа к аппаратуре.
5.4. Разграничение и контроль доступа к информации.
5.5. Предоставление привилегий на доступ.

5.6. Идентификация и установление подлинности объекта (субъекта).

5.7. Защита информации от утечки за счет побочного электромагнитного излучения и наводок.

5.8. Методы и средства защиты информации от случайных воздействий.

5.9. Методы защиты информации от аварийных ситуаций.

5.10. Организационные мероприятия по защите информации.

5.11. Организация информационной безопасности компании.

5.12. Выбор средств информационной безопасности.

5. 13. Информационное страхование.

5.1. Методы обеспечения информационной безопасности Российской Федерации

Информационная безопасность Российской Федерации является одной из составляющих национальной безопасности Российской Федерации и оказывает влияние на защищенность национальных интересов Российской Федерации в различных сферах жизнедеятельности общества и государства. Угрозы информационной безопасности Российской Федерации и методы ее обеспечения являются общими для этих сфер.

В различных сферах жизнедеятельности имеются свои особенности обеспечения информационной безопасности, связанные со спецификой объектов обеспечения безопасности, степенью их уязвимости в отношении угроз информационной безопасности Российской Федерации.

Общие методы обеспечения информационной безопасности Российской Федерации разделяются на правовые, организационно-технические и экономические.

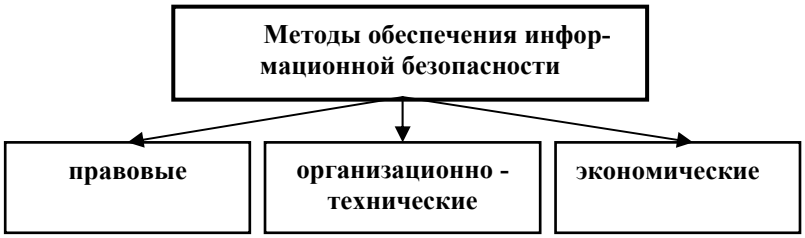


Рис. 5.1. **Методы обеспечения информационной безопасности**

К ***правовым методам*** обеспечения информационной безопасности Российской Федерации относится разработка нормативных правовых актов, регламентирующих отношения в информационной сфере, и нормативных методических документов по вопросам обеспечения информационной безопасности Российской Федерации. Наиболее важными направлениями этой деятельности являются:

- внесение изменений и дополнений в законодательство Российской Федерации, регулирующее отношения в области обеспечения информационной безопасности, в целях создания и совершенствования системы обеспечения информационной безопасности Российской Федерации, устранения внутренних противоречий в федеральном законодательстве, противоречий, связанных с международными соглашениями, к которым присоединилась Российская Федерация, и противоречий между федеральными законодательными актами и законодательными актами субъектов Российской Федерации, а также в целях конкретизации правовых норм, устанавливающих ответственность за правонарушения в области обеспечения информационной безопасности Российской Федерации;
- законодательное разграничение полномочий в области обеспечения информационной безопасности Российской Федерации между федеральными органами государственной власти и органами государственной власти субъектов Российской Федерации, определение целей, задач и механизмов участия в этой деятельности общественных объединений, организаций и граждан;
- разработка и принятие нормативных правовых актов Российской Федерации, устанавливающих ответственность юридических и физических лиц за несанкционированный доступ к информации, ее противоправное копирование, искажение и противозаконное использование, преднамеренное распространение недостоверной информации, противоправное раскрытие конфиденциальной информации, использование в преступных и корыстных целях служебной информации или информации, содержащей коммерческую тайну;
- уточнение статуса иностранных информационных агентств, средств массовой информации и журналистов, а также инвесторов при привлечении иностранных инвестиций для развития информационной инфраструктуры России;
- законодательное закрепление приоритета развития национальных сетей связи и отечественного производства космических спутников связи;
- определение статуса организаций, предоставляющих услуги глобальных информационно-телекоммуникационных сетей на тер-

ритории Российской Федерации, и правовое регулирование деятельности этих организаций;

- создание правовой базы для формирования в Российской Федерации региональных структур обеспечения информационной безопасности.

К организационно-техническим методам обеспечения информационной безопасности Российской Федерации относятся:

- создание и совершенствование системы обеспечения информационной безопасности Российской Федерации;
- усиление правоприменительной деятельности федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, включая предупреждение и пресечение правонарушений в информационной сфере, а также выявление, изобличение и привлечение к ответственности лиц, совершивших преступления и другие правонарушения в этой сфере;
- разработка, использование и совершенствование средств защиты информации и методов контроля эффективности этих средств, развитие защищенных телекоммуникационных систем, повышение надежности специального программного обеспечения;
- создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи;
- выявление технических устройств и программ, представляющих опасность для нормального функционирования информационно-телекоммуникационных систем, предотвращение перехвата информации по техническим каналам, применение криптографических средств защиты информации при ее хранении, обработке и передаче по каналам связи, контроль за выполнением специальных требований по защите информации;
- сертификация средств защиты информации, лицензирование деятельности в области защиты государственной тайны, стандартизация способов и средств защиты информации;
- совершенствование системы сертификации телекоммуникационного оборудования и программного обеспечения автоматизированных систем обработки информации по требованиям информационной безопасности;

- контроль за действиями персонала в защищенных информационных системах, подготовка кадров в области обеспечения информационной безопасности Российской Федерации;
- формирование системы мониторинга показателей и характеристик информационной безопасности Российской Федерации в наиболее важных сферах жизни и деятельности общества и государства.

К экономическим методам обеспечения информационной безопасности Российской Федерации относятся:

- разработку программ обеспечения информационной безопасности Российской Федерации и определение порядка их финансирования;
- совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-технических методов защиты информации, создание системы страхования информационных рисков физических и юридических лиц.

Обеспечение информационной безопасности Российской Федерации в сфере экономики играет ключевую роль в обеспечении национальной безопасности Российской Федерации.

Воздействию угроз информационной безопасности Российской Федерации в сфере экономики наиболее подвержены:

- система государственной статистики;
- кредитно-финансовая система;
- информационные и учетные автоматизированные системы подразделений федеральных органов исполнительной власти, обеспечивающих деятельность общества и государства в сфере экономики;
- системы бухгалтерского учета предприятий, учреждений и организаций независимо от формы собственности;
- системы сбора, обработки, хранения и передачи финансовой, биржевой, налоговой, таможенной информации и информации о внешнеэкономической деятельности государства, а также предприятий, учреждений и организаций независимо от формы собственности.

Переход к рыночным отношениям в экономике вызвал появление на внутреннем российском рынке товаров и услуг множества отечественных и зарубежных коммерческих структур – производителей и потребителей информации, средств информатизации и защиты информации. Бесконтрольная деятельность этих структур по

созданию и защите систем сбора, обработки, хранения и передачи статистической, финансовой, биржевой, налоговой, таможенной информации создает реальную угрозу безопасности России в экономической сфере. Аналогичные угрозы возникают при бесконтрольном привлечении иностранных фирм к созданию подобных систем, поскольку при этом складываются благоприятные условия для несанкционированного доступа к конфиденциальной экономической информации и для контроля за процессами ее передачи и обработки со стороны иностранных спецслужб.

Критическое состояние предприятий национальных отраслей промышленности, разрабатывающих и производящих средства информатизации, телекоммуникации, связи и защиты информации, приводит к широкому использованию соответствующих импортных средств, что создает угрозу возникновения технологической зависимости России от иностранных государств.

Серьезную угрозу для нормального функционирования экономики в целом представляют компьютерные преступления, связанные с проникновением криминальных элементов в компьютерные системы и сети банков и иных кредитных организаций.

Недостаточность нормативной правовой базы, определяющей ответственность хозяйствующих субъектов за недостоверность или сокрытие сведений об их коммерческой деятельности, о потребительских свойствах производимых ими товаров и услуг, о результатах их хозяйственной деятельности, об инвестициях и тому подобном, препятствует нормальному функционированию хозяйствующих субъектов. В то же время существенный экономический ущерб хозяйствующим субъектам может быть нанесен вследствие разглашения информации, содержащей коммерческую тайну. В системах сбора, обработки, хранения и передачи финансовой, биржевой, налоговой, таможенной информации наиболее опасны противоправное копирование информации и ее искажение вследствие преднамеренных или случайных нарушений технологии работы с информацией, несанкционированного доступа к ней. Это касается и федеральных органов исполнительной власти, занятых формированием и распространением информации о внешнеэкономической деятельности Российской Федерации.

Основными мерами по обеспечению информационной безопасности Российской Федерации в сфере экономики являются:

- организация и осуществление государственного контроля за созданием, развитием и защитой систем и средств сбора, обработки,

хранения и передачи статистической, финансовой, биржевой, налоговой, таможенной информации;

- коренная перестройка системы государственной статистической отчетности в целях обеспечения достоверности, полноты и защищенности информации, осуществляемая путем введения строгой юридической ответственности должностных лиц за подготовку первичной информации, организацию контроля за деятельностью этих лиц и служб обработки и анализа статистической информации, а также путем ограничения коммерциализации такой информации;
- разработка национальных сертифицированных средств защиты информации и внедрение их в системы и средства сбора, обработки, хранения и передачи статистической, финансовой, биржевой, налоговой, таможенной информации;
- разработка и внедрение национальных защищенных систем электронных платежей на базе интеллектуальных карт, систем электронных денег и электронной торговли, стандартизация этих систем, а также разработка нормативной правовой базы, регламентирующей их использование;
- совершенствование нормативной правовой базы, регулирующей информационные отношения в сфере экономики;
- совершенствование методов отбора и подготовки персонала для работы в системах сбора, обработки, хранения и передачи экономической информации.

Наиболее важными объектами обеспечения информационной безопасности Российской Федерации в области науки и техники являются:

- результаты фундаментальных, поисковых и прикладных научных исследований, потенциально важные для научно-технического, технологического и социально-экономического развития страны, включая сведения, утрата которых может нанести ущерб национальным интересам и престижу Российской Федерации;
- открытия, незапатентованные технологии, промышленные образцы, полезные модели и экспериментальное оборудование;
- научно-технические кадры и система их подготовки;
- системы управления сложными исследовательскими комплексами (ядерными реакторами, ускорителями элементарных частиц, плазменными генераторами и др.).

5.2. Ограничение доступа

Ограничение доступа заключается в создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям.

Ограничение доступа к автоматизированной системе обработки информации (АСОИ) заключается:

- в выделении специальной территории для размещения АСОИ;
- в оборудовании по периметру выделенной зоны специальных ограждений с охранной сигнализацией;
- в сооружении специальных зданий или других сооружений;
- в выделении специальных помещений в здании;
- в создании контрольно-пропускного режима на территории, в зданиях и помещениях.

Задача средств ограничения доступа – исключить случайный и преднамеренный доступ посторонних лиц на территорию размещения АСОИ и непосредственно к аппаратуре. В указанных целях создается защитный контур, замыкаемый двумя видами преград: физической и контрольно-пропускной. Такие преграды часто называют системой охранной сигнализации и системой контроля доступа.

Традиционные средства контроля доступа в защищаемую зону заключаются в изготовлении и выдаче допущенным лицам специальных пропусков с размещенной на них фотографией личности владельца и сведений о нем. Данные пропуска могут храниться у владельца или непосредственно в пропускной кабине охраны. В последнем случае допущенное лицо называет фамилию и свой номер, либо набирает его на специальной панели кабины при проходе через турникет, пропускное удостоверение выпадает из гнезда и поступает в руки работника охраны, который визуально сверяет личность владельца с изображением на фотографии, названную фамилию с фамилией на пропуске. Эффективность защиты данной системы выше первой. При этом исключаются потеря пропуска, его перехват и подделка. Кроме того, есть резерв в повышении эффективности защиты с помощью увеличения количества проверяемых параметров. Однако основная нагрузка по контролю при этом ложится на человека, а он, как известно, может ошибаться.

К проверяемым параметрам можно отнести биометрические методы аутентификации человека.

Биометрические технологии

Биометрические технологии – это идентификация человека по уникальным, присущим только ему биологическим признакам. На сегодняшний день биометрические системы доступа являются самыми надежными. Важным фактором увеличения популярности биометрической защиты является простота их эксплуатации, поэтому они становятся доступными для домашних пользователей.

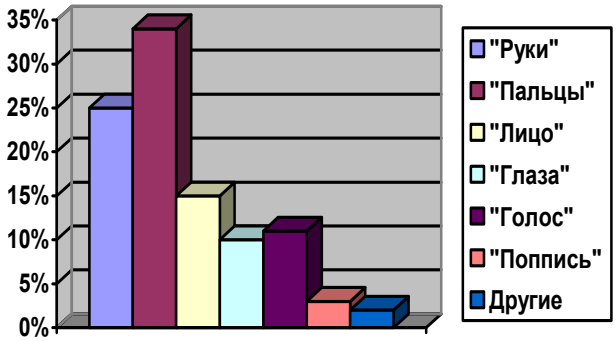


Рис. 5.2. **Статистика**

Отпечатки пальцев

Идентификация человека по отпечаткам пальцев – самый распространенный способ, использующийся биометрическими системами защиты информации. Сегодня существует три технологии снятия отпечатков пальцев. Первая из них – это использование оптических сканеров. Принцип действия этих устройств практически идентичен принципам работы обычных сканеров. Главное достоинство оптических сканеров – это их дешевизна. К недостаткам следует отнести то, что это весьма капризные приборы, требующие постоянного ухода. Пыль, грязь и царапины могут отказать в допуске легальному пользователю, кроме того, отпечаток, полученный с помощью оптического сканера, очень сильно зависит от состояния кожи. Жирная или, наоборот, сухая и уж тем более потрескавшаяся кожа может послужить причиной размытости изображения и невозможности идентификации личности.

Вторая технология основана на использовании не оптических, а электрических сканеров. Суть ее заключается в следующем. Пользователь прикладывает палец к специальной пластине, которая со-

стоит из кремниевой подложки, содержащей 90 тысяч конденсаторных пластин с шагом считывания 500 тнд. При этом получается своеобразный конденсатор. Одна пластина – это поверхность сенсора, вторая – палец человека. А поскольку потенциал электрического поля внутри конденсатора зависит от расстояния между пластинами, то карта этого поля повторяет папиллярный рисунок пальца. Электрическое поле измеряется, а полученные данные преобразуются в восьмибитовое растровое изображение. К достоинствам этой технологии можно отнести очень высокую точность получаемого отпечатка пальца, не зависящую от состояния кожи пользователя. Система прекрасно сработает даже в том случае, если палец человека испачкан. Кроме того, само устройство имеет маленькие размеры, что позволяет использовать его во многих местах. Но есть у электрического сканера и недостатки. Во-первых, изготовление сенсора, содержащего 90 тысяч конденсаторных пластин достаточно дорогое. Во-вторых, кремниевый кристалл, лежащий в основе сканера, требует герметичной оболочки. А это накладывает дополнительные ограничения на условия применения системы, в частности на внешнюю среду, наличие вибрации и ударов. В-третьих, отказ от работы при наличии сильного электромагнитного излучения.

Третья технология идентификации человека по отпечаткам пальцев – TactileSense, разработанная компанией Who Vision Systems. В этих сканерах используется специальный полимерный материал, чувствительный к разности электрического поля между гребнями и впадинами кожи. То есть фактически принцип работы устройств TactileSense такой же, как и у электрических сканеров, но у них есть ряд преимуществ. Первое – стоимость производства полимерного сенсора в сотни раз меньше, чем цена кремниевого. Второе – отсутствие хрупкой основы обеспечивает высокую прочность как поверхности сканера, так и всего устройства. Третье – миниатюрные размеры сенсора. Фактически для получения отпечатка нужна только пластинка площадью, равной площади подушечки пальца, и толщиной всего 0,075 мм. К этому нужно добавить небольшую электронную начинку. Получившийся сенсор настолько мал, что его можно без какого-либо ущерба встроить практически в любое компьютерное устройство.

Глаза

У человеческого глаза есть две уникальные для каждого человека характеристики. Это сетчатка и радужная оболочка. Первую

для построения биометрических систем обеспечения информационной безопасности используют уже давно. В этих системах сканер определяет либо рисунок кровеносных сосудов глазного дна, либо отражающие и поглощающие характеристики самой сетчатки. Обе эти технологии считаются самыми надежными среди биометрических. Сетчатку невозможно подделать, ее нельзя сфотографировать или снять откуда-нибудь, как отпечаток пальца. Правда, недостатков у систем, работающих с сетчаткой глаза, более чем достаточно. Во-первых, это высокая стоимость сканеров и их большие габариты. Во-вторых, долгое время анализа полученного изображения (не менее одной минуты). В-третьих, – неприятная для человека процедура сканирования. Дело в том, что пользователь должен во время этого процесса смотреть в определенную точку. Причем сканирование осуществляется с помощью инфракрасного луча, из-за чего человек испытывает болезненные ощущения. И, наконец, в-четвертых, – значительное ухудшение качества снимка при некоторых заболеваниях, например при катаракте. А это значит, что люди с ухудшенным зрением не смогут воспользоваться этой технологией.

Недостатки идентификации человека по сетчатке глаза привели к тому, что эта технология плохо подходит для использования в системах защиты информации. Поэтому наибольшее распространение она получила в системах доступа на секретные научные и военные объекты.

По-другому обстоят дела с системами, использующими для идентификации радужную оболочку глаза. Для их работы нужны только специальное программное обеспечение и камера. Принцип работы таких систем очень прост. Камера снимает лицо человека. Программа из полученного изображения выделяет радужную оболочку. Затем по определенному алгоритму строится цифровой код, по которому и осуществляется идентификация. Данный метод имеет ряд преимуществ. Во-первых, небольшая цена. Во-вторых, ослабленное зрение не препятствует сканированию и кодированию идентифицирующих параметров. В-третьих, камера не доставляет никакого дискомфорта пользователям.

Лицо

На сегодняшний день существует две биометрические технологии, использующие для идентификации человека его лицо. Первая представляет специальное программное обеспечение, которое получает изображение с веб-камеры и обрабатывает его. На лице

выделяются отдельные объекты (брови, глаза, нос, губы), для каждого из которых вычисляются параметры, полностью его определяющие. При этом многие современные системы строят трехмерный образ лица человека. Это нужно для того, чтобы идентификация оказалась возможной, например, при наклоне головы и повороте под небольшим углом. Достоинство у подобных систем одно – это цена. Ведь для работы нужны только специальное программное обеспечение и веб-камера, которая уже стала привычным атрибутом многих компьютеров. Недостатков идентификации человека по форме лица гораздо больше. Самый главный минус – низкая точность. Человек во время идентификации может не так повернуть голову, или его лицо может иметь не то выражение, которое хранится в базе данных. Кроме того, система, скорее всего, откажет в доступе женщине, которая накрасилась не так, как обычно, например изменив форму бровей. Можно еще вспомнить и близнецов, форма лица которых практически идентична.

Вторая технология, основанная на идентификации человека по его лицу, использует термограмму. Дело в том, что артерии человека, которых на лице довольно много, выделяют тепло. Поэтому, сфотографировав пользователя с помощью специальной инфракрасной камеры, система получает «карту» расположения артерий, которая и называется термограммой. У каждого человека она различна. Даже у однояйцевых близнецов артерии расположены по-разному. А поэтому надежность этого метода достаточно высока. К сожалению, он появился недавно и пока не получил большого распространения.

Ладонь

Так же как и в предыдущем случае существуют два способа идентификации человека по ладони. В первом используется ее форма. Основой системы является специальное устройство. Оно состоит из камеры и нескольких подсвечивающих диодов. Главная задача этого устройства – построить трехмерный образ ладони, который потом сравнивается с эталонными данными. Надежность этого способа идентификации довольно велика. Вот только прибор, сканирующий ладонь, – довольно хрупкое устройство. А поэтому условия его использования ограничены.

Вторая биометрическая технология, использующая ладонь человека, использует для идентификации термограмму. В общем, этот способ полностью идентичен определению пользователя

по термограмме лица, так что его достоинства и недостатки точно такие же.

Динамические характеристики

Динамические параметры – это поведенческие характеристики, то есть те, которые построены на особенностях, характерных для подсознательных движений в процессе воспроизведения какого-либо действия. В биометрических системах чаще всего используются голос, почерк и клавиатурный почерк.

Главными достоинствами систем, идентифицирующих людей по голосу, являются низкая цена и удобство как для пользователей, так и для администраторов. Для этого необходимо специальное программное обеспечение и микрофон, подключенный к компьютеру. К недостаткам биометрических систем, использующих голос, в первую очередь следует отнести довольно низкую надежность. Дело в том, что, используя современные высококачественные устройства, можно записать и воспроизвести голос человека и нет никакой гарантии, что система распознает подделку. Кроме того, простуда может немного изменить голос пользователя, в результате чего ему будет отказано в доступе.

Личная подпись для идентификации человека используется уже много веков. Первые компьютерные системы, использующие этот параметр, просто сравнивали полученную картинку с эталоном. Но, к сожалению, этот способ идентификации очень ненадежен. При желании злоумышленник может натренироваться и легко подделать практически любую подпись. Поэтому современные системы не просто сравнивают две картинки, но и измеряют динамические характеристики написания (время нанесения подписи, динамику нажима на поверхность и т. п.). Естественно, что для этого нужно специальное оборудование. В большинстве случаев компьютер доукомплектовывается сенсорной поверхностью, похожей на графический планшет. Но все большую и большую популярность завоевывают специальные «ручки», способные измерять степень нажима во время «письма» и прочие параметры. Главное их достоинство перед сенсорными поверхностями – минимум занимаемого места, что существенно расширяет область применения биометрических систем этого класса.

Наиболее распространенный способ идентификации человека по динамическим характеристикам – клавиатурный почерк. Дело в том, что каждый человек по-своему набирает текст на клавиатуре.

Поэтому по определенным характеристикам можно идентифицировать пользователя с довольно высокой точностью. Плюсы подобных систем очевидны. Во-первых, не нужно никакое дополнительное оборудование. Во-вторых, идентификация очень удобна для пользователя: он вводит обычный пароль, а на самом деле система точно определяет, имеет ли право сидящий за компьютером на доступ к информации. Главный недостаток использования клавиатурного почерка для идентификации личности – временное изменение этого самого почерка у пользователей под влиянием стрессовых ситуаций. Что, в свою очередь, может привести к отказу в доступе человеку, имеющему на это право.

Необходимо отметить, что ситуация на рынке биометрических систем изменяется очень быстро. Постоянно появляются новые, более надежные, а зачастую и более дешевые технологии.

Совершенствование контрольно-пропускной системы в настоящее время ведется также в направлении совершенствования конструкции пропуска-удостоверения личности путем записи кодовых значений паролей.

Физическая преграда защитного контура, размещаемая по периметру охраняемой зоны, снабжается охранной сигнализацией.

В настоящее время ряд предприятий выпускает электронные системы для защиты государственных и частных объектов от проникновения в них посторонних лиц. Гарантировать эффективность системы охранной сигнализации можно только в том случае, если обеспечены надежность всех ее составных элементов и их согласованное функционирование. При этом имеют значение тип датчика, способ оповещения или контроля, помехоустойчивость, а также реакция на сигнал тревоги. Местная звуковая или световая сигнализация может оказаться недостаточной, поэтому местные устройства охраны целесообразно подключить к специализированным средствам централизованного управления, которые при получении сигнала тревоги высылают специальную группу охраны.

Следить за состоянием датчиков может автоматическая система, расположенная в центре управления, или сотрудник охраны, который находится на объекте и при световом или звуковом сигнале принимает соответствующие меры. В первом случае местные охранные устройства подключаются к центру через телефонные линии, а специализированное цифровое устройство осуществляет периодический опрос состояния датчиков, автоматически набирая номер приемоответчика, расположенного на охраняемом объекте. При по-

ступлении в центр сигнала тревоги автоматическая система включает сигнал оповещения.

Датчики сигналов устанавливаются на различного рода ограждениях, внутри помещений, непосредственно на сейфах и т. д.

При разработке комплексной системы охраны конкретного объекта учитывают его специфику: внутреннюю планировку здания, окон, входной двери, размещение наиболее важных технических средств.

Все эти факторы влияют на выбор типа датчиков, их расположение и определяют ряд других особенностей данной системы. По принципу действия системы тревожной сигнализации можно классифицировать следующим образом:

- традиционные (обычные), основанные на использовании цепей сигнализации и индикации в комплексе с различными контактами (датчиками);
- ультразвуковые;
- прерывания луча;
- телевизионные;
- радиолокационные;
- микроволновые;
- прочие.

5.3. Контроль доступа к аппаратуре

В целях контроля доступа к внутреннему монтажу, линиям связи и технологическим органам управления используется аппаратура контроля вскрытия аппаратуры. Это означает, что внутренний монтаж аппаратуры и технологические органы и пульты управления закрыты крышками, дверцами или кожухами, на которые установлены датчики. Датчики срабатывают при вскрытии аппаратуры и выдают электрические сигналы, которые по цепям сбора поступают на централизованное устройство контроля. Установка такой системы имеет смысл при наиболее полном перекрытии всех технологических подходов к аппаратуре, включая средства загрузки программного обеспечения, пульты управления АСОИ и внешние кабельные соединители.

В идеальном случае для систем с повышенными требованиями к эффективности защиты информации целесообразно закрывать крышками под механический замок с датчиком или ставить под

контроль включение также штатных средств входа в систему – терминалов пользователей.

Контроль вскрытия аппаратуры необходим не только в интересах защиты информации от несанкционированного доступа, но и для соблюдения технологической дисциплины.

С позиций защиты информации от несанкционированного доступа контроль вскрытия аппаратуры защищает от следующих действий:

- изменения и разрушения принципиальной схемы вычислительной системы и аппаратуры;
- подключения постороннего устройства;
- изменения алгоритма работы вычислительной системы путем использования технологических пультов и органов управления;
- загрузки вредоносных программ в систему;
- использования терминалов посторонними лицами и т. д.

Основная задача систем контроля вскрытия аппаратуры – перекрытие на период эксплуатации всех нештатных и технологических подходов к аппаратуре. Если последние потребуются в процессе эксплуатации системы, выводимая на ремонт или профилактику аппаратура перед началом работ отключается от рабочего контура обмена информацией, подлежащей защите, и вводится в рабочий контур под наблюдением и контролем лиц, ответственных за безопасность информации.

Доступ к штатным входам в систему – терминалам контролируется с помощью контроля выдачи механических ключей пользователям, а доступ к информации – с помощью системы опознания и разграничения доступа, включающей применение кодов паролей, соответствующие функциональные задачи программного обеспечения и специального терминала службы безопасности информации.

Указанный терминал и устройство контроля вскрытия аппаратуры входят в состав рабочего места службы безопасности информации, с которого осуществляются централизованный контроль доступа к аппаратуре и информации и управление ее защитой на данной вычислительной системе.

5.4. Разграничение и контроль доступа к информации

Разграничение доступа в вычислительной системе заключается в разделении информации, циркулирующей в ней, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями.

Задача разграничения доступа – сокращение количества должностных лиц, не имеющих к ней отношения при выполнении своих функций, т. е. защита информации от нарушителя среди допущенного к ней персонала.

При этом деление информации может производиться по степени важности, секретности, по функциональному назначению, по документам и т. д.

Принимая во внимание, что доступ осуществляется с различных технических средств, начинать разграничение можно путем разграничения доступа к техническим средствам, разместив их в отдельных помещениях. Все подготовительные функции технического обслуживания аппаратуры, ее ремонта, профилактики, перезагрузки программного обеспечения и т. д. должны быть технически и организационно отделены от основных задач системы.

АСОИ и организация ее обслуживания должны включать следующие требования:

- техническое обслуживание АСОИ в процессе эксплуатации должно выполняться отдельным персоналом без доступа к информации, подлежащей защите;
- изменения в программном обеспечении должны производиться специально выделенным для этой цели проверенным специалистом;
- функции обеспечения безопасности информации должны выполняться специальным подразделением;
- организация доступа пользователей к базам данных должна обеспечивать возможность разграничения доступа к информации, с достаточной степенью детализации и в соответствии с заданными уровнями полномочий пользователей;
- регистрация и документирование технологической и оперативной информации должны быть разделены.

Разграничение доступа пользователей АСОИ может осуществляться по следующим параметрам:

- по виду, характеру, назначению, степени важности и секретности информации;

- по способам ее обработки (считать, записать, внести изменения, выполнить команду);
- по условному номеру терминала;
- по времени обработки и др.

Принципиальная возможность разграничения по параметрам должна быть обеспечена проектом АСОИ. А конкретное разграничение при эксплуатации АСОИ устанавливается потребителем и вводится в систему его подразделением, отвечающим за безопасность информации.

При проектировании базового вычислительного комплекса для построения АСОИ производятся:

- разработка операционной системы с возможностью реализации разграничения доступа к информации, хранящейся в памяти;
- изоляция областей доступа;
- разделение базы данных на группы;
- процедуры контроля перечисленных функций.

В качестве идентификаторов личности для реализации разграничения широко распространено применение кодов паролей. В помощь пользователю в системах с повышенными требованиями большие значения кодов паролей записываются на специальные носители – электронные ключи или карточки. Также могут применяться биометрические технологии, рассмотренные ранее.

5.5. Предоставление привилегий на доступ

Предоставление привилегий на доступ к информации заключается в том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы.

Задача метода – затруднить преднамеренный перехват информации нарушителем. Примером такого доступа может быть сейф с несколькими ключами, замок которого открывается только при наличии всех ключей. Аналогично в АСОИ может быть предусмотрен механизм разделения привилегий при доступе к особо важным данным с помощью кодов паролей.

Данный метод усложняет процедуру доступа к информации, но обладает высокой эффективностью защиты. На его принципах

можно организовать доступ к данным с санкции вышестоящего лица по запросу или без него.

При наличии дефицита в средствах, а также в целях постоянного контроля доступа к ценной информации со стороны администрации потребителя АСУ в некоторых случаях возможен вариант использования права на доступ к информации нижестоящего руководителя только при наличии его идентификатора и идентификатора его заместителя или представителя службы безопасности информации. При этом информация выдается на дисплей только руководителя, а на дисплей подчиненного – только информация о факте ее вызова.

5.6. Идентификация и установление подлинности объекта (субъекта)

Объект идентификации и установление подлинности

Идентификация – это присвоение какому-либо объекту или субъекту уникального образа, имени или числа.

Установление подлинности (*аутентификация*) заключается в проверке, является ли проверяемый объект (субъект) в самом деле тем, за кого себя выдает.

Конечная цель идентификации и установления подлинности объекта в вычислительной системе – допуск его к информации ограниченного пользования в случае положительного исхода проверки или отказ в допуске в случае отрицательного исхода проверки.

Объектами идентификации и установления подлинности в АСОИ могут быть:

- человек (оператор, пользователь, должностное лицо);
- техническое средство (терминал, дисплей, ЭВМ, АСОИ);
- документы (распечатки, листинги и др.);
- носители информации (съемные диски);
- информация на мониторе, дисплее, табло и т. д.

Установление подлинности объекта может производиться человеком, аппаратным устройством, программой, вычислительной системой и т. д.

В вычислительных системах применение указанных методов в целях защиты информации при ее обмене предполагает конфиденциальность образов и имен объектов.

При обмене информацией между человеком и ЭВМ (а при удаленных связях обязательно) вычислительными системами в сети рекомендуется предусмотреть взаимную проверку подлинности полномочий объекта или субъекта. В указанных целях необходимо, чтобы каждый из объектов (субъектов) хранил в своей памяти, недоступной для посторонних, список образов (имен) объектов (субъектов), с которыми производится обмен информацией, подлежащей защите.

Идентификация и установление подлинности личности.

В повседневной жизни идентификатором личности является его внешний вид: фигура, форма головы, черты лица, характер, его привычки, поведение и другие свойственные данному человеку признаки, которые создают образ данного человека и которые сознательно или подсознательно мы приобретаем в процессе общения с ним и храним в своей памяти.

В качестве биометрических признаков, которые могут быть использованы при идентификации субъекта доступа, можно выделить следующие:

- отпечатки пальцев;
- геометрическая форма рук;
- узор радужной оболочки и сетчатки глаз;
- расположение кровеносных сосудов;
- запах тела;
- термические параметры тела;
- форма и размеры лица;
- особенности голоса;
- биомеханические характеристики почерка;
- биомеханические характеристики «клавиатурного почерка».

Основными параметрами, по которым можно сравнить эффективность и надежность реализации того или иного способа идентификации субъекта доступа на основе биометрических характеристик личности, являются стандартные статистические показатели ошибок первого и второго рода. Ошибка первого рода устанавливает вероятность отказа в доступе легальному пользователю автоматизированной системы, ошибка второго рода – вероятность несанкционированного предоставления доступа. В современных системах разграничения доступа, основанных на применении биометрических параметров, вероятность ошибки первого рода составляет от 10^{-6} до 10^{-3}, а вероятность ошибки второго рода от $6{,}6 \times 10^{-6}$ до 10^{-2}.

Известно, что отпечатки пальцев и очертания ладони руки, тембр голоса, личная подпись и другие элементы личности носят индивидуальный характер и сохраняются на протяжении всей жизни человека. В настоящее время в этом направлении ведутся поиски технических решений и сделаны определенные успехи, но они пока носят рекламный характер и не получили широкого распространения. В разработанных для этой цели системах наблюдаются достаточно частые случаи отказа в санкционированном доступе и открытии доступа случайному пользователю. Не располагая подробными отчетами о проделанной работе, можно все же указать на предполагаемые причины этих неудач. Они кроются в недооценке задачи. Дело в том, что для выполнения процедуры установления подлинности необходимо совпадение образа, снимаемого с личности пользователя, с образом, хранящимся в памяти вычислительной системы, а для отказа в доступе система должна обладать способностью отличать похожие образы. Здесь существуют две задачи, которые необходимо решить одновременно. Для выполнения первой задачи (допуска) не требуется большого объема информации об образе (скажем даже, что чем меньше, тем лучше), а для выполнения второй (отказа) – информацию об образе необходимо увеличить на максимально возможную величину.

Пока возможности техники ограничены и объемы памяти систем распознавания хранили ограниченный объем информации об образе, преобладали случаи допуска лица, не предусмотренного системой.

С развитием техники и увеличением объема информации об образе с целью наиболее точной проверки личности и наибольшего количества ее параметров увеличивается вероятность их изменений во времени и несовпадения с параметрами образа, хранимого системой проверки, растут объемы памяти, усложняется аппаратура и увеличивается вероятность отказа в доступе лицу, имеющему на это право.

Отправной точкой при разработке систем распознавания образов было естественное стремление повысить точность воспроизведения образа с целью отобрать автоматически из множества потенциальных образов единственный, хранящийся в памяти системы. Но при этом, по-видимому, не принималась во внимание величина этого множества, а она приближается к бесконечности (населению, жившему, живущему и родившемуся в будущем на Земле). Какова должна быть точность воспроизведения образа? Какова должна быть

разница между образом разрешенной к доступу личности и образом потенциального нарушителя? Какова вероятность появления нарушителя, образ которого приближается к образу, хранимому в памяти вычислительной системы? На эти вопросы ответов нет. Следовательно, работы по системам распознавания образов в целях широкого применения для защиты информации в вычислительных системах нецелесообразны. Не следует также забывать о том, что стремление человека копировать природу не всегда приносило положительный результат.

Кроме того, системы идентификации и установления подлинности личности, основанные на антропометрических и физиологических данных человека, не отвечают самому важному требованию: конфиденциальности, так как записанные на физические носители данные хранятся постоянно и фактически являются ключом к информации, подлежащей защите, а постоянный ключ в конце концов становится доступным.

Типичным примером простой и распространенной системы аутентификации является система «ключ-замок», в которой владелец ключа является объектом установления подлинности. Но ключ можно потерять, похитить или снять с него копию, так как идентификатор личности физически от нее отделен. Система «ключ-замок» имеет локальное применение. Однако в сочетании с другими системами аутентификации и в условиях пониженных требований она применяется до сих пор. В электромеханическом замке вместо ключа может применяться код.

Одним из распространенных методов аутентификации являются присвоение лицу или другому объекту уникального имени или числа – пароля и хранение его значения в вычислительной системе. При входе в вычислительную систему пользователь вводит через терминал свой код пароля, вычислительная система сравнивает его значение со значением, хранящимся в своей памяти, и при совпадении кодов открывает доступ к разрешенной функциональной задаче, а при несовпадении – отказывает в нем.

Наиболее высокий уровень безопасности входа в систему достигается разделением кода пароля на две части: одну, запоминаемую пользователем и вводимую вручную, и вторую, размещаемую на специальном носителе – карточке, устанавливаемой пользователем на специальное считывающее устройство, связанное с терминалом. В этом случае идентификатор связан с личностью пользователя, размер пароля может быть легко запоминаемым и при хищении

карточки у пользователя будет время для замены кода пароля и получения новой карточки.

На случай защиты запоминаемой части пароля от получения ее нарушителем путем физического принуждения пользователя, возможно, будет полезно в вычислительной системе предусмотреть механизм тревожной сигнализации, основанный на применении ложного пароля. Ложный пароль запоминается пользователем одновременно с действительным и сообщается преступнику в вышеупомянутой ситуации.

Однако, учитывая опасность, которой подвергается жизнь пользователя, необходимо в вычислительной системе одновременно со скрытой сигнализацией предусмотреть механизм обязательного выполнения требований преступника, воспользовавшегося средствами аутентификации законного пользователя.

Кроме указанных методов паролей в вычислительных системах в качестве средств аутентификации применяют методы «Запрос-ответ» и «рукопожатия».

В методе «Запрос-ответ» набор ответов на *«m»* стандартных и *«n»* ориентированных на пользователя вопросов хранится в ЭВМ и управляется операционной системой. Когда пользователь делает попытку включиться в работу, операционная система случайным образом выбирает и задает ему некоторые (или все) из этих вопросов. Правильные ответы пользователя на указанные вопросы открывают доступ к системе.

Для исключения некоторых недостатков описанных выше методов операционная система может потребовать, чтобы пользователь доказал свою подлинность с помощью корректной обработки алгоритмов. Эту часть называют процедурой в режиме «рукопожатия», она может быть выполнена как между двумя ЭВМ, так и между пользователем и ЭВМ.

Методы «Запрос-ответ» и «рукопожатия» в некоторых случаях обеспечивают большую степень безопасности, но вместе с тем являются более сложными и требующими дополнительных затрат времени. Как и обычно, здесь нужно найти компромисс между требуемой степенью безопасности и простотой использования. При сложном использовании пользователь будет искать пути упрощения процедуры и в итоге найдет их, но за счет снижения эффективности средства защиты.

Идентификация и установление подлинности технических средств

Следующей ступенью при организации системы защиты информации в вычислительной системе могут быть идентификация и установление подлинности терминала, с которого входит в систему пользователь. Данная процедура также может осуществляться с помощью паролей. Пароль можно использовать не только для аутентификации пользователя и терминала по отношению к системе, но и для обратного установления подлинности ЭВМ по отношению к пользователю. Это важно, например, в вычислительных сетях, когда связь осуществляется с территориально удаленными объектами. В этом случае применяются одноразовые пароли или более сложные системы шифрования информации.

Идентификация и установление подлинности документов

В вычислительных системах в качестве документов, являющихся продуктом информационной системы и содержащих секретную информацию, могут быть распечатки с различных печатающих устройств.

Здесь необходимо подлинность документа рассматривать с двух позиций:

- получения документа, сформированного непосредственно данной вычислительной системой и на аппаратуре ее документирования;
- получения готового документа с удаленных объектов вычислительной сети или АСОИ.

В первом случае подлинность документа гарантируется вычислительной системой, имеющей средства защиты информации от НСД, а также физическими характеристиками печатающих устройств, присущими только данному устройству. Однако в ответственных случаях этого может оказаться недостаточно. Применение криптографического преобразования информации в этом случае является эффективным средством. Информация, закрытая кодом пароля, известным только передающему ее лицу и получателю, не вызывает сомнения в ее подлинности. Если код пароля, применяемый в данном случае, используется только передающим лицом и вводится им лично.

Криптографическое преобразование информации для идентификации и установления подлинности документа во втором случае, когда документ транспортировался по неохраняемой территории с

территориально удаленного объекта или продолжительное время находился на хранении, также является наиболее эффективным средством. Однако при отсутствии необходимого для этой цели оборудования невысокие требования к защите информации иногда позволяют использовать более простые средства идентификации и установления подлинности документов: опечатывание и пломбирование носителей документов с обеспечением их охраны. При этом к носителю должны прилагаться сопроводительные документы с подписями ответственных должностных лиц, заверенными соответствующими печатями.

При неавтоматизированном обмене информацией подлинность документа удостоверяется личной подписью человека, автора (авторов) документа. Проверка подлинности документа в этом случае обычно заключается в визуальной проверке совпадения изображения подписи на документе с образцом подлинника. При этом подпись располагается на одном листе вместе с текстом или частью текста документа, подтверждая тем самым подлинность текста. В особых случаях при криминалистической экспертизе проверяются и другие параметры подлинности документа.

При автоматизированной передаче документов по каналам связи, расположенным на неконтролируемой территории, меняются условия передачи документа. В этих условиях даже если сделать аппаратуру, воспринимающую и передающую изображение подписи автора документа, его получатель получит не подлинник, а всего лишь копию подписи, которая в процессе передачи может быть подвергнута повторному копированию для использования при передаче ложного документа. Поэтому при передаче документов по каналам связи в вычислительной сети используется криптографическое преобразование информации.

Область использования цифровой подписи чрезвычайно широка: от проведения финансовых и банковских операций до контроля за выполнением международных договоров и охраны авторских прав. При этом отмечается, что участники обмена документами нуждаются в защите от следующих преднамеренных несанкционированных действий:

- отказа отправителя от переданного сообщения;
- фальсификации (подделки) получателем полученного сообщения;
- изменения получателем полученного сообщения;
- маскировки отправителя под другого абонента.

Обеспечение защиты каждой стороны, участвующей в обмене, осуществляется с помощью введения специальных протоколов. Для верификации сообщения протокол должен содержать следующие обязательные положения:

- отправитель вносит в передаваемое сообщение свою цифровую подпись, представляющую собой дополнительную информацию, зависящую от передаваемых данных, имени получателя сообщения и некоторой закрытой информации, которой обладает только отправитель;
- получатель сообщения должен иметь возможность удостовериться, что полученная в составе сообщения подпись есть правильная подпись отправителя;
- получение правильной подписи отправителя возможно только при использовании закрытой информации, которой обладает только отправитель;
- для исключения возможности повторного использования устаревших сообщений верификация должна зависеть от времени.

Подпись сообщения представляет собой способ шифрования сообщения с помощью криптографического преобразования. Закрываемым элементом в преобразовании является код ключа. Если ключ подписи принадлежит конечному множеству ключей, если это множество достаточно велико, а ключ подписи определен методом случайного выбора, то полная проверка ключей подписи для пар сообщение-получатель с вычислительной точки зрения эквивалентна поиску ключа. Практически подпись является паролем, зависящим от отправителя, получателя и содержания передаваемого сообщения. Для предупреждения повторного использования подпись должна меняться от сообщения к сообщению. Получатель сообщения, несмотря на неспособность составить правильную подпись отправителя, тем не менее должен иметь возможность удостоверить для себя ее правильность или неправильность.

Идентификация и установление подлинности информации на средствах ее отображения и печати

В вычислительных системах с централизованной обработкой информации и относительно невысокими требованиями к защите установление ее подлинности на технических средствах отображения и печати гарантируется наличием системы защиты информации данной вычислительной системы. Однако с усложнением вы-

числительных систем по причинам, указанным выше, вероятность возникновения несанкционированного доступа к информации и ее модификации существенно увеличивается. Поэтому в более ответственных случаях отдельные сообщения или блоки информации подвергаются специальной защите, которая заключается в создании средств повышения достоверности информации криптографического преобразования. Установление подлинности полученной информации, включая отображение на табло и терминалах, заключается в контроле положительных результатов обеспечения достоверности информации и результатов дешифрования полученной информации до отображения ее на экране. Подлинность информации на средствах ее отображения тесно связана с подлинностью документов. Поэтому все положения, приведенные в предыдущем подразделе, справедливы и для обеспечения подлинности ее отображения. Достоверность информации на средствах отображения и печати в случае применения указанных средств защиты зависит от надежности функционирования средств, доставляющих информацию на поле отображения после окончания процедур проверки ее достоверности. Чем ближе к полю отображения (бумажному носителю) эта процедура приближается, тем достовернее отображаемая информация.

5.7. Защита информации от утечки за счет побочного электромагнитного излучения и наводок

Потенциальные угрозы

Работа средств вычислительной техники сопровождается электромагнитными излучениями и наводками на соединительные проводные линии, цепи «питания», «земля», возникающими вследствие электромагнитных воздействий в ближней зоне излучения, в которую могут попадать также провода вспомогательной и посторонней аппаратуры. Электромагнитные излучения, даже если они отвечают допустимым техническим нормам, не являются безопасными с точки зрения утечки информации и несанкционированного доступа к ней.

В некоторых случаях информацию, обрабатываемую средствами АСОИ, можно восстановить путем анализа электромагнитных излучений и наводок. Для этого необходимы их прием и декодирование. Исследования показали, что восстановление информации от некоторых средств АСОИ возможно с помощью общедоступных ра-

диоэлектронных средств. Монитор может оказаться самым слабым звеном, которое сведет на нет все меры безопасности, принятые во всех остальных частях АСОИ.

Применение в АСОИ импульсных сигналов прямоугольной формы и высокочастотной коммутации приводит к тому, что в спектре излучений будут компоненты с частотами вплоть до СВЧ. Хотя энергетический спектр сигналов убывает с ростом частоты, но эффективность излучения при этом увеличивается, и уровень излучений может оставаться постоянным до частот нескольких гигагерц. Резонансы из-за паразитных связей могут вызывать усиление излучения сигналов на некоторых частотах спектра.

Методы и средства защиты информации от побочного электромагнитного излучения и наводок информации

В целях защиты секретной информации от утечки за счет побочного электромагнитного излучения и наводок производится измерение уровня опасных сигналов. Замеры производят в нескольких точках на разных расстояниях от источника с помощью специальной аппаратуры. Если уровень сигнала на границе установленной зоны превысил допустимые значения, применяют защитные меры.

Защитные меры могут носить различный характер в зависимости от сложности, стоимости и времени их реализации, которые определяются при создании конкретной вычислительной системы. Такими мерами могут быть:

- усовершенствование аппаратуры с целью уменьшения уровня сигналов;
- установка специальных фильтров;
- применение генераторов шума;
- использование специальных экранов;
- другие меры.

В числе этих мер большие надежды возлагаются на применение в линиях и каналах связи волоконно-оптических кабелей, которые обладают следующими преимуществами:

- отсутствием электромагнитного излучения во внешнюю среду;
- устойчивостью к внешним электромагнитным излучениям;
- большой помехозащищенностью;
- скрытностью передачи;
- малыми габаритами (что позволяет прокладывать их с существующими линиями);
- устойчивостью к воздействиям агрессивной среды.

С точки зрения защиты информации волоконно-оптические кабели имеют еще одно преимущество: подключение к ним с целью перехвата передаваемых данных представляет собой значительно более сложную задачу, чем подключение к обычному проводу или кабелю с помощью индуктивных датчиков и прямого подключения. Однако замена одного кабеля другим связана с введением электрооптических и оптико-электрических преобразователей, на которые и перекладывается проблема обеспечения безопасности информации.

5.8. Методы и средства защиты информации от случайных воздействий

В целях защиты функционирования АСОИ от случайных воздействий применяются средства повышения надежности аппаратуры и программного обеспечения, а для защиты информации – средства повышения ее достоверности. Для предотвращения аварийной ситуации применяются специальные меры.

Проблема надежности автоматизированных систем решается тремя путями:

- повышением надежности деталей и узлов;
- построением надежных систем из менее надежных элементов за счет структурной избыточности (дублирование, утроение элементов, устройств, подсистем и т. п.);
- применением функционального контроля с диагностикой отказа, увеличивающего надежность функционирования системы.

Задачами функционального контроля (ФК) системы являются: своевременное обнаружение сбоев, неисправностей и программных ошибок, исключение их влияния на дальнейший процесс обработки информации и указание места отказавшего элемента, блока программы с целью последующего быстрого восстановления системы.

Существующие методы функционального контроля вычислительных систем могут быть разделены на программный, аппаратный и комбинированный (сочетание программного с аппаратным).

Сравнительная характеристика методов ФК учитывает следующие факторы:

- надежность обнаружения;
- возможность исправления ошибок после сбоев без вмешательства оператора;

- время, затрачиваемое на устранение случайных ошибок;
- количество дополнительного оборудования;
- способы применения (параллельно или с прерыванием обработки информации);
- влияние контроля на быстродействие вычислительной системы или ее производительность;
- указание места неисправности с необходимой точностью.

Программный контроль делится на программно-логический, алгоритмический и тестовый.

Наиболее распространенная форма ***программно-логического контроля*** – это двойной счет со сравнением полученных результатов.

Алгоритмический контроль заключается в том, что задача, решенная по какому-либо алгоритму, проверяется повторно по сокращенному алгоритму с достаточной степенью точности.

Программно-логический контроль позволяет надежно обнаруживать сбои, и для его осуществления не требуется дополнительного оборудования, Однако при нем более чем вдвое снижается производительность АСОИ, не обнаруживаются систематические сбои, нельзя указать место отказа и тем более сбоя, требуется дополнительная емкость памяти для программы вычислений. При алгоритмическом контроле производительность АСОИ выше, в остальном он обладает теми же недостатками и, кроме того, имеет ограниченное применение, так как не всегда удается найти для основного алгоритма сокращенный, который был бы значительно короче основного.

Тестовый контроль применяется для проверки работоспособности комплекса средств автоматизации при помощи испытательных программ.

Тестовый контроль в отличие от программно-логического проверяет не процесс переработки информации, а пребывание АСОИ или ее части в работоспособном состоянии. Кроме того, тестовый контроль не всегда обнаруживает сбои и во время проверки не может решать задачи по рабочей программе.

В настоящее время широкое применение находят методы аппаратного схемного контроля и комбинированный метод.

Аппаратный контроль в отличие от программного может обеспечивать указание о наличии сбоя или неисправности непосредственно в момент его возникновения. Аппаратный контроль в АСОИ делится на контроль по модулю; контроль при дублировании

оборудования и контроль при троировании оборудования с использованием мажоритарных элементов.

Контроль по модулю основывается на следующих принципах. Из теории чисел известно, что целое положительное число можно представить в виде сравнения:

$$\mathbf{A \equiv r_a \left(mod\, M\right)} \quad (1)$$

(считается: A сравнимо с остатком r_a модуля M), которое устанавливает следующее соотношение между числами A, r_a, и M:

$$\mathbf{A \equiv Ml + r_a}$$

где A, M, l, r_a – целые числа;
A – любое контролируемое n-разрядное число;
M – модуль, или делитель;
l – частное;
r_a – остаток от деления A на модуль M (контрольный код числа A).

При данном методе контроля каждому контролируемому члену придается еще m дополнительных разрядов, в которые записывается контрольный код, т. е. остаток r_a. Если записать все числа в виде сравнения (1), то после этого их можно будет складывать, перемножать, а результаты записывать в виде подобных сравнений:

$$\sum_{i=1}^{P} \mathbf{A_i} \equiv \sum_{i=1}^{P} \mathbf{r_{a_i}} \left(\mathbf{mod\, M}\right), \quad (2)$$

$$\prod_{i=1}^{P} \mathbf{A_i} \equiv \prod_{i=1}^{P} \mathbf{r_{a_i}} \left(\mathbf{mod\, M}\right). \quad (3)$$

Выражения (2) и (3) означают, что сумма (произведение) чисел сравнима с суммой (произведением) остатков этих чисел по модулю М.

Техническая реализация контроля по модулю заключается в разработке специальных схем, которые в технической литературе получили название «сверток». Эффективность контроля повышается с увеличением модуля. Однако с увеличением М непропорционально возрастает количество дополнительного оборудования и усложняются схемы контроля. Широкое распространение в вычислительных схемах получил контроль по модулю 2.

Дублирование оборудования позволяет путем сравнения выходных сигналов обнаружить отказ аппаратуры. Высокая эффек-

тивность такого контроля основывается на том, что вероятность одновременного отказа двух одинаковых элементов исчезающе мала. Недостатком этого метода является не всегда имеющаяся возможность определить, какой из каналов является исправным, и поэтому, чтобы процесс функционирования оставался исправным, приходится одновременно в каждом из каналов применять методы контроля, например контроль по модулю.

Троирование оборудования с элементами «голосования» позволяет наряду с увеличением вероятности безотказной работы увеличить и достоверность функционирования при помощи мажоритарных элементов. Данный метод требует, разумеется, увеличения объемов оборудования.

В настоящее время существует много разнообразных методов контроля, имеющих в зависимости от конкретных требований и условий различную степень применяемости. Некоторые из этих методов являются специализированными для определенных типов устройств и систем. Другие – приспособлены для проверки определенных видов операций и применяются в различных типах устройств.

Поскольку результат воздействия на информацию зависит от количества ошибок в данный момент времени, рассмотрим вероятность появления этих событий.

Ввод, хранение и обработка информации в АСОИ осуществляются при помощи кодов чисел и слов по определенному алгоритму. Появление сбоев приводит к тому, что в коде может возникнуть одиночная или групповая ошибка (двухкратная, трехкратная и т. д.). Ошибка может считаться одиночной, если она возникла в одном разряде кода числа или слова.

Считая ошибки в каждом разряде кода независимыми, можно определить вероятность появления ошибки і-й кратности при известной вероятности искажения одного разряда двоичного кода. В этом случае ошибки в каждом из разрядов подчиняются биномиальному распределению вероятностей. Вероятность появления однократной ошибки в n-разрядном двоичном коде может быть определена из выражения

$$\mathbf{P_1 = ng(1 - g)^{n-1}}.$$

где q – вероятность появления ошибки в отдельном разряде в течение одной операции.

Вероятность появления двухкратной ошибки:

$$P_2 = \frac{n(n-1)}{2} g^2 (1-g)^{n-2}.$$

Вероятность появления ошибок i-й кратности:

$$P_i = C_n^i g^i (1-g)^{n-1}.$$

Однако оценка значения P_i аналитическим путем связана с трудностями, которые зависят от причин, вызывающих сбои. Получение статистического материала о сбоях каждого разряда также является проблемным вопросом. Поэтому Pi может быть получено по более удобной формуле

$$P_i = \frac{n\mu_p t_{on}}{i!} e - n\mu_p t_{on},$$

где $t_{оп}$ – длительность одной операции;

μ_p – интенсивность отказов оборудования, участвующего в передаче и хранении каждого разряда двоичного кода.

С увеличением кратности ошибки вероятность ее появления уменьшается. Вероятность появления ошибки с кратностью i = 4 пренебрежимо мала. Для оценки эффективности аппаратного контроля необходимо знать вероятность обнаружения (пропуска) ошибок различной кратности при выбранном методе контроля. В связи с этим общая вероятность пропуска ошибки

$$P_{np} = \sum_{n=1}^{n} P_i P_{M.np.i}$$

где P_i – вероятность появления ошибки i-й кратности;

$P_{м.пр.i}$ – вероятность пропуска ошибки i-й кратности при выбранном методе аппаратного контроля.

Способность средств ФК обеспечить своевременно (до начала последующей обработки) обнаружение и блокировку ошибок заданной кратности определяет уровень достоверности контроля обработки информации. Существенную роль для качества ФК играет плотность распределения его средств обнаружения ошибок по всей «площади» контролируемой вычислительной системы, т. е. полнота

ее охвата функциональным контролем. В связи с этим при создании вычислительных систем используются следующие показатели качества ФК:

1) время обнаружения и локализации отказов аппаратуры с точностью до съемного элемента:

$$\mathbf{T_{обн}} = \frac{\sum_{i=1}^{m} \mathbf{t_{обн_i}}}{\mathbf{m}},$$

где m – число экспериментов;
i – номер эксперимента;
$i_{обні}$ – время обнаружения отказа в i-м эксперименте;

2) полнота контроля функционирования вычислительной системы:

$$\mathbf{K_п} = \frac{\lambda_K}{\lambda_o},$$

где λ_k – суммарная интенсивность появления отказов составных частей, охваченных контролем;

λ_0 – суммарная интенсивность отказов всех составных частей вычислительной системы;

3) достоверность контроля:

$$\mathbf{K_Д} = \frac{\mathbf{n_{обн}}}{\mathbf{n_{пр}}},$$

где $n_{обн}$ – общее число отказов, обнаруженных данной системой функционального контроля;

$n_{пр}$ – общее число отказов проведения ФК при условии появления или искусственного введения отказов в каждом опыте.

Одним из основных условий эффективного функционирования автоматизированной системы является обеспечение требуемого уровня достоверности информации. Под достоверностью информации в АСОИ понимают некоторую функцию вероятности ошибки, т. е. события, заключающегося в том, что реальная информация в системе о некотором параметре не совпадает в пределах заданной точности с истинным значением.

Необходимая достоверность достигается использованием различных методов, реализация которых требует введения в системы обработки данных информационной, временной или структурной избыточности. Достоверность при обработке данных достигается путем контроля и выявления ошибок в исходных и выводимых данных, их локализации и исправления. Условие повышения достоверности – снижение доли ошибок до допустимого уровня. В конкретных АСОИ требуемая достоверность устанавливается с учетом нежелательных последствий, к которым может привести возникшая ошибка, и тех затрат, которые необходимы для ее предотвращения.

Методы контроля при обработке информации в АСОИ классифицируют по различным параметрам:

– по количеству операций, охватываемых контролем, – единичный (одна операция), групповой (группа последовательных операций), комплексный (контролируется, например, процесс сбора данных);

– по частоте контроля – непрерывный, циклический, периодический, разовый, выборочный, по отклонениям;

– по времени контроля – до выполнения основных операций, одновременно с ними, в промежутках между основными операциями, после них;

– по виду оборудования контроля – встроенный, контроль с помощью дополнительных технических средств, безаппаратный;

– по уровню автоматизации – «ручной», автоматизированный, автоматический.

– Различают системные, программные и аппаратные методы контроля достоверности.

Системные методы включают:

- оптимизацию структуры обработки;
- поддержание характеристик оборудования в заданных пределах;
- повышение культуры обработки;
- обучение и стимулирование обслуживающего персонала;
- создание оптимального числа копий и (или) предысторий программ исходных и текущих данных;
- определение оптимальной величины пакетов данных и скорости первичной обработки, процедур доступа к массивам данных и др.

Программные методы повышения достоверности информации состоят в том, что при составлении процедур обработки данных в них предусматривают дополнительные операции, имеющие мате-

матическую или логическую связь с алгоритмом обработки данных. Сравнение результатов этих дополнительных операций с результатами обработки данных позволяет установить с определенной вероятностью наличие или отсутствие ошибок. На основании этого сравнения, как правило, появляется возможность исправить обнаруженную ошибку.

Аппаратные методы контроля и обнаружения ошибок могут выполнять практически те же функции, что и программные. Аппаратными методами обнаруживают ошибки быстрее и ближе к месту их возникновения, а также ошибки, недоступные для программных методов.

Все перечисленные методы контроля обработки данных базируются на использовании определенной избыточности. При этом различают методы контроля со структурной, временной и информационной избыточностью.

Структурная избыточность требует введения в состав АСОИ дополнительных элементов (резервирование информационных массивов и программных модулей, реализация одних и тех же функций различными программами, схемный контроль в технических средствах АСОИ и т.д.).

Временная избыточность связана с возможностью неоднократного повторения определенного контролируемого этапа обработки данных. Обычно этап обработки повторяют неоднократно и результаты обработки сравнивают между собой. В случае обнаружения ошибки производят исправления и повторную обработку.

Информационная избыточность может быть естественной и искусственной. Естественная информационная избыточность отражает объективно существующие связи между элементами обработки, наличие которых позволяет судить о достоверности информации. Искусственная информационная избыточность характеризуется введением дополнительных информационных разрядов в цифровом представлении обрабатываемых данных и дополнительных операций в процедуре их обработки, имеющих математическую или логическую связь с алгоритмом обработки данных. На основании анализа результатов дополнительных операций и процедур обработки данных, а также дополнительных информационных разрядов выявляется наличие или отсутствие ошибок определенного типа, а также возможности их исправления.

В зависимости от характера информации, особенностей алгоритмов системы, а также от задач, стоящих перед ее адресатами,

можно определить следующие зависимости содержания информации от ошибок при ее передаче:

- смысловой объем информации в сообщении уменьшается пропорционально числу искаженных разрядов в кодовой комбинации данного сообщения;
- искажение одного или нескольких разрядов приводит почти к полной потере остальной части информации, содержащейся в смысловом отрезке информации в сообщении.

Проанализируем способность средств функционального контроля и повышения достоверности информации к защите от случайных разрушений, модификации и утечки информации.

Известно, что отказы, сбои в аппаратуре и ошибки в программном обеспечении могут привести к нарушению функционирования вычислительной системы, к разрушению и изменению информации на ложную. Анализ принятого в современных автоматизированных системах представления информации в цифровом виде показывает, что на один байт приходится одна буква, цифра или символ. Одно слово может занимать в русском языке от 1 до 20 букв. Каждой букве, цифре и символу присвоены двоичные коды. Таблица кодов составлена так, что пропадание или появление одной 1 в разрядах приводит к изменению одной буквы (символа, цифры) на другую. При этом можно утверждать, что в этом случае имеет место однократная ошибка, которая относительно легко обнаруживается простыми средствами аппаратного контроля (например, контролем по модулю 2). В случае же появления двухкратной ошибки в байте измениться могут два разряда. Контроль по модулю 2 этого не обнаруживает, что уже может привести к незаметному изменению одной буквы на другую. В русском языке существуют слова, которые меняют свой смысл на другой при замене одной буквы другой. Это и есть модификация информации. При трехкратной ошибке вероятность этого события, естественно, увеличивается. Правда, вероятность появления трехкратной ошибки меньше по сравнению с двухкратной, но это слабый аргумент, так как ее величина при большом количестве аппаратных средств, интенсивности и накоплении их отказов может быть весьма ощутимой на большом отрезке времени работы вычислительной системы.

Если рассматривать искажение информации (без ее модификации) как разрушение информации, условием его возникновения может считаться однократная ошибка, несмотря на то, что пропадание одной буквы не всегда ведет к потере информации.

Для возникновения случайной утечки информации при ее обработке в вычислительной системе необходимо, чтобы в результате случайных воздействий был перепутан адрес получателя или в правильный адрес была введена другая информация, для него не предназначенная. В первом случае, например, заменилась одна из букв другой (модификация), во втором – адресация ячеек памяти ОЗУ, из которого считывалась информация до ее передачи получателю (тоже модификация).

Таким образом, можно полагать, что в нашем случае утечка информации – это частный случай ее модификации. Следовательно, средства функционального контроля в принципе защищают информацию от случайных разрушений, модификации и утечки. Рассматривая вероятность появления этих событий при отсутствии функционального контроля, заметим, что для разрушения информации (какой-то ее части) достаточно однократной ошибки, для модификации и утечки необходимы дополнительные условия. Для наступления события, выражающегося в случайной распечатке или отображении информации на средствах, не предназначенных для этой цели, необходимо, чтобы из потока ошибок появилась такая, при которой какая-либо команда изменилась на команду «печать» или «отображение», и по санкционированной команде информация была бы взята не по тому адресу из памяти или была направлена не на то техническое средство системы. Возможны и другие ситуации. Для наступления события, выражающегося в модификации информации, необходимо, чтобы из потока ошибок появилась такая ошибка или группа ошибок, благодаря которым действительная информация изменилась бы на ложную, была бы не обнаружена и подверглась бы дальнейшей обработке.

Вероятность указанных событий зависит от многих факторов, но, анализируя приведенные относительные условия их наступления, можно дать им некоторую сравнительную оценку. Вероятность разрушения информации от случайных воздействий больше, чем ее модификации, а вероятность модификации информации больше вероятности ее утечки. Эта оценка необходима для выработки подхода к функциональному контролю с позиций защиты информации, который выражается в предъявлении к средствам функционального контроля дополнительных требований, выполнение которых может потребовать дополнительных средств. Дополнительные требования заключаются в реализации уменьшения вероятности модификации и утечки информации существующими средствами

повышения надежности и достоверности информации. Для выполнения этой задачи в настоящее время применяются специальные системотехнические решения:

- изоляция областей доступа к информации;
- специальная организация работы с данными, хранящимися в памяти вычислительной системы.

Изоляция областей доступа к информации вычислительной системы осуществляется также в целях поддержки разграничения санкционированного доступа.

В целях исключения несанкционированного обмена между пользователями рекомендуется при проектировании сводить к минимуму число общих для них параметров и характеристик механизма защиты. Несмотря на то, что функции операционной системы и системы разрешения доступа перекрываются, система разрешения доступа должна конструироваться как изолированный программный модуль, т. е. защита должна быть отделена от функций управления данными. Выполнение этого принципа позволяет программировать систему разрешения доступа как автономный пакет программ с последующей независимой отладкой и проверкой. Данный пакет программ должен размещаться в защищенном поле памяти, чтобы обеспечить системную локализацию попыток проникновения извне. Всякая попытка проникновения со стороны, в том числе операционной системы, должна автоматически фиксироваться, документироваться и отвергаться, если вызов не предусмотрен.

Естественно, что реализация обособленного механизма защиты потребует увеличения объемов программ. При этом может возникнуть дублирование управляющих и вспомогательных программ, а также необходимость в разработке самостоятельных вызываемых функций.

Информация, содержащаяся в вычислительной системе, может быть поделена между пользователями, что требует размещения ее в непересекающихся областях, отведенных для ее хранения. В каждой из этих областей хранится совокупность информационных объектов, подлежащих в равной степени защите. В процессе эксплуатации системы необходимо обеспечить надежное разграничение доступа к информации. Для этой цели помимо организации доступа с помощью системы паролей в систему при проектировании закладываются дополнительные меры по изоляции областей доступа, нарушение которых по причине отказов и программных ошибок не приводило бы к несанкционированному доступу к информации.

В случае наличия в системе общего поля памяти, которое необходимо для решения поставленных задач, схемы защиты допускают обмен информацией между пользователями. Тогда применяются списковые и мандатные схемы защиты. Списковые схемы – те, в которых система охраны снабжается списком всех лиц, имеющих право доступа к информации (для получения права доступа достаточно предъявить свой идентификатор). Мандатные схемы – те, в которых система охраны реализует только один вид мандата, а пользователь должен иметь набор мандатов для доступа к каждому из необходимых ему объектов.

В списковой схеме при каждом обращении просмотр списка повторяется, т. е. доступ сопряжен с процедурой ассоциативного поиска. В мандатных схемах пользователь сам решает, какой объект ему нужен, и выбирает необходимый мандат или некоторое их количество из тех, к которым он допущен.

Анализ изложенного позволяет отметить следующие особенности требований к средствам ФК и повышению достоверности с позиций защиты информации от НСД:

- определенная целенаправленность мероприятий по ФК и повышению достоверности, выраженная в увязке технического представления информации с ее смыслом и содержанием;
- определение зависимости безопасности информации от кратности ошибок при ее обработке.

Наибольшую опасность составляют многократные ошибки, приводящие к модификации самой информации и команд, осуществляющих ее обработку. При этом уровень безопасности информации находится в прямой зависимости от количества одновременно возникающих ошибок. Способность средств функционального контроля к их обнаружению и определяет уровень безопасности информации. Поскольку вероятность появления четырехкратной ошибки относительно мала, то вероятность обнаружения двух- и трехкратных ошибок и будет мерой безопасности информации от отказов аппаратуры. Сложнее эта проблема с программными ошибками, заложенными еще на этапе проектирования программного обеспечения.

Анализ приведенных средств ФК и повышения достоверности информации, а также специальных технических решений показывает, что с увеличением количества байтов в слове вероятность его модификации от случайных воздействий уменьшается, так как увели-

чивается кодовое расстояние по отношению к другим словам, командам, сообщениям. В этом смысле наименее устойчивы короткие слова и особенно цифры. Приведенный метод защиты от переадресации памяти одному адресу присваивает дополнительную специальную процедуру и код, что, естественно, уменьшает вероятность случайного формирования такой процедуры и обращений по этому адресу других процедур и команд. Поэтому в целях повышения безопасности информации, а следовательно, и надежности вычислительной системы следует пересмотреть методы кодирования символов, команд и адресов (включая адреса устройств и процессов) на предмет увеличения кодового расстояния между ними и уменьшения вероятности превращения одной команды или адреса в другие, предусмотренные в данной системе для других целей. Это позволит не разрабатывать некоторые сложные специальные программы. которые не устраняют причины и условия появления случайных событий, а лишь обнаруживают их, да и то не всегда и в неподходящее время, т. е. когда событие уже произошло и основная задача по его предупреждению не выполнена.

5.9. Методы защиты информации от аварийных ситуаций

Защита информации от аварийных ситуаций заключается в создании средств предупреждения, контроля и организационных мер по исключению НСД на комплексе средств автоматизации в условиях отказов его функционирования, отказов системы защиты информации, систем жизнеобеспечения людей на объекте размещения и при возникновении стихийных бедствий.

Практика показывает, что хотя аварийная ситуация – событие редкое (вероятность ее появления зависит от многих причин, в том числе не зависящих от человека, и эти причины могут быть взаимосвязаны), защита от нее необходима, так как последствия в результате ее воздействия, как правило, могут оказаться весьма тяжелыми, а потери – безвозвратными. Затраты на защиту от аварийных ситуаций могут быть относительно малы, а эффект в случае аварии – большим.

Отказ функционирования АСОИ может повлечь за собой отказ системы защиты информации, может открыться доступ к ее носителям, что может привести к преднамеренному разрушению, хищению или подмене носителя. Несанкционированный доступ к

внутреннему монтажу аппаратуры может привести к подключению посторонней аппаратуры, разрушению или изменению принципиальной электрической схемы.

Отказ системы жизнеобеспечения может привести к выводу из строя обслуживающего и контролирующего персонала. Стихийные бедствия: пожар, наводнение, землетрясение, удары молнии и т. д. – могут также привести к указанным выше последствиям. Аварийная ситуация может быть создана преднамеренно нарушителем. В последнем случае применяются организационные мероприятия.

На случай отказа функционирования АСОИ подсистема контроля вскрытия аппаратуры снабжается автономным источником питания. Для исключения безвозвратной потери информации носители информации дублируются и хранятся в отдельном удаленном и безопасном месте. Для защиты от утечки информация должна храниться в закрытом криптографическим способом виде. В целях своевременного принятия мер по защите системы жизнеобеспечения устанавливаются соответствующие датчики, сигналы с которых поступают на централизованные системы контроля и сигнализации.

Наиболее частой и типичной естественной угрозой является пожар. Он может возникнуть по вине обслуживающего персонала, при отказе аппаратуры, а также в результате стихийного бедствия.

5.10. Организационные мероприятия по защите информации

Организационные мероприятия по защите информации в АСОИ заключаются в разработке и реализации административных и организационно-технических мер при подготовке и эксплуатации системы.

Организационные меры, по мнению зарубежных специалистов, несмотря на постоянное совершенствование технических мер, составляют значительную часть (50%) системы защиты. Они используются тогда, когда вычислительная система не может непосредственно контролировать использование информации. Кроме того, в некоторых ответственных случаях в целях повышения эффективности защиты полезно иногда технические меры продублировать организационными.

Организационные меры по защите систем в процессе их функционирования и подготовки охватывают решения и процеду-

ры, принимаемые руководством организации – потребителя системы. Хотя некоторые из них могут определяться внешними факторами, например законами или правительственными постановлениями, большинство проблем решается внутри организации в конкретных условиях.

В большинстве исследований, посвященных проблемам защиты информации, и в существующих зарубежных публикациях основное внимание уделялось либо правовому аспекту и связанным с ним социальным и законодательным проблемам, либо техническим приемам решения специфических проблем защиты. По сравнению с ними организационным вопросам недоставало той четкой постановки, которая присуща техническим проблемам, и той эмоциональной окраски, которая свойственна правовым вопросам.

Составной частью любого плана мероприятий должно быть четкое указание целей, распределение ответственности и перечень организационных мер защиты. Конкретное распределение ответственности и функций по реализации защиты от организации к организации может изменяться, но тщательное планирование и точное распределение ответственности являются необходимыми условиями создания эффективной жизнеспособной системы защиты.

Организационные меры по защите информации в АСОИ должны охватывать этапы проектирования, разработки, изготовления, испытаний, подготовки к эксплуатации и эксплуатации системы.

В соответствии с требованиями технического задания в организации проектировщике наряду с техническими средствами разрабатываются и внедряются организационные мероприятия по защите информации на этапе создания системы. Под этапом создания понимаются проектирование, разработка, изготовление и испытание системы. При этом следует отличать мероприятия по защите информации, проводимые организацией-проектировщиком, разработчиком и изготовителем в процессе создания системы и рассчитанные на защиту от утечки информации в данной организации, и мероприятия, закладываемые в проект и разрабатываемую документацию на систему, которые касаются принципов организации защиты в самой системе и из которых вытекают организационные мероприятия, рекомендуемые в эксплуатационной документации организацией-разработчиком, на период ввода и эксплуатации системы. Выполнение этих рекомендаций есть определенная гарантия защиты информации в АСОИ.

К организационным мероприятиям по защите информации в процессе создания системы относятся:

- организация разработки, внедрения и использования средств;
- управление доступом персонала на территорию, в здания и помещения;
- введение на необходимых участках проведения работ с режимом секретности;
- разработка должностных инструкций по обеспечению режима секретности в соответствии с действующими в стране инструкциями и положениями;
- при необходимости выделение отдельных помещений с охранной сигнализацией и пропускной системой;
- разграничение задач по исполнителям и выпуску документации;
- присвоение грифа секретности материалам, документации, аппаратуре и хранение их под охраной в отдельных помещениях с учетом и контролем доступа исполнителей;
- постоянный контроль за соблюдением исполнителями режима и соответствующих инструкций;
- установление и распределение ответственных лиц за утечку информации.

Организационные мероприятия, закладываемые в инструкцию по эксплуатации на систему и рекомендуемые организации-потребителю, должны быть предусмотрены на периоды подготовки и эксплуатации системы.

Указанные мероприятия как метод защиты информации предполагают систему организационных мер, дополняющих и объединяющих перечисленные выше технические меры в единую систему безопасности информации.

5.11. Организация информационной безопасности компании

При организации информационной безопасности компании принимается политика безопасности. На основе принятой политики информационной безопасности компании определяются наиболее опасные угрозы, пути их реализации и способы нейтрализации характерные для конкретной автоматизированной системы обработки информации (АСОИ).

Таблица 5.1

Угрозы системе электронного документооборота (при автоматизированной обработке)

Угроза	Атака	Время проведения атаки	Объект атаки (местоположение атакуемого)	Субъект атаки (местоположение атакующего)	Код угрозы
Модификация электронных документов (ЭД)	Изменение ПО	Вне процесса функционирования системы	Любая станция ЛВС	Эта же станция ЛВС	И1
				Любая станция ЛВС → Сервер (через LOGIN SCRIPT)	
			Почтовый сервер	Почтовый сервер	
				Любая станция ЛВС	
			Сервер	С любой станции ЛВС	
	Неправильный ввод ЭД	В процессе функционирования системы	Любая станция ЛВС	Эта же станция ЛВС	И2
				Любая станция ЛВС → Сервер (через LOGIN SCRIPT)	
	Внедрение программной закладки	В процессе функционирования системы	Любая станция ЛВС	Эта же станция ЛВС	И3
				Любая станция ЛВС → Сервер (через LOGIN SCRIPT)	
			Почтовый сервер	Почтовый сервер	
				Любая станция ЛВС	
			Сервер	Любая станция ЛВС	
	Перехват ЭД	В процессе функционирования системы	Сервер	Любая станция ЛВС	И4
		В процессе передачи данных	Сеть передачи данных	Промежуточные узлы	И5

Угроза	**Атака**	**Время проведения атаки**	**Объект атаки (местоположение атакуемого)**	**Субъект атаки (местоположение атакующего)**	**Код угрозы**
			Модем	Промежуточные узлы	
Ввод несуществующего ЭД	Изменение ПО	Вне процесса функционирования системы	Любая станция ЛВС	Эта же станция ЛВС	*И1*
				Любая станция ЛВС → Сервер (через LOGIN SCRIPT)	
			Почтовый сервер	Почтовый сервер	
			Сервер	Любая станция ЛВС	
				Любая станция ЛВС	
	Внедрение программной закладки	В процессе функционирования системы	Любая станция ЛВС	Эта же станция ЛВС	*И3*
				Любая станция ЛВС → Сервер (через LOGIN SCRIPT)	
			Почтовый сервер	Почтовый сервер	
			Сервер	Любая станция ЛВС	
				Любая станция ЛВС	
	«Ручной ввод»	В процессе функционирования системы	Сервер	Любая станция ЛВС	*И6*
			Почтовый сервер	Почтовый сервер	
				Любая станция ЛВС	
			ЛВС	Любая станции ЛВС	
		В процессе передачи данных	Сеть передачи данных	Промежуточные узлы	*И7*
			Модем	Промежуточные узлы	
Нарушение конфиденциальности ЭД	Изменение ПО	Аналогично предыдущему случаю			
	Внедрение программной закладки				
	Просмотр с экрана	В процессе функционирования	Любая станция ЛВС	Любая станция ЛВС	*И8*

Угроза	Атака	Время проведения атаки	Объект атаки (местоположение атакуемого)	Субъект атаки (местоположение атакующего)	Код угрозы
		системы	Почтовый сервер	Почтовый сервер	
	Перехват ЭД	В процессе функционирования системы	ЛВС	Любая станция ЛВС	И4
		В процессе передачи данных	Сеть передачи данных	Промежуточные узлы	И5
			Модем		
	Несанкционированное копирование	Вне процесса функционирования системы	Сервер	Любая станция ЛВС	И9
Отказ от факта получения ЭД	Изменение ПО	В процессе функционирования системы	Любая станция ЛВС	Любая станция ЛВС	И3
			Почтовый сервер	Почтовый сервер	
		В процессе передачи данных	Внешняя организация	Внешняя организация	
Отказ от авторства ЭД	Аналогично предыдущему случаю				
Дублирование ЭД	Изменение ПО	Аналогично предыдущему случаю			
	Внедрение программной закладки				
	«Повтор в сети»	В/вне процесса функционирования системы	Сервер	Любая станция сети	И12
			ЛВС	Любая станция сети	
			Сеть передачи данных	Промежуточные узлы	

Угроза	Атака	Время проведения атаки	Объект атаки (местоположение атакуемого)	Субъект атаки (местоположение атакующего)	Код угрозы
			Модем		
Потеря или уничтожение ЭД	Перехват ЭД	В процессе функционирования системы	Сервер	Любая станция сети	И4
			ЛВС	Любая станция сети	
			Сеть передачи данных	Промежуточные узлы	
			Модем		
	Несанкционированное копирование	Вне процесса функционирования системы	Сервер	Любая станция ЛВС	И9
	Изменение ПО	Аналогично предыдущему случаю			
	Внедрение программн. закладки				
НСД к АРМ системы электронного документооборота	НСД	В/вне процесса функционирования системы	Любая станция ЛВС	Эта же станция ЛВС	И13
				Любая станция ЛВС → Сервер (через LOGIN SCRIPT)	
			Почтовый сервер	Почтовый сервер	
				Любая станция ЛВС	
			Сервер	Любая станция ЛВС	
			Любая станция ЛВС	Из внешней сети (Internet)	
НСД к каналу передачи данным	НСД к каналу	В процессе функционирования системы	ЛВС	Любая станция сети	И14
		В процессе передачи данных	Сеть передачи данных	Промежуточный узел	И15

Угроза	**Атака**	**Время проведения атаки**	**Объект атаки (местоположение атакуемого)**	**Субъект атаки (местоположение атакующего)**	**Код угрозы**
			Модем		
Нападение из внешней сети	Атака из внешней сети	В/Вне процесса функционирования системы	Сервер		И18
			Станция сети		
			Модем		
			Маршрутизатор		
Нарушение работоспособности процесса функционирования системы	Изменение ПО, изменение конфигурации аппаратных средств, внедрение программных закладок	В/Вне процесса функционирования системы	На всех технологических участках	На всех технологических участках	И17
Несанкционированное конфигурирование маршрутизаторов	Несанкционированное конфигурирование маршрутизаторов	В/Вне процесса функционирования системы	Маршрутизаторы	Любая станция сети передачи данных	И18

Таблица 5.2

Меры защиты от реализации угроз

Код угрозы	Меры защиты		
	Организационные	**Физические**	**Технические**
И1	1. Инструкция по внесению изменений в конфигурации ПО 2. Инструкции пользователям 3. Задание ответственности за нарушение установленных правил 4. Инструкция по изменению полномочий пользователей	1. Разграничение доступа в помещения 2. Физическая защита помещений	1. Запрет загрузки АРМ с гибких магнитных дисков 2. Защита исполняемых файлов от изменения 3. Замкнутая среда разрешенных для запуска программ для каждого пользователя системы 4. Периодический контроль целостности исполняемых файлов и настроек программных средств 5. Использование ЭЦП 6. Регистрация событий
И3	1. Инструкция по внесению изменений в конфигурации ПО 2. Инструкции пользователям 3. Задание ответственности за нарушение установленных правил	1. Разграничение доступа в помещения 2. Физическая защита помещений	1. Запрет загрузки АРМ с гибких магнитных дисков 2. Защита исполняемых и системных файлов от изменения 3. Замкнутая среда разрешенных для запуска программ для каждого пользователя системы 4. Периодический контроль целостности системы 5. Регистрация событий 6. Использование средств обнаружения нападений
И5	1. Договор с внешней организаций	1. За рамками полномочий организации	1. Преобразование информации 2. Использование ЭЦП 3. Контроль времени

Код угрозы	**Меры защиты**		
	Организационные	**Физические**	**Технические**
И6	1. Инструкция по изменению полномочий пользователей 2. Инструкции пользователям 3. Задание ответственности за нарушение установленных правил	1. Изоляция защищаемой системы от других систем организации	1. Ограничение доступа к РС, серверу и т.п. 2. Разрешение доступа к серверу только с защищенных рабочих станций 3. Ограничение доступа к серверу по номеру сетевой карты 4. Запрет одновременного доступа к серверу пользователей с одинаковым именем 5. Регистрация событий 6. Использование средств обнаружения нападений
И8	1. Инструкции пользователям 2. Задание ответственности за нарушение установленных правил	1. Разграничение доступа в помещения 2. Защита помещений	1. Хранитель экрана 2. Ограничение доступа к РС 3. Разграничение доступа к РС
И9	1. Инструкции пользователям 2. Задание ответственности за нарушение установленных правил	1. Разграничение доступа в помещения 2. Физическая защита помещений	1. Ограничение доступа к серверу по номеру сетевой карты 2. Разрешение доступа к серверу только с защищенных рабочих станций 3. Запрет одновременного доступа к серверу пользователей с одинаковым именем 4. Преобразование информации 5. Защита консоли сервера 6. Регистрация событий 7. Использование средств обнаружения нападений

Код уг-розы	**Меры защиты**		
	Организационные	**Физические**	**Технические**
И11	1. Инструкции пользователям 2. Задание ответственности за нарушение установленных правил	1. Изоляция защищаемой системы от других систем организации	1. Ограничение доступа к РС 2. Разграничение доступа к РС 3. Регистрация событий 4. Использование средств обнаружения нападений
И12	1. Инструкции пользователям 2. Задание ответственности за нарушение установленных правил 3. Ведение архивов ЭПД и ЭД	1. Изоляция защищаемой системы от других систем организации	1. Квитирование 2. ЭЦП 3. Контроль времени 4. Регистрация событий
И13	1. Инструкции пользователям 2. Задание ответственности за нарушение установленных правил 3. Инструкция по использованию СЗИ от НСД 4. Ограничение людей, имеющих право конфигурировать маршрутизаторы	1. Разграничение доступа в помещения 2. Физическая защита помещений 3. Изоляция защищаемой системы от других систем организации	1. Ограничение доступа к РС, серверу 2. Разграничение доступа пользователей к РС, серверу 3. Регистрация событий 4. Хранитель экрана 5. Изменение стандартного имени администратора системы защиты 6. Разрешение работы в сети только одного администратора системы защиты или администратора сети 7. Владельцем всех исполняемых файлов в системе, а также критических настроек должен быть администратор системы защиты 8. Использование средств обнаружения нападений 9. Использование межсетевых экранов Использование антивирусных программ

Код угрозы	**Меры защиты**		
	Организационные	**Физические**	**Технические**
			10. Использование всех встроенных в маршрутизаторы средств защиты
И14	1. Инструкции пользователям 2. Задание ответственности за нарушение установленных правил	1. Защита кабельной системы	Нет
И15	1. За рамками полномочий ОРГАНИЗАЦИИ		
И16	1. Инструкции пользователям 2. Задание ответственности за нарушение установленных правил	1. Разграничение доступа в помещения 2. Физическая защита помещений	1. Ограничение доступа к архиву ЭПД 2. Резервное копирование 3. Использование антивирусных программ
И17	Все меры	Все меры	Все меры
И18	1. Инструкция по использованию Интернет 2. Договор с внешней организацией 3. Инструкции пользователям 4. Задание ответственности за нарушение установленных правил		1. Ограничение числа используемых модемов 2. Физическая изоляция РС для доступа в глобальные сети от АРМ системы ЭП и ЭД 3. Ограничение доступа к РС, имеющим модемы 4. Регистрация событий 5. Использование средств обнаружения нападений 6. Использование межсетевых экранов 7. Использование всех встроенных в маршрутизаторы средств защиты

5.12. Выбор средств информационной безопасности

В настоящее время без применения средств и методов защиты информации не обходится ни одна отрасль экономической деятельности человека. Современный отечественный и зарубежный рынок представляет большое количество всевозможных программных и аппаратных средств, направленных на защиту информации. Финансовые затраты на приобретение и содержание данных средств колеблются в больших пределах. Поэтому актуальным стал вопрос об оптимальном выборе средства защиты информации, при этом, чтобы оно удовлетворяло как возрастающим требованиям к защите информации, так и имело приемлемую цену.

Очевидно, что ожидаемая полная стоимость защиты информации слагается: с одной стороны, из ожидаемых потерь от реализации злоумышленником угроз информации и, с другой стороны, затрат на приобретение и содержание средств защиты. График зависимости ожидаемой полной стоимости защиты информации от затрат на ее приобретение, содержание и стоимости ущерба от реализации угроз информации показан на рис. 5.3.

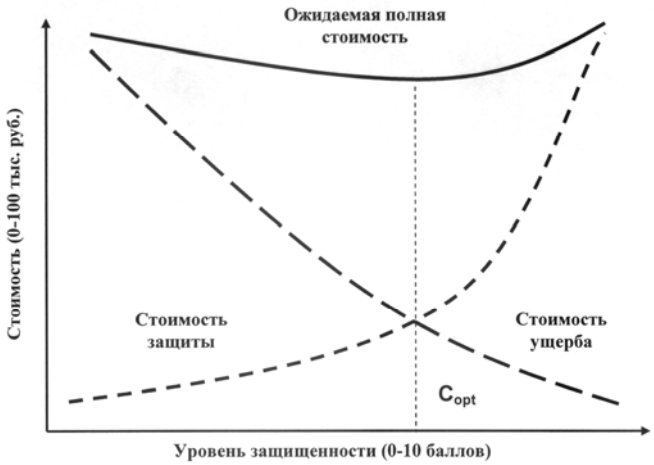


Рис. 5.3. **График зависимости ожидаемой полной стоимости защиты информации от затрат на ее приобретение, содержание и стоимости ущерба от реализации угроз информации**

Совершенно очевидно, что оптимальным решением проблемы защиты информации было бы выделение средств в размере $\mathbf{C_{opt}}$, поскольку именно при этом обеспечивается минимизация общей стоимости защиты информации.

Решение вопроса оценки ожидаемых потерь при нарушении защищенности информации принципиально может быть получено лишь тогда, когда речь идет о защите информации, которую как-то можно оценить, в основном, промышленной, коммерческой и им подобной, хотя и здесь встречаются весьма серьезные трудности. Что касается оценки ущерба при нарушении средств защиты информации, содержащей государственную, военную и им подобную тайну, то здесь до настоящего времени строгие подходы к ее получению не найдены.

Для определения затрат на приобретение и содержание средств, обеспечивающих требуемый уровень защищенности информации, необходимо, рассмотрев предполагаемые угрозы информации, выбрать те, которые действительно могут иметь место в конкретном случае. Необходимо определить уровень ущерба от реализации каждой из этих угроз.

Итак, предположим, что известно **n** видов угроз информации и ожидаемый уровень ущерба $\mathbf{r_j}$ ($\mathbf{j = \overline{1,n}}$) от реализации каждой из них в течение определенного срока (срока планирования). Кроме того, имеется перечень из m устройств, относительно которых известны затраты на содержание устройства c_i,($\mathbf{i = \overline{1,m}}$) в течение данного срока, которые могут включать цену устройства, оплату труда обслуживающего персонала, расход на техническое обеспечение и др., и кроме того известен уровень нейтрализации устройством каждой из угроз p_{ij} ($\mathbf{i = \overline{1,m}}$; $\mathbf{j = \overline{1,n}}$).

Обозначим за A_{ij} событие, при котором устройство i нейтрализует угрозу j, и пусть известны вероятности $\mathbf{P(A_{ij}) = p_{ij}}$ для всех возможных i и j.

Следовательно, чтобы рассчитать наиболее рациональные затраты на защиту информации, необходимо минимизировать функцию

$$\mathbf{F(x)} = \sum_{\mathbf{i}=1}^{\mathbf{m}} \mathbf{x_i c_i} + \sum_{\mathbf{j}=1}^{\mathbf{n}} \mathbf{r_j}\left[1 - \mathbf{P(Y_1 A_{1j} + Y_2 A_{2j} + .. + Y_m A_{mj})}\right], \quad (1)$$

где $\mathbf{x_i}$ - булевы переменные (0 - устройство решено не использовать и 1 - принято решение об использовании устройства), $\mathbf{Y_i}$ - либо достоверное событие (если устройство будет использовано), либо невозможное (устройство использовано не будет). Первая сумма является затратами на защиту информации, вторая - потерями от реализации угроз при достигнутом уровне защиты.

События A_{ij} независимы. Известно, что вероятность суммы независимых случайных событий $\mathbf{X_1, X_2, .., X_n}$ равна

$$\begin{aligned}&\mathbf{P(X_1 + X_2 + X_3 + ... + X_n) = P(X_1) + P(X_2)(1 - P(X_1)) +}\\&\mathbf{+ P(X_3)(1 - P(X_1))(1 - P(X_2)) + ...}\\&\mathbf{... + P(X_n)(1 - P(X_1))(1 - P(X_2))...(1 - P(X_1))\,.}\end{aligned} \qquad (2)$$

С учетом (2) формула (1) примет вид:

$$\begin{aligned}\mathbf{F(x)} = \sum_{\mathbf{i}=1}^{\mathbf{m}} \mathbf{x_i c_i} + \sum_{\mathbf{j}=1}^{\mathbf{n}} \mathbf{r_j}\{1 - [&(\mathbf{x}_1\mathbf{P(A_{1j})} + \mathbf{x}_2\mathbf{P(A_{2j})}(1 - \mathbf{x}_1\mathbf{P(A_{1j})}) +\\&+ \mathbf{x}_3\mathbf{P(A_{3j})}(1 - \mathbf{x}_1\mathbf{P(A_{1j})})(1 - \mathbf{x}_2\mathbf{P(A_{2j})}) + ..\\&+ \mathbf{x_m P(A_{mj})}(1 - \mathbf{x}_1\mathbf{P(A_{1j})})(1 - \mathbf{x}_2\mathbf{P(A_{2j})}) \cdot ... \cdot (1 - \mathbf{x}_{m-1}\mathbf{P(A_{m-1,j})})]\}\end{aligned}$$

Если минимизировать функцию $\mathbf{F(x)}$ относительно переменных x_i, то можно выявить, какие из устройств следует использовать, чтобы общие расходы на защиту информации и само значение затрат (в частности, затрат на обеспечение безопасности и потерь от реализации угроз) были минимальны.

В расчеты можно ввести такой параметр, как время. Тогда расход на содержание устройства c_i можно представить в виде двух составляющих: цена устройства (если требуется его приобретение) и затраты на обслуживание. Затраты на обслуживание вычисляются как произведение времени на затраты в единицу времени. Величину r_j можно представить как произведение трех величин: времени планирования, частоты реализации угрозы и финансового ущерба от реализации одной угрозы.

На основе вышесказанного следует, что для экономически выгодного приобретения набора средств защиты информации компьютерных систем необходимо решить ряд задач:

1. Рассмотрев предполагаемые угрозы информации, выбрать те, которые действительно могут иметь место в конкретном случае, и определить уровень ущерба от реализации каждой из этих угроз.

2. Для определения уровня ущерба от реализации каждой из угроз экономической информации необходимо иметь достаточное количество статистических данных о проявлениях этих угроз и их последствиях. По России такая статистика практически отсутствует, однако некоторые банковские структуры ее собирают. В США же, сбору и обработке этих данных уделяется большое внимание. В результате этого получено большое количество данных по ряду угроз, которые могут быть положены в основу данных расчетов.

3. Решение вопроса оценки ожидаемых потерь, при нарушении защищенности информации, принципиально может быть получено лишь тогда, когда речь идет о защите информации, которую как-то можно оценить, в основном экономической, промышленной, коммерческой и им подобной.

4. Необходимо оценить надежность элементов системы защиты. Но на текущий момент нет общепринятой методики оценки защищенности компьютерных систем, как и нет общетеоретического подхода к решению этой проблемы. Поэтому появляется вопрос о разработке методики, благодаря которой можно с достаточной точностью оценить надежность как отдельных элементов защиты, так и системы защиты в целом.

5. 13. Информационное страхование

Создание системы информационной безопасности компании на основе программных и технических средств экономически нецелесообразно. В этой связи актуальность приобретает использование механизма страхования.

Активное развитие рынка информационного страхования должно обеспечить распределение последствий от наступления информационных рисков среди максимально большого количества компаний. Учитывая то, что размер убытков от наступления информационных рисков может оказаться весьма существенным и в отдельных случаях даже стать причиной банкротства, которое в дальнейшем может привести к падению финансовых показателей целого ряда компаний, информационное страхование в данном случае может выступить в качестве инструмента, поддерживающего стабильность рынка.

Остановимся более подробно на вопросе о том, как применение информационного страхования может повысить эффективность работы АСОИ компании. Предположим, что компания при нормальной работе имеет доход I_1^e, при этом с вероятностью p можно сказать, что потери компании в случае нанесения вреда хранимой у нее информации составят

$$\mathbf{L^e = I_1^e - I_o^e}$$

где I_0^e – доход компании в случае нанесения ущерба ее информационной системе.

Убытки компании могут быть следующие:

- прямые убытки от информационных рисков;
- убытки, связанные с восстановлением информации;
- убытки, связанные с перерывами в производстве;
- убытки, связанные с потерей клиентов;
- убытки, связанные с ответственностью перед третьими лицами.

Защита, предоставляемая по полису страхования информационных рисков, может, по желанию клиента, распространяться одну из групп, а также на все группы.

Обозначим через s размер страхового возмещения, которое будет выплачено страховой компанией в случае наступления страхового случая, при этом стоимость страховой защиты составляет y долларов за 1 доллар покрытия. В случае наступления страхового случая (которое может произойти с вероятностью p) полезность страхования информационных рисков будет соответствовать доходу компании в случае отсутствия убытков, связанных с причинением ущерба хранимой информации, за вычетом расходов на покупку полиса, плюс размер возмещения, полученного по условиям страхования:

$$\mathbf{U\left(I_1^e - ys + s\right)}.$$

При безубыточном прохождении полиса (вероятность этого составляет 1-p) полезность будет определяться на основе дохода компании при отсутствии убытков минус расходы, связанные с оплатой страховой премии:

$$\mathbf{U\left(I_1^e - ys\right)}.$$

Таким образом, при покупке полиса страхования удается максимизировать ожидаемую полезность для обоих случаев – как при наступлении страхового случая, так и при безубыточном прохождении полиса:

$$\mathbf{s^* = \arg\max EU = pU\left(I_1^e - L^e - ys + s\right) + (1-p)U\left(I_1^e - ys\right)}$$

Компания может выбрать один из трех путей защиты от информационных рисков:

- развитие классических средств защиты информации;
- создание специальных резервов (самострахование);
- страхование.

Как самострахование, так и страхование выполняют функцию по минимизации последствий наступления ущерба, связанного с причинением вреда информации. Основная разница между ними состоит в том, что в случае страхования ущерб будет распределяться между целой группой страхователей, а в случае создания специальных резервов (самострахование) возмещение будет происходить целиком из собственных средств. Вложение же денег в классические средства защиты информации – попытка уменьшить не размер, а вероятность наступления убытков.

Страхование информационных рисков в нашей стране осуществляется рядом компаний. Следует отметить тот факт, что страхование информационных рисков пока еще во многом служит не для обеспечения защиты от информационных рисков, а для подчеркивания имиджа Страхователя.

Рассмотрим методику страхования информационных рисков Ингосстраха. К расчетным показателям относятся:

q – ожидаемое количество договоров страхования;

Sc – средняя страховая сумма по одному договору страхования;

Sв – средняя сумма страхового возмещения по одному договору страхования;

P – вероятность наступления страхового события по виду информационного риска (этих видов предусмотрено 6).

Страховой тариф (*Tc*) определяется как сумма:

$$\mathbf{Tc = NC + RN + Ng,}$$

где *NC* – основная часть нетто-ставки;

RN – рисковая надбавка;

Ng – нагрузка.

В основе расчета тарифных ставок лежит показатель убыточности (величина выплат на 100 руб. страховой суммы), а сам расчет тарифных ставок произведен на основании предполагаемых объемов страховых операций.

Таблица 5.3

Вид риска	Показатель			
	Sc	*Sв*	*P*	*q*
A	30000000	10000000	0,008	100
B	30000000	15000000	0,006	100
C	30000000	20000000	0,003	100
D	30000000	20000000	0,001	100
E	30000000	25000000	0,002	100
F	30000000	15000000	0,005	100

A – утрата, уничтожение или повреждение застрахованных информационных активов вследствие непреднамеренных ошибок в проектировании, разработке, создании, инсталляции, конфигурировании, обслуживании или эксплуатации информационных систем;

B – утрата, уничтожение или повреждение застрахованных информационных активов вследствие компьютерных атак, совершенных против страхователя;

C – утрата, уничтожение или повреждение застрахованных информационных активов в результате действий компьютерных вирусов;

D – неправомерное списание финансовых активов в электронной форме со счетов страхователя в результате ввода мошеннических электронных команд в информационную систему страхователя или в результате несанкционированной модификации компьютерного кода страхователя, или передачи фальсифицированного электронного поручения, якобы исходящего от имени страхователя, в банк или депозитарий страхователя, ставших следствием несанкционированного доступа к информационной системе страхователя со стороны третьих лиц, не имеющих на это соответствующих полномочий;

E – утрата, уничтожение или повреждение застрахованных информационных активов или финансовых активов в электронной форме в результате умышленных противоправных действий сотрудника страхователя, совершенных самостоятельно или в сговоре для извлечения незаконной личной финансовой выгоды или нанесения страхователю ущерба;

F – убытки от временного прекращения предпринимательской деятельности вследствие наступления событий.

Как известно, основная часть нетто-ставки (*NC*) соответствует средним выплатам страховщика, зависящим от вероятности наступления страхового случая, средней страховой суммы и среднего возмещения и рассчитывается по формуле

$$\mathbf{NC} = \frac{\mathbf{S_в} \times \mathbf{P} \times \mathbf{g}}{\mathbf{S_c}}.$$

Нетто-ставка (себестоимость страховой услуги) предназначена для создания страхового фонда, обеспечивающего эквивалентность взаимоотношений между страховщиком и страхователем, а также финансовую устойчивость страховой компании.

Принцип эквивалентности состоит в следующем: страхователь должен заплатить страховщику столько, сколько в среднем на него ожидается произвести выплат, но, принимая на себя риск страхователя, страховщик кроме средних ожидаемых потерь должен взимать некоторую плату «за риск» – некоторым образом компенсирующую возможность флуктуации выплат.

Другим расчетным показателем является рисковая надбавка. Она вводится для того, чтобы учесть вероятные отклонения количества страховых случаев относительно их среднего значения. Возможны два варианта расчета рисковой надбавки:

- для каждого риска (страхового события) отдельно;
- по нескольким видам рисков (по всему или части страхового портфеля).

Для расчета рисковой надбавки (*RN*), учитывающей вероятность превышения суммы выплат по перспективному портфелю над ее средними значениями, Ингосстрах использует первый способ. В условиях последующей активизации практики страхования информационных рисков, повышения его привлекательности для страхователей, особенно при страховании отдельных видов и проявлений рисков, очевидно, что рисковая надбавка может рассчитываться по всему страховому полю, что позволит уменьшить ее размер.

Методикой Ингосстраха предусмотрен расчет еще двух показателей:

- совокупной нетто-ставки (*SN*);
- брутто-ставки (*BC*).

Учитывая принятые обозначения, формула расчета совокупной нетто-ставки принимает такой вид:

$$\mathbf{SN = NC + RN.}$$

Формула для расчета брутто-ставки (*BC*), традиционно включающей совокупную нетто-ставку (*SN*) и нагрузку (*Ng*), определенную Ингосстрахом на уровне 30%, представляет собой отношение:

$$\mathbf{BC = \frac{SN}{(1 - Ng)}}.$$

Результаты расчета тарифных ставок свидетельствуют о том, что наиболее реальными (следовательно, с более высокими тарифными ставками) у страхователей считаются информационные риски, возникшие вследствие направленных против него компьютерных атак, умышленных противоправных действий сотрудников страхователя, а также убытков от временного прекращения предпринимательской деятельности.

Таблица 5.4

Вид риска	Расчетные величины			
	BC	*NC*	*RN*	*SN*
A	1,06	0,27	0,47	0,74
B	1,29	0,30	0,60	0,90
C	1,10	0,20	0,57	0,77
D	0,56	0,07	0,33	0,40
E	1,09	0,17	0,59	0,76
F	1,14	0,25	0,55	0,80

Осуществив расчет результирующей тарифной ставки по страхованию информационных систем, Ингосстрах определил тарифную ставку в размере 1,04 (руб.) со 100 руб. страховой суммы и зафиксировал диапазон существенного колебания ставки страховой премии по конкретному договору страхования за счет применения повышающих (от 1,0 до 5,0) и понижающих (от 0,2 до 1,0) коэффициентов.

Ввиду практически полного отсутствия опыта работы с информационными рисками, страховые компании зачастую устанавливают тарифы, которые в действительности не отражают реальную вероятность наступления страхового случая, связанного с нанесением ущерба информации. Страхование информационных рисков осуществляется в качестве дополнительного бонуса к основному полису страхования, покрывающего, например, риски причинения ущерба имуществу компании.

Между тем стоит заметить, что, учитывая темпы развития интереса страхования информационных рисков за рубежом, можно уверенно сказать, что и в нашей стране отношение к данному виду страхования будет меняться, и в достаточно скором времени комплексная система информационной безопасности компаний будет действительно комплексной и будет в дополнение ко всем остальным включать еще и экономические методы защиты информации, в частности механизм страхования.

Вопросы

1. Методы обеспечения информационной безопасности Российской Федерации.
2. Правовые методы обеспечения информационной безопасности Российской Федерации.
3. Организационно-технические методы обеспечения информационной безопасности Российской Федерации.
4. Экономические методы обеспечения информационной безопасности Российской Федерации.
5. Основные меры по обеспечению информационной безопасности Российской Федерации в сфере экономики.
6. Наиболее важные объекты обеспечения информационной безопасности Российской Федерации в области науки и техники.
7. Ограничение доступа как метод обеспечения информационной безопасности.
8. Биометрические методы аутентификации человека.
9. Статистика применения биометрических технологий.
10. Отпечатки пальцев как биометрическая характеристика идентификации человека.
11. Глаза как биометрическая характеристика идентификации человека.
12. Лицо как биометрическая характеристика идентификации человека.
13. Ладонь как биометрическая характеристика идентификации человека.
14. Динамические характеристики как биометрическая характеристика идентификации человека.
15. Классификация систем тревожной сигнализации.
16. Контроль доступа к аппаратуре как метод обеспечения информационной безопасности.

17. Разграничение и контроль доступа к информации как метод обеспечения информационной безопасности.
18. Предоставление привилегий на доступ как метод обеспечения информационной безопасности.
19. Идентификация и установление подлинности объекта (субъекта).
20. Объекты идентификации и установления подлинности в АСОИ.
21. Идентификация и установление подлинности личности.
22. Идентификация и установление подлинности технических средств.
23. Идентификация и установление подлинности документов.
24. Идентификация и установление подлинности информации на средствах ее отображения и печати.
25. Защита информации от утечки за счет побочного электромагнитного излучения и наводок.
26. Методы и средства защиты информации от побочного электромагнитного излучения и наводок информации.
27. Методы и средства защиты информации от случайных воздействий.
28. Методы защиты информации от аварийных ситуаций.
29. Организационные мероприятия по защите информации.
30. Организация информационной безопасности компании.
31. Выбор средств информационной информации.
32. Информационное страхование.

Тесты

1. Метод защиты информации ограничение доступа заключается:

1. в контроле доступа к внутреннему монтажу, линиям связи и технологическим органам управления;
2. в создании физической замкнутой преграды с организацией доступа лиц, связанных с объектом функциональными обязанностями;
3. в разделении информации на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями;
4. в том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы;
5. в проверке, является ли проверяемый объект (субъект) тем, за кого себя выдает.

2. Метод защиты информации контроль доступа к аппаратуре заключается:

1. в контроле доступа к внутреннему монтажу, линиям связи и технологическим органам управления;
2. в создании физической замкнутой преграды с организацией доступа лиц, связанных с объектом функциональными обязанностями;
3. в разделении информации на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями;
4. в том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы;
5. в проверке, является ли проверяемый объект (субъект) тем, за кого себя выдает.

3. Метод защиты информации разграничение и контроль доступа к информации заключается:

1. в контроле доступа к внутреннему монтажу, линиям связи и технологическим органам управления;
2. в создании физической замкнутой преграды с организацией доступа лиц, связанных с объектом функциональными обязанностями;
3. в разделении информации на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями;
4. в том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы;
5. в проверке, является ли проверяемый объект (субъект) тем, за кого себя выдает.

4. Метод защиты информации предоставление привилегий на доступ заключается:

1. в контроле доступа к внутреннему монтажу, линиям связи и технологическим органам управления;
2. в создании физической замкнутой преграды с организацией доступа лиц, связанных с объектом функциональными обязанностями;
3. в разделении информации на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями;

4. в том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы;
5. в проверке, является ли проверяемый объект (субъект) тем, за кого себя выдает.

5. Метод защиты информации идентификация и установление подлинности заключается:

1. в контроле доступа к внутреннему монтажу, линиям связи и технологическим органам управления;
2. в создании физической замкнутой преграды с организацией доступа лиц, связанных с объектом функциональными обязанностями;
3. в разделении информации на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями;
4. в том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы;
5. в проверке, является ли проверяемый объект (субъект) тем, за кого себя выдает.

Тема 6.

Криптографические методы информационной безопасности

Изучив тему 6, студент должен:
знать:

- виды шифров;
- в чем заключается шифрование и кодирование информации;
- порядок применения электронной подписи.

акцентировать внимание на понятиях:

- шифр, ключ, шифрование информации, кодирование информации, стеганография, электронная цифровая подпись.

Содержание темы (дидактические единицы и их характеристика):

Классификация криптографических методов. Характеристики существующих шифров. Кодирование. Стеганография. Электронная цифровая подпись.

Цели и задачи изучения темы: Получение знаний в области криптографических методов защиты информации.

Порядок изучения темы

Распределение бюджета времени по теме:

- количество часов отведенных на практические занятия, из них в компьютерной аудитории – 4/4;
- количество часов, отведенных на самостоятельную работу, – 16.

Виды самостоятельной работы студентов:

- изучение учебного пособия «Информационная безопасность»;
- подготовка к участию в форуме по теме «Криптографические методы информационной безопасности»;
- изучение дополнительной литературы;
- выполнение тестовых заданий по теме.

Методические указания по изучению вопросов темы

При изучении учебных вопросов:

- изучить тему 6 по учебному пособию «Информационная безопасность»;
- принять участие в форуме по теме «Криптографические методы информационной безопасности»;
- изучить дополнительные материалы.

При изучении темы необходимо:

- *читать литературу*:

1. Информационная безопасность: Уч. Пособие. – М.: МЭСИ, 2007.
2. Герасименко В.А., Малюк А.А. Основы защиты информации, – М.: ППО «Известия», 1997. Гл. 1,2.
3. Мельников В.И. Защита информации в компьютерных системах. – М.: Финансы и статистика, 1997. – Разд. 1.
4. Милославская Н.Г., Толстой А.И. Интрасети: доступ в Internet, защита. – М.: ООО «ЮНИТИ-ДАНА», 2000., Гл. 1.
5. Проскурин В.Г., Крутов С.В. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах. – М.: Радио и связь, 2000.
6. Белкин П.Ю. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных. – М.: Радио и связь, 1999.

- *посетить сайты:* www.compulenta.ru, www.isecurity.ru, www.oxpaha.ru, www.cyberterrorism report.ru.

Вопросы темы

6.1. Классификация методов криптографического закрытия информации.

6.2. Шифрование.

6.3. Кодирование.

6.4. Стеганография.

6.5. Электронная цифровая подпись.

6.1. Классификация методов криптографического закрытия информации

Криптографические методы являются наиболее эффективными средствами защиты информации в автоматизированных системах обработки информации (АСОИ). А при передаче информации по линиям связи они являются единственным реальным средством предотвращения несанкционированного доступа.

Вопросами криптографического закрытия информации занимается наука ***криптология*** (криптос – тайный, логос – наука). Криптология имеет два основных направления – ***криптографию*** и ***криптоанализ.*** Цели этих направлений противоположны. Криптография занимается построением и исследованием математических методов преобразования информации, а криптоанализ – исследованием возможности расшифровки информации без ключа. Термин «криптография» происходит от двух греческих слов: криптос – тайный, графейн – писать. Таким образом, это тайнопись, система шифрования сообщения с целью сделать его непонятным для непосвященных лиц.

Имеются две большие группы шифров: шифры перестановки и шифры замены.

Шифр перестановки изменяет только порядок следования символов исходного сообщения. Это такие шифры, преобразования которых приводят к изменению только следования символов открытого (исходного) сообщения.

Шифр замены меняет каждый символ на другой, не изменяя порядок их следования. Это такие шифры, преобразования которых приводят к замене каждого символа открытого сообщения на другие символы, причем порядок следования символов закрытого сообщения совпадает с порядком следования соответствующих символов открытого сообщения.

Стойкость метода – это тот минимальный объем зашифрованного текста, статистическим анализом которого можно вскрыть исходный текст. Таким образом, стойкость шифра определяет допустимый объем информации, зашифровываемый при использовании одного ключа.

Трудоемкость метода определяется числом элементарных операций, необходимых для шифрования одного символа исходного текста.

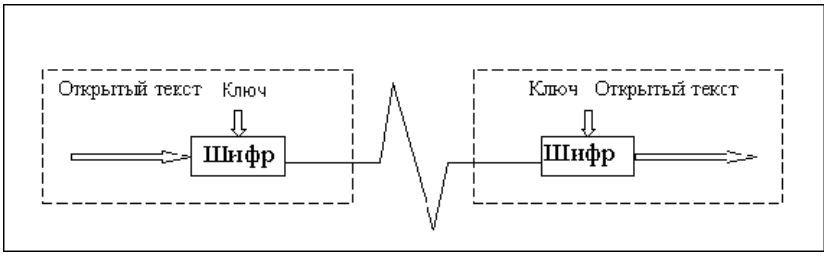


Рис. 6.1. **Шифрование информации**

***Основные требования к криптографическому закрытию информации*:**

1. Сложность и стойкость криптографического закрытия данных должны выбираться в зависимости от объема и степени секретности данных.
2. Надежность закрытия должна быть такой, чтобы секретность не нарушалась даже в том случае, когда злоумышленнику становится известен метод шифрования.
3. Метод закрытия, набор используемых ключей и механизм их распределения не должны быть слишком сложными.
4. Выполнение процедур прямого и обратного преобразований должно быть формальным. Эти процедуры не должны зависеть от длины сообщений.
5. Ошибки, возникающие в процессе преобразования, не должны распространяться по системе.
6. Вносимая процедурами защиты избыточность должна быть минимальной.

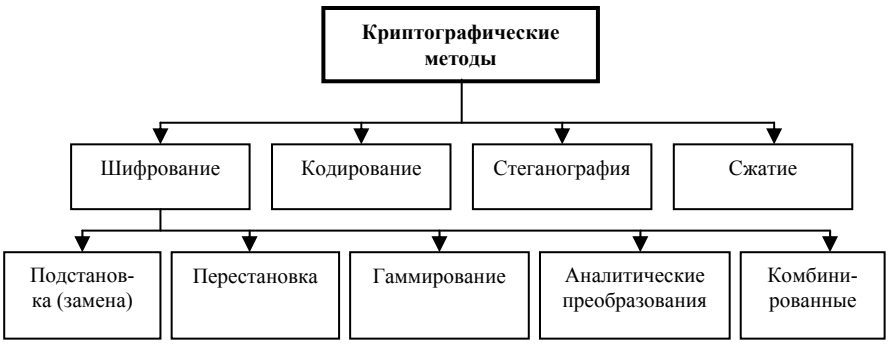


Рис. 6.2. **Классификация методов криптографического закрытия информации**

6.2. Шифрование

В криптографической терминологии исходное послание именуется открытым текстом (plaintext или cleartext). Изменение исходного текста так, чтобы скрыть от прочих его содержание, называют ***шифрованием*** (encryption). Зашифрованное сообщение называют ***шифротекстом*** (ciphertext). Процесс, при котором из шифротекста извлекается открытый текст, называют ***дешифровкой*** (clecryption). В процессе шифровки и дешифровки используется ***ключ*** (key). Алгоритм шифрования обеспечивает невозможность дешифрования зашифрованного текста без знания ключа.

Открытый текст обычно имеет произвольную длину. Если текст большой и не может быть обработан шифратором (компьютером) целиком, то он разбивается на блоки фиксированной длины, а каждый блок шифруется отдельно, независимо от его положения во входной последовательности. Такие криптосистемы называются системами блочного шифрования.

Криптосистемы разделяются на:

- симметричные;
- асимметричные (с открытым ключом).

В симметричных криптосистемах, как для шифрования, так и для дешифрования, используется один и тот же ключ.

В системах с открытым ключом используются два ключа – открытый и закрытый, которые математически (алгоритмически) связаны друг с другом. Информация шифруется с помощью открытого ключа, который доступен всем желающим, а расшифровывается лишь с помощью закрытого ключа, который известен только получателю сообщения.

Криптография кроме криптосистем (симметричных, с открытым ключом) изучает еще и системы управления ключами.

Системы управления ключами – это информационные системы, целью которых является составление и распределение ключей между пользователями информационной системы.

Разработка ключевой, парольной информации является типовой задачей администратора безопасности системы. Ключ может быть сгенерирован как массив нужного размера статистически независимых и равновероятно распределенных на двоичном множестве {О, 1} элементов.

Пароли также необходимо менять. Пароли должен генерировать и раздавать пользователям системный администратор по безопасности, исходя из основного принципа: обеспечения равной вероятности появления каждого из символов алфавита в пароле.

Все современные криптосистемы построены по ***принципу Кирхгоффа*:** секретность зашифрованных сообщений определяется секретностью ключа.

Это означает, что даже если алгоритм шифрования будет известен криптоаналитику, то он не сможет расшифровать закрытое сообщение, если не располагает соответствующим ключом.

Все классические шифры соответствуют этому принципу и спроектированы таким образом, чтобы не было пути вскрыть их более эффективным способом, чем полный перебор по всему ключевому пространству, то есть перебор всех возможных значений ключа. Ясно, что стойкость таких шифров определяется размером используемого в них ключа.

В российских шифрах используется 256-битовый ключ, а объем ключевого пространства составляет 2^{256}. Ни на одном реально существующем или возможном в недалеком будущем компьютере нельзя подобрать ключ (полным перебором) за время, меньшее многих сотен лет.

Симметричные криптосистемы

Симметричные криптосистемы подразделяются на следующие преобразования: подстановка, перестановка, гаммирование и блочные шифры (рис. 6.3).

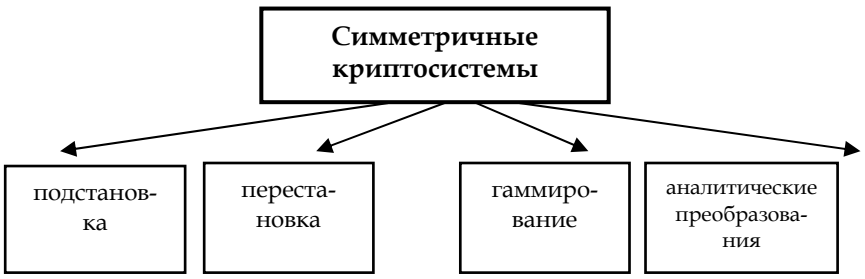


Рис. 6.3. **Классификация симметричных криптосистем**

Шифрование методом замены (подстановки)

Наиболее простой метод шифрования. Символы шифруемого текста заменяются другими символами, взятыми из одного алфавита (одноалфавитная замена) или нескольких алфавитов (многоалфавитная подстановка).

Одноалфавитная подстановка

Простейшая подстановка – прямая замена символов шифруемого сообщения другими буквами того же самого или другого алфавита.

Стойкость метода простой замены низкая. Зашифрованный текст имеет те же самые статистические характеристики, что и исходный, поэтому, зная стандартные частоты появления символов в том языке, на котором написано сообщение, и подбирая по частотам появления символы в зашифрованном сообщении, можно восстановить таблицу замены. Для этого требуется лишь достаточно длинный зашифрованный текст, для того, чтобы получить достоверные оценки частот появления символов. Поэтому простую замену используют лишь в том случае, когда шифруемое сообщение достаточно коротко.

Стойкость метода равна 20–30, трудоемкость определяется поиском символа в таблице замены. Для снижения трудоемкости при шифровании таблица замены сортируется по шифруемым символам, а для расшифровки формируется таблица дешифрования, которая получается из таблицы замены сортировкой по заменяющим символам.

Многоалфавитная одноконтурная обыкновенная подстановка

Для замены символов используются несколько алфавитов, причем смена алфавитов проводится последовательно и циклически: первый символ заменяется на соответствующий символ первого алфавита, второй – второго алфавита и т.д. пока не будут исчерпаны все алфавиты. После этого использование алфавитов повторяется.

Рассмотрим шифрование с помощью таблицы Вижинера – квадратной матрицы с n^2 элементами, где n – число символов используемого алфавита. В первой строке матрицы содержится исходный алфавит, каждая следующая строка получается из предыдущей циклическим сдвигом влево на один символ.

Таблица Вижинера для русского алфавита:

А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ь Ы Ъ Э Ю Я
Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ь Ы Ъ Э Ю Я А
В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ь Ы Ъ Э Ю Я А Б
Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ь Ы Ъ Э Ю Я А Б В
Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ь Ы Ъ Э Ю Я А Б В Г
Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ь Ы Ъ Э Ю Я А Б В Г Д
Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ь Ы Ъ Э Ю Я А Б В Г Д Е
З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ь Ы Ъ Э Ю Я А Б В Г Д Е Ж
И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ь Ы Ъ Э Ю Я А Б В Г Д Е Ж З
Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ь Ы Ъ Э Ю Я А Б В Г Д Е Ж З И
К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ь Ы Ъ Э Ю Я А Б В Г Д Е Ж З И Й
Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ь Ы Ъ Э Ю Я А Б В Г Д Е Ж З И Й К
М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ь Ы Ъ Э Ю Я А Б В Г Д Е Ж З И Й К Л
Н О П Р С Т У Ф Х Ц Ч Ш Щ Ь Ы Ъ Э Ю Я А Б В Г Д Е Ж З И Й К Л М
О П Р С Т У Ф Х Ц Ч Ш Щ Ь Ы Ъ Э Ю Я А Б В Г Д Е Ж З И Й К Л М Н
П Р С Т У Ф Х Ц Ч Ш Щ Ь Ы Ъ Э Ю Я А Б В Г Д Е Ж З И Й К Л М Н О
Р С Т У Ф Х Ц Ч Ш Щ Ь Ы Ъ Э Ю Я А Б В Г Д Е Ж З И Й К Л М Н О П
С Т У Ф Х Ц Ч Ш Щ Ь Ы Ъ Э Ю Я А Б В Г Д Е Ж З И Й К Л М Н О П Р
Т У Ф Х Ц Ч Ш Щ Ь Ы Ъ Э Ю Я А Б В Г Д Е Ж З И Й К Л М Н О П Р С
У Ф Х Ц Ч Ш Щ Ь Ы Ъ Э Ю Я А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т
Ф Х Ц Ч Ш Щ Ь Ы Ъ Э Ю Я А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У
Х Ц Ч Ш Щ Ь Ы Ъ Э Ю Я А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф
Ц Ч Ш Щ Ь Ы Ъ Э Ю Я А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х
Ч Ш Щ Ь Ы Ъ Э Ю Я А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц
Ш Щ Ь Ы Ъ Э Ю Я А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч
Щ Ь Ы Ъ Э Ю Я А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш
Ь Ы Ъ Э Ю Я А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ
Ы Ъ Э Ю Я А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ь
Ъ Э Ю Я А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ь Ы
Э Ю Я А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ь Ы Ъ
Ю Я А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ь Ы Ъ Э
Я А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ь Ы Ъ Э Ю

Для шифрования необходимо задать ключ – слово с неповторяющимися символами. Таблицу замены получают следующим образом: строку «Символы шифруемого текста» формируют из первой строки матрицы Вижинера, а строки из раздела «Заменяющие символы» образуются из строк матрицы Вижинера, первые символы которых совпадают с символами ключевого слова.

При шифровании и дешифровании нет необходимости держать в памяти всю матрицу Вижинера, поскольку используя свойства циклического сдвига, можно легко вычислить любую строку матрицы по ее номеру и первой строке.

Стойкость метода равна стойкости метода подстановки, умноженной на количество используемых при шифровании алфавитов, т.е. на длину ключевого слова: $20 \times L$, где L – длина ключевого слова.

С целью повышения стойкости шифрования предлагаются следующие усовершенствования таблицы Вижинера:

1. Во всех (кроме первой) строках таблицы буквы располагаются в произвольном порядке.
2. В качестве ключа используются случайные последовательности чисел, которые задают номера используемых строк матрицы Вижинера для шифрования.

Многоалфавитная одноконтурная монофоническая подстановка

В монофонической подстановке количество и состав алфавитов выбираются таким образом, чтобы частоты появления всех символов в зашифрованном тексте были одинаковыми. При таком положении затрудняется криптоанализ зашифрованного текста с помощью его статистической обработки. Выравнивание частот появления символов достигается за счет того, что для часто встречающихся символов исходного текста предусматривается большее число заменяющих символов, чем для редко встречающихся.

Пример таблицы монофонической замены:

А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ь Ы Ъ Э Ю Я _
Ф Н (Щ И Г E R A Д Ы ~ @ S Л Я Ж ^ С Ш М Б Q П Т Х Ю Ъ Р } \ _ #
* Н У Щ D + E R = Д Ц Й Ч [В Ь) О & { М Б Q П Т Х Ю Ъ Р } \ _ <
Л Н (Щ И] E R % Д Ы ~ @ G / Я Э З « Ш М Б Q П Т Х Ю Ъ Р } \ _ W
Ф Н У Щ D K E R A Д Ц Й Ч S + Ь Ж ^ С { М Б Q П Т Х Ю Ъ Р } \ _ V

Шифрование проводится так же, как и при простой подстановке, с той лишь разницей, что после шифрования каждого символа соответствующий ему столбец алфавитов циклически сдвигается вверх на одну позицию. Таким образом, столбцы алфавитов как бы образуют независимые друг от друга кольца, поворачиваемые вверх на один знак каждый раз после шифрования соответствующего знака исходного текста.

Многоалфавитная многоконтурная подстановка

Многоконтурная подстановка заключается в том, что для шифрования используются несколько наборов (контуров) алфавитов, используемых циклически, причем каждый контур в общем случае имеет свой индивидуальный период применения. Частным случаем многоконтурной полиалфавитной подстановки является замена по таблице Вижинера, если для шифрования используется несколько ключей, каждый из которых имеет свой период применения.

Стойкость простой многоалфавитной подстановки оценивается величиной $20 \times n$, где n – число различных алфавитов, используемых для замены. Усложнение многоалфавитной подстановки существенно повышает ее стойкость. Монофоническая подстановка может быть весьма стойкой (и даже теоретически нераскрываемой), однако строго монофоническую подстановку реализовать на практике трудно, а любые отклонения от монофоничности снижают реальную стойкость шифра.

Шифрование методом перестановки

При шифровании перестановкой символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока этого текста.

Простая перестановка

Выбирается размер блока шифрования в n столбцов и m строк и ключевая последовательность, которая формируется из натурального ряда чисел 1,2,...,n случайной перестановкой.

Шифрование проводится в следующем порядке:

1. Шифруемый текст записывается последовательными строками под числами ключевой последовательности, образуя блок шифрования размером $n \times m$.
2. Зашифрованный текст выписывается колонками в порядке возрастания номеров колонок, задаваемых ключевой последовательностью.
3. Заполняется новый блок и т.д.

Например, зашифруем текст
ГРУЗИТЕ_АПЕЛЬСИНЫ_БОЧКАХ
блоком размером 8×3 и ключом 5-8-1-3-7-4-6-2.

Таблица простой перестановки будет иметь вид:

Ключ						
5	8	1	3	7	4	6
Г Р	У	З	И	Т	Е	_
А	П	Е	Л	Ь	С	И
Ы _	Б	О	Ч	К	А	Х

Зашифрованное сообщение:

УЕБ_НХЗЛОЕСЛГАЫЕИАИЬЧРП_

Расшифрование выполняется в следующем порядке:

1. Из зашифрованного текста выделяется блок символов размером n × m.
2. Этот блок разбивается на n групп по m символов.
3. Символы записываются в те столбцы таблицы перестановки, номера которых совпадают с номерами групп в блоке. Расшифрованный текст читается по строкам таблицы перестановки.
4. Выделяется новый блок символов и т.д.

Перестановка, усложненная по таблице

При усложнении перестановки по таблицам для повышения стойкости шифра в таблицу перестановки вводятся неиспользуемые клетки таблицы. Количество и расположение неиспользуемых элементов является дополнительным ключом шифрования.

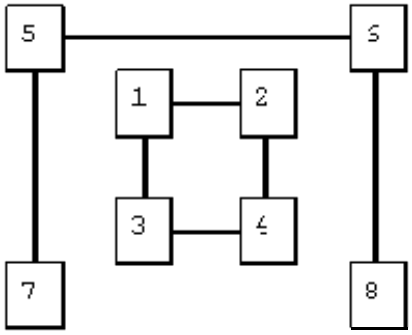
При шифровании текста в неиспользуемые элементы не заносятся символы текста и в зашифрованный текст из них не записываются никакие символы – они просто пропускаются. При расшифровке символы зашифрованного текста также не заносятся в неиспользуемые элементы.

Для дальнейшего увеличения криптостойкости шифра можно в процессе шифрования менять ключи, размеры таблицы перестановки, количество и расположение неиспользуемых элементов по некоторому алгоритму, причем этот алгоритм становится дополнительным ключом шифра.

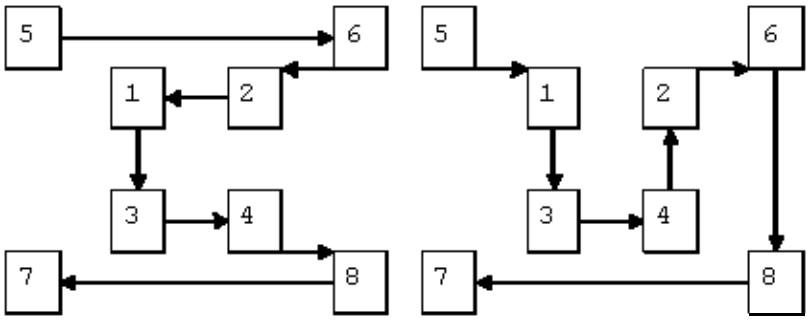
Перестановка, усложненная по маршрутам

Высокую стойкость шифрования можно обеспечить усложнением перестановок по маршрутам типа гамильтоновских. При этом для записи символов шифруемого текста используются вершины некоторого гиперкуба, а знаки зашифрованного текста считываются по маршрутам Гамильтона, причем используются несколько различных маршрутов. Для примера рассмотрим шифрование по маршрутам Гамильтона при n=3.

Структура трехмерного гиперкуба:



Номера вершин куба определяют последовательность его заполнения символами шифруемого текста при формировании блока. В общем случае n-мерный гиперкуб имеет n^2 вершин. Маршруты Гамильтона имеют вид:



Последовательность перестановок символов в шифруемом блоке для первой схемы 5-6-2-1-3-4-8-7, а для второй 5-1-3-4-2-6-8-7. Аналогично можно получить последовательность перестановок для других маршрутов: 5-7-3-1-2-6-8-4, 5-6-8-7-3-1-2-4, 5-1-2-4-3-7-8-6 и т.д.

Размерность гиперкуба, количество, вид выбираемых маршрутов Гамильтона составляют секретный ключ метода.

Стойкость простой перестановки однозначно определяется размерами используемой матрицы перестановки. Например, при использовании матрицы 16×16 число возможных перестановок достигает 1.4E26. Такое число вариантов невозможно перебрать даже с использованием ЭВМ. Стойкость усложненных перестановок еще выше. Однако следует иметь в виду, что при шифровании перестановкой полностью сохраняются вероятностные характеристики исходного текста, что облегчает криптоанализ.

Шифрование методом гаммирования

Суть метода состоит в том, что символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, называемой гаммой. Иногда такой метод представляют как наложение гаммы на исходный текст, поэтому он получил название «гаммирование».

Последовательность гаммы удобно формировать с помощью датчика псевдослучайных чисел (ПСЧ).

Стойкость гаммирования однозначно определяется длиной периода гаммы. При использовании современных ПСЧ реальным становится использование бесконечной гаммы, что приводит к бесконечной теоретической стойкости зашифрованного текста.

Шифрование с помощью аналитических преобразований

Достаточно надежное закрытие информации может обеспечить использование при шифровании некоторых аналитических преобразований. Например, можно использовать методы алгебры матриц – в частности умножение матрицы на вектор.

В качестве ключа задается квадратная матрица ||a|| размера n×n. Исходный текст разбивается на блоки длиной n символов. Каждый блок рассматривается как n-мерный вектор. А процесс шифрования блока заключается в получении нового n-мерного вектора (зашифрованного блока) как результата умножения матрицы ||a|| на исходный вектор.

Расшифрование текста происходит с помощью такого же преобразования, только с помощью матрицы, обратной ||a||. Очевидно, что ключевая матрица ||a|| должна быть невырожденной.

Комбинированные методы шифрования

Достаточно эффективным средством повышения стойкости шифрования является комбинированное использование нескольких различных способов шифрования, т.е. последовательное шифрование исходного текста с помощью двух или более методов.

Стойкость комбинированного шифрования не ниже произведения стойкостей используемых способов.

Криптосистемы с открытым ключом (асимметричные)

Слабым местом криптографических систем, при их практической реализации, является проблема распределения ключей. Для того чтобы был возможен обмен конфиденциальной информацией между двумя субъектами информационной системы, ключ должен быть сгенерирован одним из них, а затем, в конфиденциальном порядке, передан другому. В общем случае для передачи ключа опять же требуется использование криптосистемы.

Для решения этой проблемы на основе результатов, полученных классической и современной математикой, были предложены системы с открытым ключом.

Суть их состоит в том, что каждым адресатом информационной системы генерируются два ключа, связанные между собой по определенному правилу. Один ключ объявляется открытым, а другой закрытым. Открытый ключ публикуется и доступен любому, кто желает послать сообщение адресату. Секретный ключ сохраняется в тайне.

Исходный текст шифруется открытым ключом и передается адресату. Зашифрованный текст не может быть расшифрован тем же открытым ключом. Дешифрование сообщение возможно только с использованием закрытого ключа, который известен только адресату (рис. 6.4).

Асимметричные криптографические системы используют так называемые необратимые или односторонние функции, которые обладают следующим свойством: при заданном значении x относительно просто вычислить значение $f(x)$, однако если $y=f(x)$, то нет простого пути для вычисления значения x.

Алгоритмы шифрования с открытым ключом получили широкое распространение в современных информационных системах.

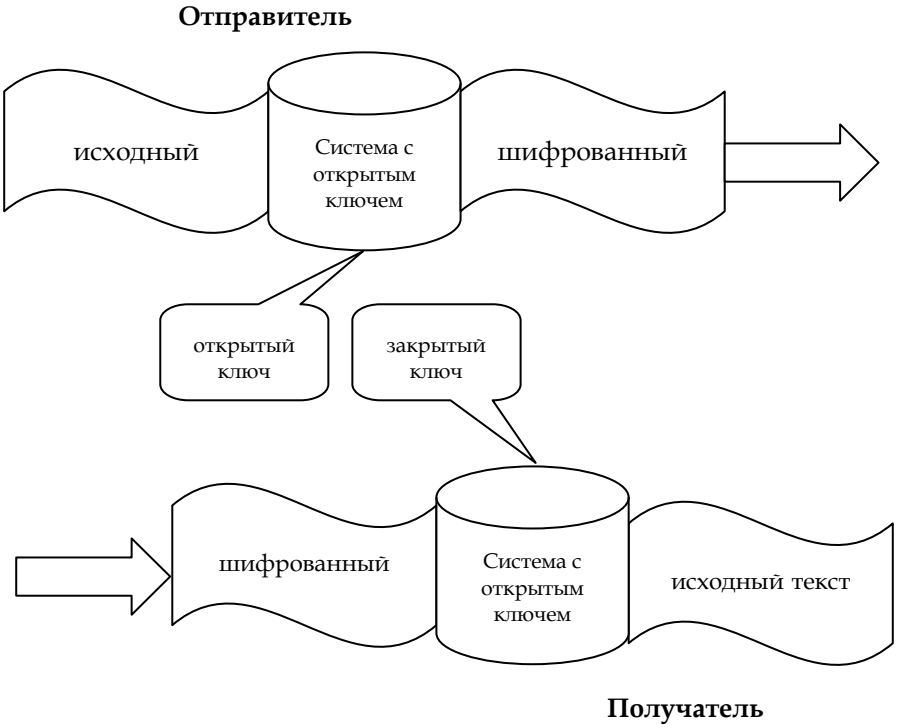


Рис. 6.4. **Криптосистема с открытым ключом**

Алгоритмы криптосистем с открытым ключом можно использовать как:

- самостоятельные средства защиты передаваемых и хранимых данных.
- средства для распределения ключей.
- средства аутентификации пользователей.

Алгоритмы криптосистем с открытым ключом более трудоемки, чем традиционные криптосистемы, поэтому использование их в качестве самостоятельных средств защиты нерационально. Поэтому на практике рационально с помощью криптосистем с открытым ключом распределять ключи, объем которых как информации незначи-

телен. А потом с помощью обычных алгоритмов осуществлять обмен большими информационными потоками.

Несмотря на довольно большое число различных криптосистем с открытым ключом, наиболее популярна – криптосистема RSA, разработанная в 1977 г. и получившая название в честь ее создателей: Ривеста, Шамира и Эйдельмана.

Ривест, Шамир и Эйдельман воспользовались тем фактом, что нахождение больших простых чисел в вычислительном отношении осуществляется легко, но разложение на множители произведения двух таких чисел практически невыполнимо. Доказано (теорема Рабина), что раскрытие шифра RSA эквивалентно такому разложению. Поэтому для любой длины ключа можно дать нижнюю оценку числа операций для раскрытия шифра, а с учетом производительности современных компьютеров оценить и необходимое на это время.

Пусть $n=p\times q$, где p и q – различные простые числа, а e и d удовлетворяют уравнению

$$e\times d(mod\ (p-1)\times(q-1))=1.$$

Если p и q – достаточно большие простые числа, то разложение n практически не осуществимо. Это и заложено в основу системы шифрования RSA.

$\{e,n\}$ – образует открытый ключ, а $\{d,n\}$ – закрытый (или наоборот).

Открытый ключ публикуется и доступен каждому, кто желает послать владельцу ключа сообщение, которое зашифровывается указанным алгоритмом. После шифрования, сообщение невозможно раскрыть с помощью открытого ключа. Владелец же закрытого ключа без труда может расшифровать принятое сообщение.

Шифрование осуществляется по формуле: $S_{шифр}=S^e\ mod\ N$.

Дешифрование осуществляется по формуле: $S = S^d_{шифр}\ mod\ N.$

Где S – исходный текст, $S_{шифр}$ – преобразованный текст, при этом $S < N$.

6.2.3. Характеристики существующих шифров

DES

DES (Data Encryption Standart) – это симметричный алгоритм шифрования, т.е. один ключ используется как для зашифровывания, так и для расшифровывания сообщений. Разработан фирмой IBM и

утвержден правительством США в 1977 г. как официальный стандарт.

DES имеет блоки по 64 бит и основан на 16-кратной перестановке данных, также для зашифровывания использует ключ в 56 бит. Существует несколько режимов DES, например Electronic Code Book (ECB) и Cipher Block Chaining (CBC).

IDEA

IDEA (International Data Algorithm) – это вторая версия блочного шифра, разработанного К. Лейем (Lai) и Д. Месси (Massey) в конце 80-х гг. Это шифр, состоящий из 64-битных повторяющихся блоков с 128-битным ключом и восемью проходами (rounds). Дешифрование выполняется по тому же принципу, что и шифрование. Структура шифра была разработана для легкого воплощения как программно, так и аппаратно, и безопасность IDEA основывается на использовании трех не совместимых типов арифметических операций над 16-битными словами. Скорость программного IDEA сравнима со скоростью DES.

Один из принципов создания IDEA – затруднить дифференциальный криптоанализ. Ни одна линейная криптоаналитическая атака не закончилась успешно, и не было выявлено алгебраически слабых мест.

RC2 и RC4

RC2 и RC4 – это блочные шифры с ключом переменной длины, созданные Роном Ривестом (Ron Rivest) для RSA Data Security. «RC» расшифровывается как «Ron's Code» или «Rivest Cipher (шрифт)». RC2 быстрее чем DES и был специально разработан для замены DES. Он может быть реализован более или менее защищенным, чем DES, в зависимости от длины ключа. RC2 алгоритм конфиденциален и является собственностью RSA Data Security. RC2 может использоваться там, где используется DES.

RC2 и RC4 с ключами 128 бит обеспечивают такой же уровень безопасности, как и IDEA или тройной DES. RC2 и RC4 используется широко разработчиками, чьи продукты экспортируются за пределы США, поскольку экспортировать DES запрещено.

RSA

RSA (авторы: Rivest, Shamir и Alderman) это система с открытым ключом (public-key), предназначенная как для шифрования, так и для аутентификации, была разработана в 1977 г. Она основана на трудности разложения очень больших целых чисел на простые сомножители.

RSA – очень медленный алгоритм. Для сравнения, на программном уровне DES по меньше мере в 100 раз быстрее RSA, а на аппаратном в 1000 – 10000 раз, в зависимости от выполнения.

ГОСТ 28147-89

ГОСТ 28147-89 – это стандарт, принятый в 1989 г. в Советском Союзе и установивший алгоритм шифрования данных, составляющих гостайну. По свидетельству причастных к его реализациям и использованию людей, алгоритм был разработан в 70-е гг. в 8-м Главном Управлении КГБ СССР, тогда он имел гриф СС (совершенно секретно). Затем гриф был понижен до С (секретно), а когда в 89-м г. алгоритм был проведен через Госстандарт и стал официальным государственным стандартом, гриф с него был снят, однако алгоритм оставался ДСП (для служебного пользования). В начале 90-х г. он стал полностью открытым.

ГОСТ предусматривает 3 режима шифрования (простая замена, гаммирование, гаммирование с обратной связью) и один режим выработки имитовставки. Первый из режимов шифрования предназначен для шифрования ключевой информации и не может использоваться для шифрования других данных, для этого предусмотрены два других режима шифрования. Режим выработки имитовставки (криптографической контрольной комбинации) предназначен для имитозащиты шифруемых данных, то есть для их защиты от случайных или преднамеренных несанкционированных изменений.

Алгоритм построен по тому же принципу, что и DES – это классический блочный шифр с секретным ключом – однако отличается от DES большей длиной ключа, большим количеством раундов и более простой схемой построения самих раундов.

В силу намного большей длины ключа ГОСТ гораздо устойчивей DESa к вскрытию путем полного перебора по множеству возможных значений ключа.

ГОСТ не запантентован, поэтому его может свободно использовать любое юридическое и физическое лицо, если это не противоречит законодательству страны где находится это лицо. Со стороны авторов ГОСТа претензий нет и быть не может, так как юридические права на алгоритм ни за кем не закреплены.

6.3. Кодирование

Процесс кодирования информации осуществляется заменой слов и предложений исходной информации кодами. В качестве кодов могут использоваться сочетания букв, цифр, букв и цифр. При кодировании и обратном преобразовании используются специальные таблицы или словари. Кодирование информации целесообразно применять при небольшом объеме кодируемой информации. Такой вид криптографического преобразования применим, например, в командных линиях АСУ. Недостатками кодирования конфиденциальной информации является необходимость хранения и распространения кодировочных таблиц, которые необходимо часто менять, чтобы избежать раскрытия кодов статистическими методами обработки перехваченных сообщений.

6.4. Стеганография

В отличие от других методов криптографического преобразования информации методы стеганографии позволяют скрыть не только смысл хранящейся или передаваемой информации, но и сам факт хранения или передачи закрытой информации. В компьютерных системах практическое использование стеганографии является перспективным направлением. В основе всех методов стеганографии лежит маскирование закрытой информации среди открытых файлов. Обработка мультимедийных файлов в компьютерных системах открывает практически неограниченные возможности перед стеганографией.

Существует несколько методов скрытой передачи информации. Одним из них является метод скрытия с использованием текстовых файлов. За текстовым открытым файлом записывается скрытый двоичный файл, объем которого много меньше текстового файла. В конце текстового файла помещается метка. При обращении к этому текстовому файлу стандартными средствами операционной системы считывание прекращается по достижении метки, и скрытый файл остается недоступен. Для двоичных файлов никаких меток в конце файла не предусмотрено. Конец такого файла определяется при обработке атрибутов, в которых хранится длина файла в байтах. Доступ к скрытому файлу может быть получен, если файл открыть как двоичный. Скрытый файл может быть зашифрован. Если

кто-то случайно обнаружит скрытый файл, то зашифрованная информация будет воспринята как сбой в работе системы.

Графическая и звуковая информация представляются в числовом виде. Так, в графических объектах наименьший элемент изображения может кодироваться одним байтом. В младшие разряды определенных байтов изображения в соответствии с алгоритмом криптографического преобразования помещаются биты скрытого файла. Если правильно подобрать алгоритм преобразования и изображение, на фоне которого помещается скрытый файл, то человеческому глазу практически невозможно отличить полученное изображение от исходного. Очень сложно выявить скрытую информацию и с помощью специальных программ.

Наилучшим образом для внедрения скрытой информации подходят изображения местности: фотоснимки со спутников, самолетов и т. п. С помощью средств стеганографии могут маскироваться текст, изображение, речь, цифровая подпись, зашифрованное сообщение. Комплексное использование стеганографии и шифрования многократно повышает сложность решения задачи обнаружения и раскрытия конфиденциальной информации.

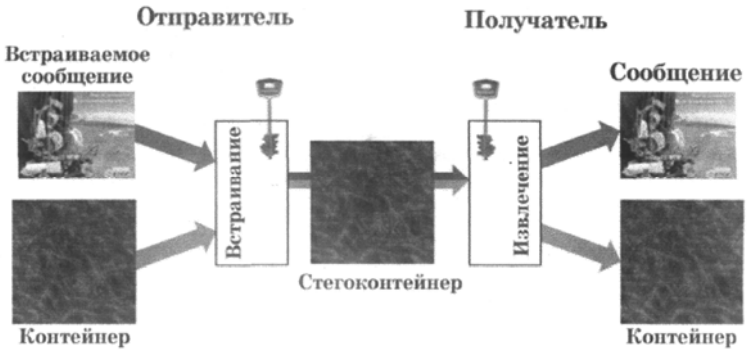


Рис. 6.5. **Технология стеганографии**

Сжатие

Сжатие информации может быть отнесено к методам криптографического преобразования информации с определенными оговорками. Целью сжатия является сокращение объема информации. В то же время сжатая информация не может быть прочитана или использована без обратного преобразования. Учитывая доступность средств сжа-

тия и обратного преобразования, эти методы нельзя рассматривать как надежные средства криптографического преобразования информации. Даже если держать в секрете алгоритмы, то они могут быть сравнительно легко раскрыты статистическими методами обработки. Поэтому сжатые файлы конфиденциальной информации подвергаются последующему шифрованию. Для сокращения времени целесообразно совмещать процесс сжатия и шифрования информации.

Организационные проблемы криптозащиты

Рассмотренные значения стойкости шифров являются потенциальными величинами. Они могут быть реализованы при строгом соблюдении правил использования криптографических средств защиты.

Основные правила криптозащиты:

1. Сохранение в тайне ключей.
2. Исключение дублирования.
3. Достаточно частая смена ключей.

Под дублированием здесь понимается повторное шифрование одного и того же отрывка текста с использованием тех же ключей (например, если при первом шифровании произошел сбой). Нарушение этого правила резко снижает надежность шифрования, так как исходный текст может быть восстановлен с помощью статистического анализа двух вариантов зашифрованного текста.

Важнейшим правилом криптозащиты является достаточно частая смена ключей. Причем частота может определяться исходя из длительности использования ключа или исходя из объема зашифрованного текста. При этом смена ключей по временному графику является защитной мерой против возможного их хищения, смена после шифрования определенного объема текста - от раскрытия шифра статистическими методами.

Нельзя допускать, чтоб злоумышленник имел возможность направить в систему ряд специально подобранных сообщений и получить их в зашифрованном виде. Такого взлома не может выдержать ни одна криптосистема!

Важными аспектами организации криптозащиты являются выбор способа закрытия, распределение ключей и доставка их в места пользования (механизм распределения ключей).

Выбор способа защиты тесно связан с трудоемкостью метода шифрования, степенью секретности закрываемых данных, стойкостью метода и объемом шифруемой информации.

Одним из принципов криптографии является предположение о несекретности метода закрытия информации. Предполагается, что необходимая надежность закрытия обеспечивается только за счет сохранения в тайне ключей. Отсюда вытекает принципиальная важность формирования ключей, распределения их и доставка в пункты назначения. Основные правила механизма распределения ключей:

1. Ключи должны выбираться случайно.
2. Выбранные ключи должны распределяться таким образом, чтобы не было закономерностей в изменении ключей от пользователя к пользователю.
3. Должна быть обеспечена тайна ключей на всех этапах функционирования системы. Ключи должны передаваться по линиям связи, почте или курьерами в зашифрованном виде с помощью другого ключа. На практике часто образуется иерархия ключей шифрования, в которой ключи нижнего уровня при пересылке шифруются с помощью ключей верхнего уровня. Ключ в вершине иерархии не шифруется, а задается и хранится у доверенного лица, рассылается пользователям курьерами. Чем ниже уровень ключа, тем чаще он меняется и рассылается по линиям связи. Подобная схема шифрования ключей часто используется в сетях.

6.5. Электронная цифровая подпись

Электронная цифровая подпись (англ. digital signature) – цифровой код (последовательность символов), присоединяемый к электронному сообщению для идентификации отправителя.

По назначению электронная цифровая подпись соответствует обычной подписи на документе, подтверждающей юридические полномочия документа. Электронная цифровая подпись получается методами асимметричной криптографии, основанными на математической функции, комбинирующей открытый текст с последовательностью чисел (ключом).

Алгоритм устроен таким образом, что пара «открытый ключ участника А – закрытый ключ участника Б» позволяет зашифровать сообщение, а пара «закрытый ключ А – открытый ключ Б» его дешифровать.

Технология электронной цифровой подписи пересылаемого документа начинается с формирования его дайджеста (digest) – короткой последовательности чисел, восстановить исходный текст по

которой нельзя. Любое изменение исходного документа вызовет его несоответствие дайджесту. К дайджесту добавляется информация о том, кто подписывает документ, штамп времени и прочее. Получившаяся строка далее зашифровывается секретным ключом подписывающего с использованием того или иного алгоритма. Получившийся зашифрованный набор бит и представляет собой электронную подпись. К подписи обычно прикладывается открытый ключ подписывающего. Получатель дешифрует подпись с помощью открытого ключа. Если подпись нормально дешифровалась и ее содержимое соответствует документу (дайджест и др.), то сообщение считается подтвержденным.

Рис. 6.6. **Технология электронной цифровой подписи**

В целях повышения безопасности используют многократное шифрование блоков информации разными ключами.

В России, для обеспечения правовых условий использования электронной цифровой подписи в электронных документах, принят Федеральный закон от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи». Действие закона распространяется на отношения, возникающие при совершении гражданско-правовых сделок и в других предусмотренных законодательством Российской Федерации случаях.

В законе приводятся следующие основные понятия:

электронный документ – документ, в котором информация представлена в электронно-цифровой форме;

электронная цифровая подпись – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе;

владелец сертификата ключа подписи – физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы);

средства электронной цифровой подписи – аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций – создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей;

сертификат средств электронной цифровой подписи – документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной цифровой подписи установленным требованиям;

закрытый ключ электронной цифровой подписи – уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в элек-

тронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи;

открытый ключ электронной цифровой подписи – уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе;

сертификат ключа подписи – документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и которые выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи;

подтверждение подлинности электронной цифровой подписи в электронном документе – положительный результат проверки соответствующим сертифицированным средством электронной цифровой подписи с использованием сертификата ключа подписи принадлежности электронной цифровой подписи в электронном документе владельцу сертификата ключа подписи и отсутствия искажений в подписанном данной электронной цифровой подписью электронном документе;

пользователь сертификата ключа подписи – физическое лицо, использующее полученные в удостоверяющем центре сведения о сертификате ключа подписи для проверки принадлежности электронной цифровой подписи владельцу сертификата ключа подписи;

информационная система общего пользования – информационная система, которая открыта для использования всеми физическими и юридическими лицами и в услугах которой этим лицам не может быть отказано;

корпоративная информационная система – информационная система, участниками которой может быть ограниченный круг лиц, определенный ее владельцем или соглашением участников этой информационной системы.

Вопросы

1. Криптографические методы информационной безопасности.
2. Классификация методов криптографического закрытия информации.
3. Чем занимается наука криптология.
4. Что такое криптоанализ.
5. Стойкость криптографического метода.
6. Трудоемкость криптографического метода.
7. Основные требования к криптографическому закрытию информации.
8. Шифрование.
9. Классификация криптосистем.
10. Симметричные криптосистемы.
11. Классификация симметричных криптосистем.
12. Шифрование методом замены (подстановки).
13. Одноалфавитная подстановка.
14. Многоалфавитная одноконтурная обыкновенная подстановка.
15. Многоалфавитная одноконтурная монофоническая подстановка.
16. Многоалфавитная многоконтурная подстановка.
17. Шифрование методом перестановки.
18. Шифрование методом гаммирования.
19. Шифрование с помощью аналитических преобразований.
20. Комбинированные методы шифрования.
21. Криптосистемы с открытым ключом (асимметричные).
22. Характеристики существующих шифров.
23. Кодирование.
24. Стеганография.
25. Основные правила криптозащиты.
26. Основные правилами механизма распределения ключей.
27. Электронная цифровая подпись.
28. Технология электронной цифровой подписи.
29. Электронный документ это.
30. Электронная цифровая подпись это.
31. Владелец сертификата ключа подписи это.
32. Средства электронной цифровой подписи это.
33. Сертификат средств электронной цифровой подписи.
34. Закрытый ключ электронной цифровой подписи.
35. Открытый ключ электронной цифровой подписи.
36. Сертификат ключа подписи.

37. Подтверждение подлинности электронной цифровой подписи в электронном документе.
38. Пользователь сертификата ключа подписи.
39. Информационная система общего пользования.
40. Корпоративная информационная система.

Тесты

1. Шифрование методом подстановки:

1. символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста;
2. символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности;
3. шифрование заключается в получении нового вектора как результата умножения матрицы на исходный вектор;
4. символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов;
5. замена слов и предложений исходной информации шифрованными.

2. Шифрование методом перестановки:

1. символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста;
2. символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности;
3. шифрование заключается в получении нового вектора как результата умножения матрицы на исходный вектор;
4. символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов;
5. замена слов и предложений исходной информации шифрованными.

3. Шифрование методом гаммирования:

1. символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста;
2. символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности;
3. шифрование заключается в получении нового вектора как результата умножения матрицы на исходный вектор;

4. символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов;
5. замена слов и предложений исходной информации шифрованными.

4. Шифрование методом аналитических преобразований:
1. символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста;
2. символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности;
3. шифрование заключается в получении нового вектора как результата умножения матрицы на исходный вектор;
4. символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов;
5. замена слов и предложений исходной информации шифрованными.

5. Символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста, это метод:
1. гаммирования;
2. подстановки;
3. кодирования;
4. перестановки;
5. аналитических преобразований.

6. Символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов, это метод:
1. гаммирования;
2. подстановки;
3. кодирования;
4. перестановки;
5. аналитических преобразований.

7. Символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, это метод:
1. гаммирования;
2. подстановки;
3. кодирования;
4. перестановки;
5. аналитических преобразований.

8. Шифрование заключается в получении нового вектора как результата умножения матрицы на исходный вектор, это метод:

1. гаммирования;
2. подстановки;
3. кодирования;
4. перестановки;
5. аналитических преобразований.

9. Шифр DES – это:

1. система, которая предусматривает 3 режима шифрования (простая замена, гаммирование, гаммирование с обратной связью) и один режим выработки имитовставки;
2. система с открытым ключом, предназначенная как для шифрования, так и для аутентификации, основана на трудности разложения очень больших целых чисел на простые сомножители;
3. блочные шифры с ключом переменной длины, продукт экспортируется за пределы страны;
4. шифр, состоящий из 64-битных повторяющихся блоков с 128-битным ключом и восемью проходами;
5. симметричный алгоритм шифрования, имеет блоки по 64 бит и основан на 16-кратной перестановке данных, для зашифровывания использует ключ в 56 бит.

10. Шифр IDEA – это:

1. система, которая предусматривает 3 режима шифрования (простая замена, гаммирование, гаммирование с обратной связью) и один режим выработки имитовставки;
2. система с открытым ключом, предназначенная как для шифрования, так и для аутентификации, основана на трудности разложения очень больших целых чисел на простые сомножители;
3. блочные шифры с ключом переменной длины, продукт экспортируется за пределы страны;
4. шифр, состоящий из 64-битных повторяющихся блоков с 128-битным ключом и восемью проходами;
5. симметричный алгоритм шифрования, имеет блоки по 64 бит и основан на 16-кратной перестановке данных, для зашифровывания использует ключ в 56 бит.

11. Шифр RC2 или RC4 – это:

1. система, которая предусматривает 3 режима шифрования (простая замена, гаммирование, гаммирование с обратной связью) и один режим выработки имитовставки;
2. система с открытым ключом, предназначенная как для шифрования, так и для аутентификации, основана на трудности разложения очень больших целых чисел на простые сомножители;
3. блочные шифры с ключом переменной длины, продукт экспортируется за пределы страны;
4. шифр, состоящий из 64-битных повторяющихся блоков с 128-битным ключом и восемью проходами;
5. симметричный алгоритм шифрования, имеет блоки по 64 бит и основан на 16-кратной перестановке данных, для зашифровывания использует ключ в 56 бит.

12. Шифр RSA – это:

1. система, которая предусматривает 3 режима шифрования (простая замена, гаммирование, гаммирование с обратной связью) и один режим выработки имитовставки;
2. система с открытым ключом, предназначенная как для шифрования, так и для аутентификации, основана на трудности разложения очень больших целых чисел на простые сомножители;
3. блочные шифры с ключом переменной длины, продукт экспортируется за пределы страны;
4. шифр, состоящий из 64-битных повторяющихся блоков с 128-битным ключом и восемью проходами;
5. симметричный алгоритм шифрования, имеет блоки по 64 бит и основан на 16-кратной перестановке данных, для зашифровывания использует ключ в 56 бит.

13. Шифр ГОСТ 28147-89 – это:

1. система, которая предусматривает 3 режима шифрования (простая замена, гаммирование, гаммирование с обратной связью) и один режим выработки имитовставки;
2. система с открытым ключом, предназначенная как для шифрования, так и для аутентификации, основана на трудности разложения очень больших целых чисел на простые сомножители;
3. блочные шифры с ключом переменной длины, продукт экспортируется за пределы страны;
4. шифр, состоящий из 64-битных повторяющихся блоков с 128-битным ключом и восемью проходами;

5. симметричный алгоритм шифрования, имеет блоки по 64 бит и основан на 16-кратной перестановке данных, для зашифровывания использует ключ в 56 бит.

14. Система, которая предусматривает 3 режима шифрования (простая замена, гаммирование, гаммирование с обратной связью) и один режим выработки имитовставки, – это шифр:

1. IDEA;
2. RSA;
3. ГОСТ 28147-89;
4. RC2 или RC4;
5. DES.

15. Система с открытым ключом, предназначенная как для шифрования, так и для аутентификации, основана на трудности разложения очень больших целых чисел на простые сомножители – это шифр:

1. IDEA;
2. RSA;
3. ГОСТ 28147-89;
4. RC2 или RC4;
5. DES.

16. Блочные шифры с ключом переменной длины, продукт экспортируется за пределы страны – это шифр:

1. IDEA;
2. RSA;
3. ГОСТ 28147-89;
4. RC2 или RC4;
5. DES.

17. Шифр, состоящий из 64-битных повторяющихся блоков с 128-битным ключом и восемью проходами, – это шифр:

1. IDEA;
2. RSA;
3. ГОСТ 28147-89;
4. RC2 или RC4;
5. DES.

18. Симметричный алгоритм шифрования имеет блоки по 64 бит и основан на 16 кратной перестановке данных, для зашифровывания использует ключ в 56 бит – это шифр:

1. IDEA;
2. RSA;
3. ГОСТ 28147-89;
4. RC2 или RC4;
5. DES.

Тема 7.

Лицензирование и сертификация в области защиты информации

Изучив тему 7, студент должен:
знать:

- нормы и требования российского законодательства в области лицензирования и сертификации;
- правила построения и функционирования системы лицензирования ФАПСИ;
- порядок оформления и получения лицензий и сертификатов в области информационной безопасности.

акцентировать внимание на понятиях:

- лицензия, сертификат, электронная цифровая подпись, шифровальное средство.

Содержание темы (дидактические единицы и их характеристика):

Нормы и требования российского законодательства в области лицензирования и сертификации. Правила построения и функционирования системы лицензирования ФАПСИ. Порядок оформления и получения лицензий и сертификатов в области информационной безопасности.

Цели и задачи изучения темы: Получение знаний в области лицензирования и сертификации. Ознакомление с правилами построения и функционирования системы лицензирования ФАПСИ. Получение знаний о порядке оформления и получения лицензий и сертификатов в области информационной безопасности.

Порядок изучения темы

Распределение бюджета времени по теме:

- количество часов, отведенных на практические занятия, из них в компьютерной аудитории – 4/4;
- количество часов, отведенных на самостоятельную работу, – 16.

Виды самостоятельной работы студентов:

- изучение учебного пособия «Информационная безопасность»;
- подготовка к участию в форуме по теме «Нормы и требования российского законодательства в области лицензирования и сертификации»;
- изучение дополнительной литературы;
- выполнение тестовых заданий по теме.

Методические указания по изучению вопросов темы

При изучении учебных вопросов:

- изучить тему 7 по учебному пособию «Информационная безопасность»;
- принять участие в форуме по теме «Нормы и требования российского законодательства в области лицензирования и сертификации»;
- изучить дополнительные материалы.

При изучении темы необходимо:

- *читать литературу*:

1. Информационная безопасность: Уч. Пособие. – М.: МЭСИ, 2007.
2. Горбатов В.С. Фатьянов А.А. Правовые основы защиты информации. – М.: МИФИ 1999.
3. Закон Российской Федерации от 10.06.93 «О сертификации продукции и услуг».
4. Закон «О федеральных органах правительственной связи и информации».
5. Закон «О государственной тайне».
6. Постановление Правительства от 24.12.94 №1418 «О лицензировании отдельных видов деятельности».
7. Закон «Об информации, информатизации и защите информации» от 20.02.95 № 24-ФЗ.
8. Постановление от 26.06.95 № 608 «О сертификации средств защиты информации».

- *посетить сайты:* www.sbcinfo/index.htm.

Вопросы темы

1. Законодательство в области лицензирования и сертификации.
2. Правила функционирования системы лицензирования.

7.1. Законодательство в области лицензирования и сертификации

Нормы и требования российского законодательства в области лицензирования и сертификации включают в себя положения ряда нормативных актов Российской Федерации различного уровня.

Первым по времени открытым правовым нормативным актом, который бы регулировал вопросы оборота средств криптографической защиты информации, является принятое *28 мая 1991 г. постановление Верховного Совета СССР № 2195-1 «О видах деятельности, которыми предприятия вправе заниматься только на основании специальных разрешений (лицензий)»*. Этим документом был утвержден перечень отдельных видов деятельности, которыми предприятия на территории страны вправе заниматься только при наличии у них специального разрешения или лицензии.

19 февраля 1993 г. Верховным Советом Российской Федерации был принят закон «О федеральных органах правительственной связи и информации» № 4524-1. Статья 11 данного закона предоставила Федеральному агентству права по определению порядка разработки, производства, реализации, эксплуатации шифровальных средств, предоставления услуг в области шифрования информации, а также порядка проведения работ по выявлению электронных устройств перехвата информации в технических средствах и помещениях государственных структур. Одновременно Федеральному агентству этой статьей дано право осуществлять лицензирование указанных видов деятельности и сертификацию соответствующих товаров и услуг. Пунктом м) той же статьи 11 данного закона Федеральному агентству предоставлено право осуществлять лицензирование и сертификацию телекоммуникационных систем и комплексов высших органов государственной власти Российской Федерации и закрытых (защищенных) с помощью шифровальных средств, систем и комплексов телекоммуникаций органов государственной власти субъектов Российской Федерации, федеральных органов исполнительной власти, а также организаций, предприятий, банков и иных учреждений, расположенных на территории России, независимо от их ведомственной принадлежности и форм собственности.

Полномочия по лицензированию деятельности в области защиты информации, содержащей сведения, составляющие государственную тайну, а также по сертификации средств ее защиты предоставлены Федеральному агентству *законом Российской Федерации от 21.07.93 «О государственной тайне» № 5485-1*. Статья 20 этого закона определила государственные органы, ответственные за защиту такой информации. Статья 27 предписывает осуществлять допуск предприятий, учреждений и организаций к работам по созданию средств защиты секретной информации и оказанию услуг по защите сведений, составляющих государственную тайну, путем получения ими лицензий на данную деятельность. Статья 28 устанавливает обязательность сертификации технических средств, предназначенных для защиты секретных сведений, и определяет государственные органы, ответственные за проведение сертификации указанных средств (ФАПСИ, Министерство обороны, Гостехкомиссия и Министерство безопасности, правопреемником которого является ФСБ).

Во исполнение этих законов в августе 1993 г. Правительством Российской Федерации принято специальное постановление, которое полностью определяет порядок создания и использования криптографических (шифровальных) средств, предназначенных для защиты информации, содержащей сведения, составляющие государственную тайну, начиная от стадии подготовки технического задания на проведение научно-исследовательских работ до серийного производства и установки шифровальной техники в сложные закрытые (защищенные) системы и комплексы обработки, хранения и передачи информации.

Кроме того, в соответствии с упомянутыми законами, а также на основании *закона Российской Федерации от 10.06.93 «О сертификации продукции и услуг»*

№ 5151-1 ФАПСИ *15 ноября 1993 г.* зарегистрировало в Госстандарте России «*Систему сертификации средств криптографической защиты информации» РОСС.RU.0001.030001.* Данный документ определил организационную структуру системы сертификации шифровальных средств ФАПСИ, а также установил основные правила проведения сертификационных исследований и испытаний криптографических средств защиты информации и закрытых с их помощью систем и комплексов обработки, хранения и передачи информации.

В начале 1994 г. Президентом и Правительством был принят пакет нормативных актов, определивших порядок импорта и экспорта шифровальных средств и нормативно-технической докумен-

тации к ним на территории Российской Федерации. Во-первых – это *распоряжение Президента России от 11 февраля 1994 г. № 74-П «О контроле за экспортом из Российской Федерации отдельных видов сырья, материалов, оборудования, технологий и научно-технической информации, которые могут быть применены при создании вооружения и военной техники».* Данным распоряжением утвержден соответствующий перечень, в котором, в частности, указывается, что аппаратура, узлы, компоненты, программное обеспечение и технология производства, специально разработанные или модифицированные для использования в криптографии или выполнения криптоаналитических функций, подлежат экспортному контролю. Во-вторых, – *постановление Правительства от 15.04.94 № 331 «О внесении дополнений и изменений в постановления Правительства Российской Федерации от 06.11.92 № 854 «О лицензировании и квотировании экспорта и импорта товаров (работ, услуг) на территории Российской Федерации» и от 10.12.92 № 959 «О поставках продукции и отходов производства, свободная реализация которых запрещена».* И, наконец, в-третьих – *постановление от 01.07.94 № 758 «О мерах по совершенствованию государственного регулирования экспорта товаров и услуг». 31 октября 1996 г.* этот перечень был дополнен *постановлением Правительства N 1299*, которым утверждено Положение «О порядке лицензирования экспорта и импорта товаров (работ, услуг) в Российской Федерации».

Перечисленные документы установили в том числе, что ввоз и вывоз средств криптографической защиты информации (шифровальной техники) и нормативно-технической документации к ней в стране может осуществляться исключительнона основании лицензии Министерства внешних экономических связей Российской Федерации, выдаваемой на основании решения ФАПСИ о выдаче лицензии. Кроме того, данные документы определили общий порядок выдачи экспортных лицензий на шифровальные средства, направленный на предотвращение утечки секретных сведений и технологий при вывозе из страны средств защиты информации.

Предоставленные Федеральному агентству законами «О федеральных органах правительственной связи и информации» и «О государственной тайне» права по определению порядка осуществления и лицензированию деятельности в области защиты информации нашли свое отражение в *«Положении о государственном лицензировании деятельности в области защиты информации», которое утверждено 27 апреля 1994 г. совместным решением № 10 ФАПСИ и Гостехкомиссии России*, разграничившим сферы компетенции двух этих ведомств

и определившим механизм практического лицензирования, действующий по настоящее время.

Обязательное государственное лицензирование деятельности в области защиты информации криптографическими методами, а также в области выявления электронных устройств перехвата информации в технических средствах и помещениях государственных структур введено *постановлением Правительства от 24.12.94 № 1418 «О лицензировании отдельных видов деятельности»*. Данное постановление распространяет механизм обязательного лицензирования на все виды деятельности в области криптографической защиты информации, независимо от ее характера и степени секретности, на все субъекты этой деятельности, независимо от их организационно-правовой формы, включая и физических лиц.

Новым шагом в деле правового обеспечения деятельности в области защиты информации явилось принятие Федеральным Собранием России *Федерального закона «Об информации, информатизации и защите информации» от 20.02.95 № 24-ФЗ*. Данный закон впервые официально вводит понятие «конфиденциальной информации», которая рассматривается как документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации, и устанавливает общие правовые требования к организации защиты такой информации в процессе ее обработки, хранения и циркуляции в технических устройствах и информационных и телекоммуникационных системах и комплексах и организации контроля за осуществлением мероприятий по защите конфиденциальной информации. При этом следует подчеркнуть, что Закон не разделяет государственную и частную информацию как объект защиты в том случае, если доступ к ней ограничивается.

Кроме того, закон определяет на государственно-правовом уровне электронную цифровую подпись как средство защиты информации от несанкционированного искажения, подмены (имитозащиты) и подтверждения подлинности отправителя и получателя информации (аутентификации сторон). В соответствии со ст. 5 «юридическая сила документа, хранимого, обрабатываемого и передаваемого с помощью автоматизированных информационных и телекоммуникационных систем, может подтверждаться электронной цифровой подписью». При этом «юридическая сила электронной цифровой подписи признается при наличии в автоматизированной системе программно-технических средств, обеспечивающих идентификацию подписи, и соблюдении установленного режима их

использования». Далее закон раскрывает требования, предъявляемые к специализированным программно-техническим средствам, реализующим электронную цифровую подпись, и порядку их использования в информационно-телекоммуникационных системах.

Так, ст. 19 закона «Об информации, информатизации и защите информации» устанавливает обязательность сертификации средств обработки и защиты документированной информации с ограниченным доступом, предназначенных для обслуживания граждан и организаций, а также обязательность получения лицензий для организаций, осуществляющих проектирование и производство средств защиты информации.

Статья 20 определяет основные цели защиты информации. В соответствии с этой статьей таковыми, в частности, являются: предотвращение утечки, хищения, утраты, искажения и подделки информации; предотвращение угроз безопасности личности, общества и государства; предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных сведений; сохранение государственной тайны и конфиденциальности информации.

Пункт 3 ст. 21 возлагает контроль за соблюдением требований к защите информации, за эксплуатацией специальных средств защиты информации, а также обеспечение организационных мер защиты информационных систем, обрабатывающих информацию с ограниченным доступом, в негосударственных структурах на органы государственной власти.

Очень важна ст. 22, которая определяет права и обязанности субъектов в области защиты информации. В частности, пп. 2 и 5 обязывают владельца информационной системы обеспечивать необходимый уровень защиты конфиденциальной информации и оповещать собственников информационных ресурсов о фактах нарушения режима защиты информации. Пунктом 3 риск, связанный с использованием несертифицированных информационных систем и средств их обеспечения и защиты, возлагается на собственника (владельца) систем и средств. Риск, связанный с использованием информации, полученной из таких систем, относится на потребителя информации. Пункт 4 устанавливает право собственника документов или информационной системы обращаться в организации, осуществляющие сертификацию средств защиты таких систем, для

проведения анализа достаточности мер защиты его ресурсов и систем и получения консультаций.

Статья 23 Закона «Об информации, информатизации и защите информации» посвящена защите прав субъектов в сфере информационных процессов и информатизации. Статья устанавливает, что защита прав субъектов в данной сфере осуществляется судом, арбитражным судом и третейскими судами, которые могут создаваться на постоянной или временной основе.

Подписанный 3 апреля 1995 г. *Указ Президента Российской Федерации № 334 «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации»* запрещает любую деятельность, связанную с разработкой, производством, реализацией и эксплуатацией шифровальных средств, предоставлением услуг в области шифрования информации, без лицензии ФАПСИ. Пункты 2, 3 данного документа устанавливают обязательное использование исключительно сертифицированных средств защиты информации во всех государственных структурах, в том числе и в государственных банках Российской Федерации, на предприятиях, работающих по государственному заказу, а также на предприятиях и в организациях при их информационном взаимодействии с Центральным банком России и его структурными подразделениями. Таким образом, обязательность сертификации распространяется теперь не только на средства защиты информации, содержащей сведения, составляющие государственную тайну, но и на средства защиты любой государственно значимой информации независимо от грифа ее секретности. Кроме того, Указ формирует механизм реализации перечисленных выше законодательных актов, возлагая ответственность за их выполнение на ФАПСИ, а также правоохранительные, таможенные и налоговые органы страны.

В течение первой половины 1995 г. Правительством Российской Федерации во исполнение закона «О государственной тайне» *приняты постановление от 15 апреля 1995 г. № 333 «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны» и постановление от 26.06.95 № 608 «О сертификации средств защиты информации».*

Указанные постановления формируют механизм получения предприятиями и организациями, независимо от их организационно-правовой формы, лицензии на право осуществления любой деятельности, связанной с информацией, составляющей государственную тайну, а также общий порядок сертификации средств защиты, предназначенных для защиты секретной информации. В частности, пп. 2 Положения, утвержденного постановлением № 333, устанавливает органы, уполномоченные на ведение лицензионной деятельности, связанной с проведением работ со сведениями, составляющими государственную тайну. Таковыми являются Федеральная служба безопасности России и ее территориальные органы, ФАПСИ, Гостехкомиссия и Служба внешней разведки. Тем же пунктом определяются полномочия перечисленных ведомств:

- выдача лицензий по допуску предприятий и организаций к проведению работ, связанных с использованием секретных сведений, на территории Российской Федерации возлагается на органы ФСБ, а за границей – СВР России;
- выдача лицензий на право создания средств защиты информации возлагается на Гостехкомиссию и ФАПСИ;
- выдача лицензий на право осуществления мероприятий и(или) оказания услуг в области защиты государственной тайны возлагается на ФСБ и ее территориальные органы, Гостехкомиссию, ФАПСИ и СВР.

Постановление от 15.04.95 № 333 устанавливает, что лицензия на право деятельности по проведению работ, связанных с использованием сведений, составляющих государственную тайну, с созданием средств защиты информации и оказанием услуг по защите государственной тайны, может быть выдана предприятию или организации, независимо от формы его собственности, исключительно на основании результатов специальной экспертизы заявителя, в ходе которой будет установлено наличие на данном предприятии всех необходимых условий для сохранения доверенных ему секретных сведений, и государственной аттестации их руководителей, ответственных за защиту сведений, составляющих государственную тайну.

Постановление от 26 июня 1995 г. № 608 устанавливает общие принципы организации систем сертификации средств защиты информации, содержащей сведения, составляющие государственную тайну, всеми ведомствами Российской Федерации, наделенными законом правом проводить подобную сертификацию. Статьи Поло-

жения определяют участников системы сертификации средств защиты информации, их права и обязанности; схемы проведения сертификационных испытаний; порядок выдачи, приостановления и аннулирования сертификатов; порядок оплаты услуг по сертификации, контроля за качеством сертифицированных изделий, а также ответственность сторон за выполнение ими своих обязательств в системе сертификации. Кроме того, данным Положением к средствам защиты информации отнесены и средства контроля эффективности защиты информации.

Принятый Государственной Думой *Федеральный закон «Об участии в международном информационном обмене» от 5 июня 1996 г. N 85-ФЗ* определяет необходимость сертификации средств международного информационного обмена и необходимость лицензирования деятельности в области международного информационного обмена при работе с конфиденциальной информацией. Закон предоставляет ФАПСИ право участвовать в определении перечней документированной информации, вывоз которой из Российской Федерации, и иностранных информационных продуктов, ввоз которых в Российскую Федерацию, ограничен, определять порядок лицензирования деятельности в области международного информационного обмена при работе с конфиденциальной информацией, а также определять порядок сертификации средств и аттестования систем международного информационного обмена.

Перечисленные нормативные акты определили полномочия и компетенцию ФАПСИ в сфере лицензирования деятельности в области защиты и сертификации средств защиты информации.

Лицензированию Федеральным агентством в соответствии с его компетенцией подлежит деятельность по следующим направлениям:

- создание средств защиты информации;
- осуществление мероприятий и оказание услуг по защите государственной тайны;
- деятельность, связанная с шифровальными средствами;
- предоставление услуг в области шифрования информации;
- выявление технических устройств скрытого съема информации, электронных закладных устройств и программных закладок в технических средствах и помещениях государственных структур;
- создание систем и комплексов телекоммуникаций органов государственной власти Российской Федерации;
- создание закрытых (защищенных) с использованием шифровальных средств систем и комплексов телекоммуникаций;

- создание и реализация средств выявления технических устройств скрытого съема информации, электронных закладных устройств и программных закладок.

Указанные направления включают определенное множество отдельных видов деятельности, к которым относятся: разработка, производство, реализация (продажа), эксплуатация, монтаж, установка (инсталяция), наладка, сертификационные испытания, ввоз в страну, вывоз из страны и др.

Сертификации Федеральным агентством в соответствии с его компетенцией подлежат:

- средства (системы, комплексы) криптографической защиты информации;
- средства выявления закладных устройств и программных закладок;
- защищенные технические средства обработки информации;
- закрытые (защищенные) информационные системы и комплексы телекоммуникаций.

В своей деятельности по лицензированию и сертификации ФАПСИ руководствуется положениями указанных выше нормативных актов и строго придерживается исполнения предоставленных ему права и полномочий.

7.2. Правила функционирования системы лицензирования

Рассмотрим правила построения и функционирования системы лицензирования ФАПСИ, вытекающие из приведенных выше нормативных актов и основанные на правах и полномочиях, предоставленных ими Федеральному агентству.

1. *Лицензирование в области защиты информации является обязательным.*

Данное правило устанавливает, что для занятия деятельностью в области защиты информации необходимо получение права на ее осуществление. Причем распространяется это требование на все без исключения направления и отдельные виды деятельности.

2. *Деятельность в области защиты информации физических и юридических лиц, не прошедших лицензирование, запрещена.*

Из содержания данного правила вытекает, что субъекты, не получившие право на осуществление деятельности в области защиты информации и продолжающие ее осуществлять, нарушая установленный порядок, занимаются тем самым противоправной деятельностью. В отношении таких субъектов могут быть применены санкции, предусмотренные действующим Гражданским кодексом и законодательством об административной и уголовной ответственности.

3. *Лицензии ФАПСИ и решения ФАПСИ о выдаче лицензии на право осуществления деятельности в области защиты информации, лицензирование которой относится к компетенции Федерального агентства, выдаются, в основном, юридическим лицам – предприятиям, организациям и учреждениям, независимо от их организационно-правовой формы.*

Данное правило лишь на первый взгляд ущемляет интересы физических лиц, которым не предоставляются права на промышленную, коммерческую деятельность, связанную с шифровальными средствами. Включение данного постулата обусловлено рядом факторов. Во-первых, разработка (производство, монтаж, наладка и т.д.) шифровальных средств требует участия высококлассных специалистов разного профиля. Во-вторых, требованиям, предъявляемым ФАПСИ к заявителю, физическое лицо удовлетворить не в состоянии. В-третьих, для проведения работ в этой области необходимо обеспечение выполнения режимных требований и (для ознакомления, например, с нормами требований по безопасности) наличия допуска к сведениям, составляющим государственную тайну. Лицензии выдаются конкретным юридическим лицам - предприятиям, а не министерствам, ведомствам или ассоциациям в целом. Если разрешаемая в лицензии деятельность не является для лицензиата основной, то в лицензии указывается структурное подразделение, которому предоставляется право осуществления указанного в лицензии вида деятельности.

4. *Лицензии ФАПСИ и решения ФАПСИ о выдаче лицензии выдаются только предприятиям, зарегистрированным на территории Российской Федерации.*

5. *Лицензия ФАПСИ выдается только на основании результатов специальной экспертизы заявителя на соответствие требованиям к предприятию на право деятельности в области защиты информации по заявленному направлению работ и аттестации руководителя предприятия или лиц, уполномоченных им для руководства лицензируемой деятельностью.*

Данное положение устанавливает одну из основных норм, определяющих сущностные и процедурные аспекты системы лицензирования ФАПСИ: лицензия может быть выдана не каждому заяви-

телю, а только предприятию, обладающему соответствующими возможностями, достаточными для осуществления заявленных видов деятельности. Проверка возможностей предприятия осуществляется в ходе специальной экспертизы путем экспертных оценок специалистами специально создаваемых комиссий. С данными требованиями заявитель может быть ознакомлен в Лицензионном центре ФАПСИ. Кроме того, по результатам специальной экспертизы заявителя определяются состав и конкретная формулировка разрешенных видов деятельности, а также условия их осуществления. Уточнение формулировок для различных видов деятельности и заявителей может быть проведено с учетом следующих факторов:

- уровня конфиденциальности защищаемой информации;
- уровня секретности сведений, используемых при осуществлении заявляемой деятельности;
- типа используемого криптографического алгоритма;
- способа технической реализации изделия;
- уровня квалификации персонала;
- назначения изделия, наличия или отсутствия сертификата на него;
- страны – производителя изделия;
- категории помещений и технических средств.

6. *Решение ФАПСИ о выдаче лицензии дается предприятию, подавшему заявление на его получение, на основании результатов технической экспертизы изделия и(или) специальной экспертизы заявителя.*

Основными задачами технической экспертизы являются установление соответствия предъявляемого изделия заявляемым характеристикам (классу, типу шифровальных средств) и проверка возможного использования в коммерческих шифрсредствах алгоритмов и способов их реализации, составляющих государственную тайну.

7. Лицензия, выданная ФАПСИ, действует на всей территории Российской Федерации, если иное не оговорено в ней особо.

Могут налагаться следующие ограничения:

- для региональных представителей, работающих по договорам на реализацию шифрсредств, – в рамках сферы их деятельности;
- для фирм-разработчиков, – разработка криптографических средств защиты и защищенных средств и систем в интересах региональных государственных и коммерческих структур.

8. *Лицензии ФАПСИ и решения ФАПСИ о выдаче лицензии подписываются генеральным директором Федерального агентства или лицом, его замещающим, и заверяются гербовой печатью ФАПСИ.*

9. *Передача лицензии другим юридическим лицам запрещена*.

10. *Лицензия имеет ограниченный срок действия, по истечении которого осуществляется переоформление лицензии в порядке, предусмотренном для ее выдачи*.

Данные нормы определены постановлением Правительства Российской Федерации от 24.12.94 № 1418 для всех систем лицензирования.

11. *Лицензирование осуществляется на платной основе.*

Размер платы за рассмотрение заявления и за выдачу лицензии фиксирован. Размер платы за специальную экспертизу определяется договором на ее проведение.

12. *Для получения лицензии или решения о выдаче лицензии предприятие обязано представить определенный перечень документов, состав которых определяется нормативными актами Правительства Российской Федерации и ФАПСИ.*

Представляемые заявителем документы регистрируются в уполномоченном подразделении Федерального агентства по мере их поступления. Заявление регистрируется только при наличии всех требуемых для оформления лицензии документов.

13. *Рассмотрение заявления и специальная экспертиза должны проводиться в сроки, ограниченные соответствующими нормативными актами*.

На настоящий момент продолжительность рассмотрения заявления установлена сроком 30 суток с момента поступления всех необходимых документов (с возможностью увеличения этого срока в отдельных случаях еще максимум на 60 суток). Специальная экспертиза имеет аналогичную продолжительность с момента заключения договора на ее проведение.

14. *Отказ заявителю в выдаче лицензии должен быть мотивирован.*

Заявителю может быть отказано в получении лицензии в случаях:

- если в документах, представленных заявителем, имеется недостоверная или искаженная информация;
- отрицательного заключения по результатам специальных экспертиз, установивших несоответствие условиям, необходимым для осуществления заявленного вида деятельности и условиям безопасности;
- отрицательного заключения по результатам аттестации руководителя предприятия или лица, уполномоченного им на ведение лицензируемой деятельности;
- отрицательного заключения по результатам технических экспертиз.

15. *При ликвидации предприятия выданная лицензия теряет юридическую силу.*

В случае реорганизации предприятия, изменения его дислокации или наименования юридического лица, утраты лицензии осуществляется ее переоформление. Переоформление лицензии в указанных случаях, за исключением изменения наименования юридического лица, осуществляется в порядке, предусмотренном для ее выдачи.

16. *Выданная лицензия может быть приостановлена или аннулирована.*

Приостановление или аннулирование лицензии осуществляется в случаях:

- представления лицензиатом соответствующего заявления;
- обнаружения недостоверных данных в документах, представленных для получения лицензии;
- нарушения лицензиатом условий действия лицензии;
- невыполнения лицензиатом предписаний или распоряжений государственных органов или приостановления ими деятельности предприятия в соответствии с законодательством Российской Федерации;
- ликвидации предприятия.

Приостановление действия лицензии влечет за собой прекращение деятельности лицензиата по виду деятельности (работ, услуг), указанному в лицензии, до устранения выявленных нарушений.

17. *Решение ФАПСИ о выдаче лицензии на ввоз (вывоз) шифровальных средств выдается только на конкретную партию изделий. Наличие заключенных договоров не является основанием для выдачи положительного решения о возможности ввоза(вывоза) шифровальных средств.*

Данные нормы соответствуют установленному порядку внешнеэкономической деятельности. Заключаемые договора, как правило, содержат статью, учитывающую форс-мажорные обстоятельства, предусматривающие возможный отказ уполномоченных государственных органов в выдаче лицензии на ввоз(вывоз) шифровальных средств. Конкретная партия товара определяется объемом, этапностью и сроками поставок, оговоренных конкретным договором.

Собственно лицензирование деятельности предприятий в области защиты информации включает следующие действия:

- выдачу лицензий (решений о выдаче лицензий) - подачу, рассмотрение заявления на лицензирование, оформление и выдачу лицензий (решений о выдаче лицензий), переоформление лицензий;
- проведение специальной экспертизы заявителя;

- проведение аттестации руководителя предприятия или лиц, уполномоченных им для руководства лицензируемой деятельностью;
- проведение технической экспертизы изделий.

Для получения лицензии заявитель представляет заявление с указанием:

- наименования и организационно-правовой формы, юридического адреса, номера расчетного счета и реквизитов соответствующего банка;
- вида (видов) деятельности с формулировкой видов в соответствии с «Положением о государственном лицензировании в области защиты информации»;
- срока действия лицензии.

Заявление подписывается руководителем предприятия (либо лицом его замещающим) с расшифровкой подписи и заверяется основной печатью предприятия. Заявление на лицензирование подается на имя генерального директора Федерального агентства и направляется только почтой.

Переписка по рабочим материалам и конкретным вопросам, возникающим в ходе процесса лицензирования, в том числе представление дополнительных или ранее не представленных материалов, осуществляется с уполномоченным подразделением Лицензионного центра ФАПСИ.

Заявление о выдаче лицензии принимается к рассмотрению только при наличии всех необходимых, определенных нормативными актами документов, включающих, в первую очередь, заключение по результатам специальной экспертизы, подтверждающее наличие на предприятии необходимых условий для проведения работ по заявленным видам деятельности и соответствие их предъявляемым ФАПСИ требованиям, а также копию документа, подтверждающего прохождение аттестации руководителем предприятия. Заявитель несет ответственность за достоверность представленных сведений. В ходе рассмотрения заявления ФАПСИ вправе произвести проверку достоверности представляемых сведений.

К заявлению на получение лицензии прилагаются:

- копия свидетельства о государственной регистрации предприятия;
- копии учредительных документов (устава, договора и т.д.) с предъявлением оригиналов, если копии не заверены нотариусом;

- копии документов, подтверждающих право собственности, право полного хозяйственного ведения, и (или) договора аренды на имущество, необходимое на ведение заявленной деятельности;
- справка налогового органа о постановке на учет;
- представление органов государственной власти Российской Федерации с рекомендацией или ходатайством о выдаче лицензии;
- документ, подтверждающий оплату рассмотрения заявления.

Проведение специальной экспертизы осуществляется экспертными комиссиями, формируемыми либо Лицензионным центром ФАПСИ, либо аттестационными центрами в рамках определенных этим центрам полномочий.

Возможны два варианта проведения лицензирования:

Первый вариант. Предприятие подает заявление на получение лицензии со всеми перечисленными выше документами, считая его одновременно и заявкой на проведение специальной экспертизы, результаты которой затем прилагаются к поданному заявлению. Датой принятия заявления к рассмотрению в этом случае считается дата утверждения экспертного заключения. Этот вариант является основным.

Второй вариант. Предприятие заранее, на основании отдельной заявки, получает экспертное заключение в Лицензионном центре ФАПСИ или в рекомендованном ему аттестационном центре и вместе с другими требуемыми документами направляет его с заявлением. Датой принятия заявления к рассмотрению в этом случае считается дата регистрации в ФАПСИ полного пакета всех необходимых правильно оформленных документов.

Решение о выдаче или отказе в выдаче лицензии принимается в течение 30 дней со дня принятия заявления к рассмотрению. Выдача лицензий или мотивированных отказов в выдаче лицензий, принятие решений о приостановлении или аннулировании лицензий является прерогативой генерального директора ФАПСИ. Оформленная надлежащим образом лицензия (подписанная генеральным директором ФАПСИ, удостоверенная гербовой печатью Агентства, имеющая уникальный номер, проставленный срок действия и дату регистрации ее в Государственном реестре лицензий ФАПСИ) вручается лицензиату в установленном порядке. Копия лицензии хранится в Лицензионном центре Федерального агентства.

Лицензионный центр ФАПСИ вправе на этапе предварительного рассмотрения заявления согласовать с предприятием вопрос о

снятии заявления или изменении запрашиваемого объема работ. Если заявление оформлено правильно и в приложении имеются все необходимые документы, то Лицензионный центр ФАПСИ регистрирует поступившие документы и направляет заявителю уточненные для него требования по конкретным видам деятельности, а также указывает аттестационный центр, который будет проводить специальную экспертизу.

Подготовленное на основании требований обоснование необходимых условий для осуществления работ по заявленным видам деятельности заявитель представляет в определенный для него аттестационный центр, после чего заключается договор на проведение специальной экспертизы. Если представленная документация или сведения не полны, ФАПСИ не принимает такое заявление к рассмотрению.

Организация и проведение специальных экспертиз предприятий, в целом, возлагается на Лицензионный центр ФАПСИ или уполномоченный аттестационный центр.

Специальная экспертиза заявителя осуществляется на основании заявки предприятия, содержащей лицензируемые виды деятельности и перечни необходимых для их обеспечения производственного и испытательного оборудования, нормативной и методической документации, имеющихся на предприятии, краткой характеристики состава и квалификации персонала предприятия.

Специальная экспертиза заявителя осуществляется экспертной комиссией, состав которой и примерные сроки работы доводятся до заявителя официальным порядком.

В случае необходимости аттестация руководителей предприятий или лиц, уполномоченных ими на руководство лицензируемой деятельностью, может быть проведена Лицензионным центром ФАПСИ или аттестационным центром в ходе проведения специальной экспертизы предприятия. Экспертная комиссия вправе засчитать в качестве документа об аттестации руководителя предприятия официальный документ о прохождении переподготовки по соответствующему профилю на курсах, имеющих лицензию на осуществление учебной деятельности и право квалифицировать уровень полученных знаний.

Расходы на специальную экспертизу, а также на аттестацию руководителя предприятия полностью относятся на счет заявителя. Экспертиза проводится на основе хозяйственного договора между Лицензионным центром ФАПСИ или аттестационным центром и

предприятием-заявителем. Оплата работы членов экспертной комиссии производится исключительно центром, осуществлявшим экспертизу, за счет средств, получаемых в соответствии с указанным договором.

Конкретный порядок проведения специальных экспертиз заявителей, методические рекомендации по организации и проведению аттестации руководителей предприятий или лиц, уполномоченных ими на руководство лицензируемой деятельностью, определяются ведомственной инструкцией, разрабатываемой Лицензионным центром ФАПСИ.

Целями такой экспертизы являются:

- обоснованное отнесение какого-либо аппаратного, аппаратно-программного или программного средства или его функциональной части, встроенного блока, программного модуля к категориям средств защиты информации, средств криптографической защиты информации (шифровальных средств) и(или) защищенного оборудования;
- обоснованное отнесение научно-технической и(или) нормативно-технической документации или технологии к категориям информации и технологии двойного применения, которые могут быть использованы при создании военной техники;
- определение уровня защищенности конфиденциальной информации при ее обработке, хранении и передаче по линиям связи, а также эффективности контроля ее защиты в конкретных защищенных системах и комплексах телекоммуникаций, объектах информатики и информационно-телекоммуникационных системах и комплексах;
- определение уровня эффективности обнаружения закладных электронных устройств перехвата информации техническими средствами;
- контроль за деятельностью лицензиатов в области защиты информации.

Техническая экспертиза проводится на основании решения Федерального агентства или Лицензионного центра ФАПСИ либо самим Лицензионным центром, либо, по его поручению, аккредитованными аттестационными или испытательными сертификационными центрами (лабораториями), а также в предусмотренных законодательными или иными нормативными актами Российской Фе-

дерации случаях на основании обращений судебных, правоохранительных, таможенных, налоговых органов или отдельных предприятий, по заявлениям субъектов лицензионной и внешнеторговой деятельности в области защиты информации.

Вопросы

1. Лицензирование и сертификация в области защиты информации.
2. Законодательство в области лицензирования и сертификации.
3. Нормы и требования российского законодательства в области лицензирования и сертификации.
4. Постановление Правительства РФ № 2195-1 «О видах деятельности, которыми предприятия вправе заниматься только на основании специальных разрешений (лицензий)».
5. Закон РФ «О федеральных органах правительственной связи и информации» № 4524-1.
6. Закон Российской Федерации от 21.07.93 «О государственной тайне» № 5485-1.
7. Постановление Правительства РФ от 24.12.94 № 1418 «О лицензировании отдельных видов деятельности».
8. Федеральный Закон «Об информации, информатизации и защите информации» от 20.02.95 № 24-ФЗ?
9. Указ Президента РФ № 334 «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации».
10. Постановление Правительства РФ от 15 апреля 1995 г. № 333 «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны».
11. Постановление Правительства РФ от 26.06.95 № 608 «О сертификации средств защиты информации».
12. Федеральный Закон «Об участии в международном информационном обмене» от 5 июня 1996 г. N 85-ФЗ.
13. Какие виды деятельности подлежат лицензированию.

14. Какие средства подлежат сертификации Федеральным агентством.
15. Правила функционирования системы лицензирования.
16. В каких случаях заявителю может быть отказано в получении лицензии?
17. В каких случаях выданная лицензия может быть приостановлена или аннулирована?
18. Какие документы прилагаются к заявлению на получение лицензии?
19. Каковы цели специальной экспертизы?

Тест

1. Сертификации подлежат:

1. средства криптографической защиты информации;
2. средства выявления закладных устройств и программных закладок;
3. защищенные технические средства обработки информации;
4. защищенные информационные системы и комплексы телекоммуникаций;
5. все вышеперечисленные средства.

Тема 8.

Критерии безопасности компьютерных систем «Оранжевая книга». Руководящие документы Гостехкомиссии

Изучив тему 8, студент должен:
знать:

- руководящие документы Гостехкомиссии Российской Федерации;
- стандарт США «Оранжевая книга»;

уметь:

- классифицировать автоматизированные системы, согласно руководящим документам Гостехкомиссии Российской Федерации.

акцентировать внимание на понятиях:

- стратегия, подотчетность, гарантии, минимальная защита, индивидуальная защита, мандатная защита, верифицированная защита, идентификация, шифрование.

Содержание темы (дидактические единицы и их характеристика):

Наиболее известным документом, определяющим критерии, по которым должна оцениваться защищенность вычислительных систем, и те механизмы защиты, которые должны использоваться в системах обработки секретной (конфиденциальной) информации, является так называемая «Оранжевая книга», представляющая собой стандарт США. Гостехкомиссия при Президенте Российской Федерации разработала и опубликовала пять руководящих документов, посвященных вопросам защиты компьютерных систем.

Цели и задачи изучения темы: Получение знаний по критериям, с помощью которых оценивается защищенность вычислитель-

ных систем. Ознакомление со стандартом США «Оранжевая книга». Изучение руководящих документов Гостехкомиссии Российской Федерации.

Порядок изучения темы

Распределение бюджета времени по теме:

- количество часов, отведенных на практические занятия, из них в компьютерной аудитории – 4/4;
- количество часов, отведенных на самостоятельную работу, – 16.

Виды самостоятельной работы студентов:

- изучение учебного пособия «Информационная безопасность»;
- подготовка к участию в форуме по теме «Руководящие документы Гостехкомиссии Российской Федерации»;
- изучение дополнительной литературы;
- выполнение тестовых заданий по теме.

Методические указания по изучению вопросов темы

При изучении учебных вопросов:

- изучить тему 8 по учебному пособию «Информационная безопасность»;
- принять участие в форуме по теме «Руководящие документы Гостехкомиссии Российской Федерации»;
- изучить дополнительные материалы.

При изучении темы необходимо:

- *читать литературу*:

1. «Информационная безопасность: Уч. пособие. – М.: МЭСИ, 2007.
2. Гостехкомиссия России. Руководящий документ. «Защита от несанкционированного доступа к информации термины и определения».
3. Гостехкомиссия России. Руководящий документ. «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации».
4. Гостехкомиссия России. Руководящий документ. «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации».
5. Гостехкомиссия России. Руководящий документ. «Автоматизированные системы. Защита от несанкционированного доступа к

информации. Классификация автоматизированных систем и требования по защите информации».

6. Гостехкомиссия России. Руководящий документ. «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты секретной информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники».

- *посетить сайты:* www.sbcinfo/index.htm.

Вопросы темы

1. Критерии безопасности компьютерных систем «Оранжевая книга».
2. Руководящие документы Гостехкомиссии Российской Федерации.

8.1. Критерии безопасности компьютерных систем. «Оранжевая книга»

Наиболее известным документом, определяющим критерии, по которым должна оцениваться защищенность вычислительных систем, и те механизмы защиты, которые должны использоваться в системах обработки секретной (конфиденциальной) информации, является так называемая «Оранжевая книга», представляющая собой стандарт США «Критерии оценки гарантированно защищенных вычислительных систем в интересах министерства обороны США», принятый в 1983 г. Его принятию предшествовали пятнадцатилетние исследования, проводившиеся специально созданной рабочей группой и национальным бюро стандартов США.

Стандартом предусмотрено шесть фундаментальных требований, которым должны удовлетворять те вычислительные системы, которые используются для обработки конфиденциальной информации. Требования разделены на три группы: стратегия, подотчетность, гарантии – в каждой группе по два требования следующего содержания.

1. Стратегия.

Требование 1 – стратегия обеспечения безопасности: необходимо иметь явную и хорошо определенную стратегию обеспечения безопасности.

Требование 2 – маркировка: управляющие доступом метки должны быть связаны с объектами.

2. Подотчетность.

Требование 3 – идентификация: индивидуальные субъекты должны идентифицироваться.

Требование 4 – подотчетность: контрольная информация должна храниться отдельно и защищаться так, чтобы со стороны ответственной за это группы имелась возможность отслеживать действия, влияющие на безопасность.

3. Гарантии.

Требование 5 – гарантии: вычислительная система в своем составе должна иметь аппаратные/программные механизмы, допускающие независимую оценку на предмет достаточного уровня гарантии того, что система обеспечивает выполнение изложенных выше требований (с первого по четвертое).

Требование 6 – постоянная защита: гарантированно защищенные механизмы, реализующие перечисленные требования, должны быть постоянно защищены от «взламывания» и/или несанкционированного внесения изменений.

В зависимости от конкретных значений, которым отвечают автоматизированные системы, они разделены на четыре группы (D, C, B, A), которые называются:

D – минимальная защита;

C – индивидуальная защита;

B – мандатная защита;

A – верифицированная защита.

Группы систем делятся на классы: системы относимые к группе D, образуют один класс D, к группе C – два класса C1 и C2, к группе B – три класса B1, B2, B3, к группе A – один класс A1 с выделением части систем вне класса.

Краткая характеристика классов

D – минимальная защита – системы, подвергнутые оцениванию, но не отвечающие требованиям более высоких классов;

C1 – защита, основанная на индивидуальных мерах, – системы, обеспечивающие разделение пользователей и данных. Они содержат внушающие доверие средства, способные реализовать ограничения по доступу, накладываемые на индивидуальной основе, т.е. позволяющие пользователям иметь надежную защиту их информации и не дающие другим пользователям считывать или разрушать их данные. Допускается кооперирование пользователей по уровням секретности;

C2 – защита, основанная на управляемом доступе, – системы, осуществляющие не только разделение пользователей, как в системах C1, но и разделение их по осуществляемым действиям;

B1 – защита, основанная на присваивании имен отдельным средствам безопасности, – системы, располагающие всеми возможностями систем класса C, и дополнительно должны быть формальные модели механизмов обеспечения безопасности, присваивания имен защищаемым данным (включающим и выдаваемым за пределы системы) и средства мандатного управления доступом ко всем поименованным субъектам и объектам;

B2 – структурированная защита – системы, построенные на основе ясно определенной формально задокументированной модели, с мандатным управлением доступом ко всем субъектам и объектам, располагающие усиленными средствами тестирования и средствами управления со стороны администратора системы;

B3 – домены безопасности – системы, монитор обращений которых контролирует все запросы на доступ субъектов к объектам, не допускающие несанкционированных изменений. Объем монитора должен быть небольшим с тем, чтобы его состояние и работу можно было сравнительно легко контролировать и тестировать. Кроме того должны быть предусмотрены: сигнализация о всех попытках несанкционированных действий и восстановление работоспособности системы;

A1 – верифицированный проект – системы, функционально эквивалентные системам класса B3, но верификация которых осуществлена строго формальными методами. Управление системой осуществляется по строго определенным процедурам. Обязательно введение должности администратора безопасности.

За время, прошедшее со времени разработки требований «Оранжевой книге», многие из них уже устарели. Появился ряд новых требований к безопасности компьютерных систем, не отраженных в «Оранжевой книги». Это связано с тем, что за это время было обнаружено множество ранее неизвестных угроз безопасности компьютерным системам.

К основным недостаткам «Оранжевой книги» относятся следующие:

- совершенно не рассматриваются криптографические средства защиты информации;
- практически не рассматриваются вопросы обеспечения защиты системы от атак, направленных на временный вывод системы из строя (атаки класса «отказ в обслуживании»);

- не уделяется должного внимания вопросам защиты защищаемой системы от негативных воздействий программных закладок и компьютерных вирусов;
- недостаточно подробно рассматриваются вопросы взаимодействия нескольких экземпляров защищенных систем в локальной или глобальной вычислительной сети;
- требования к средствам защиты от утечки конфиденциальной информации из защищенной системы ориентированы на хранение конфиденциальной информации в базах данных и мало приемлемы для защиты электронного документооборота.

8.2. Руководящие документы Гостехкомиссии

В 1992 г. Гостехкомиссия при Президенте Российской Федерации опубликовала пять руководящих документов, посвященных вопросам защиты компьютерных систем:

- «Защита от несанкционированного доступа к информации. Термины и определения»;
- «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации»;
- «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»;
- «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»;
- «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты секретной информации от несанкционированного доступа в автоматизированных системах и средства вычислительной техники».

Рассмотрим один из основных руководящих документов «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации». В данном документе выделено девять классов защищенности автоматизированных систем от несанкционированного доступа к информации, а для каждого класса определен минимальный состав необходимых механизмов защиты и

требования к содержанию защитных функций каждого из механизмов в каждом из классов систем.

Классы систем разделены на три группы, причем основным критерием деления на группы приняты специфические особенности обработки информации, а именно:

третья группа – системы, в которых работает один пользователь, допущенный ко всей обрабатываемой информации, размещенной на носителях одного уровня конфиденциальности. К группе отнесены два класса, обозначенные 3Б и 3А;

вторая группа – системы, в которых работает несколько пользователей, которые имеют одинаковые права доступа ко всей информации, обрабатываемой и/или хранимой на носителях различного уровня конфиденциальности. К группе отнесены два класса, обозначенные 2Б и 2А;

первая группа – многопользовательские системы, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности, причем различные пользователи имеют различные права на доступ к информации. К группе отнесено пять классов: 1Д, 1Г, 1В, 1Б, 1А.

Требования к защите растут от систем класса 3Б к классу 1А.

Все механизмы защиты разделены на четыре подсистемы следующего назначения:

1. управление доступом;
2. регистрация и учета;
3. криптографическое закрытие;
4. обеспечение целостности.

Состав перечисленных подсистем приведен в табл.7.1, причем знаком (+) обозначена необходимость соответствующих средств для каждой группы.

Наличие рассмотренных методик и закрепление их в официальных документах создает достаточно надежную базу для защиты информации на регулярной основе.

Однако нетрудно видеть, что, с точки зрения современной постановки задачи защиты информации, имеющиеся методики являются недостаточными по ряду причин, а именно:

1. Они ориентированы на защиту информации только в средствах ЭВТ, в то время как имеет место устойчивая тенденция органического сращивания автоматизированных и традиционных технологий обработки информации;

2. учитываются далеко не все факторы, оказывающие существенное влияние на уязвимость информации, а потому и подлежащие учету при определении требований к защите;

3. в научном плане они обоснованы недостаточно (за исключением требований к защите информации от утечки по техническим каналам).

Таблица 7.1

Состав средств защиты для типовых систем

Подсистемы и требования	**Классы систем**								
	3Б	**3А**	**2Б**	**2А**	**1Д**	**1Г**	**1В**	**1Б**	**1А**
1. Подсистема управления доступом 1.1. Идентификация, проверка подлинности и контроль доступа субъектов в систему:	+	+	+	+	+	+	+	+	+
к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ;	-	-	-	+	-	+	+	+	+
к программам;	-	-	-	+	-	+	+	+	+
к томам, каталогам, файлам, записям, полям записей.	-	-	-	+	-	+	+	+	+
1.2. Управление потоками информации.	-	-	-	+	-	+	+	+	+
2. Подсистема регистрации и учета 2.1. Регистрация и учет: Входа/выхода субъектов доступа в/из системы (узла сети);	+	+	+	+	+	+	+	+	+
выдачи печатных (графических) выходных документов;	-	+	-	+	-	+	+	+	+
запуска/завершения программ процессов (заданий, задач);	-	-	-	+	-	+	+	+	+
доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи;	-	-	-	+	-	+	+	+	+
доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей;	-	-	-	+	-	+	+	+	+
изменения полномочий субъектов доступа;	-	-	-	-	-	-	+	+	+
создаваемых защищаемых объектов доступа.	-	-	-	+	-	-	+	+	+

Подсистемы и требования	Классы систем								
	3Б	**3А**	**2Б**	**2А**	**1Д**	**1Г**	**1В**	**1Б**	**1А**
2.2. Учет носителей информации.	+	+	+	+	+	+	+	+	+
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей.	-	+	-	+	-	+	+	+	+
2.4. Сигнализация попыток нарушения защиты.	-	-	-	-	-	-	+	+	+
3. Криптографическая подсистема 3.1. Шифрование конфиденциальной информации.	-	-	-	+	-	-	-	+	+
3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах.	-	-	-	-	-	-	-	-	+
3.3. Использование аттестованных (сертифицированных) криптографических средств.	-	-	-	+	-	-	-	+	+
4. Подсистема обеспечения целостности 4.1. Обеспечение целостности программных средств и обрабатываемой информации.	+	+	+	+	+	+	+	+	+
4.2. Физическая охрана средств вычислительной техники и носителей информации.	+	+	+	+	+	+	+	+	+
4.3. Наличие администратора (службы) защиты информации в АСОД.	-	-	-	+	-	-	+	+	+
4.4. Периодическое тестирование СЗИ НСД.	+	+	+	+	+	+	+	+	+
4.5. Наличие средств восстановления СЗИ НСД.	+	+	+	+	+	+	+	+	+
4.6. Использование сертифицированных средств защиты.	-	+	-	+	-	-	+	+	+

Вопросы

1. Критерии безопасности компьютерных систем.
2. «Оранжевая книга».
3. Какие группы фундаментальных требований определены в «Оранжевой книге»?
4. Требования группы фундаментальных требований «Оранжевой книги» Стратегия.
5. Требования группы фундаментальных требований «Оранжевой книги» Подотчетность.
6. Требования группы фундаментальных требований «Оранжевой книги» Гарантии.
7. На какие группы разделяются автоматизированные системы в «Оранжевой книге».
8. Краткая характеристика классов в «Оранжевой книге».
9. Основные недостатки «Оранжевой книги».
10. Руководящие документы Гостехкомиссии.
11. Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».

Тесты

1. В стандарте США «Оранжевой книге» фундаментальное требование, которое относится к группе Стратегия:

1. индивидуальные субъекты должны идентифицироваться;
2. контрольная информация должна храниться отдельно и защищаться так, чтобы со стороны ответственной за это группы имелась возможность отслеживать действия, влияющие на безопасность;
3. необходимо иметь явную и хорошо определенную систему обеспечения безопасности;
4. вычислительная система в своем составе должна иметь аппаратные/программные механизмы, допускающие независимую оценку на предмет того, что система обеспечивает выполнение изложенных требований;
5. гарантированно защищенные механизмы, реализующие перечисленные требования, должны быть постоянно защищены от «взламывания» и/или несанкционированного внесения изменений.

2. В стандарте США «Оранжевой книге» фундаментальное требование, которое относится к группе Стратегия:

1. управляющие доступом метки должны быть связаны с объектами;
2. контрольная информация должна храниться отдельно и защищаться так, чтобы со стороны ответственной за это группы имелась возможность отслеживать действия, влияющие на безопасность;
3. индивидуальные субъекты должны идентифицироваться;
4. вычислительная система в своем составе должна иметь аппаратные/программные механизмы, допускающие независимую оценку на предмет того, что система обеспечивает выполнение изложенных требований;
5. гарантированно защищенные механизмы, реализующие перечисленные требования, должны быть постоянно защищены от «взламывания» и/или несанкционированного внесения изменений.

3. В стандарте США «Оранжевой книге» фундаментальное требование, которое относится к группе Подотчетность:

1. управляющие доступом метки должны быть связаны с объектами;
2. необходимо иметь явную и хорошо определенную систему обеспечения безопасности;
3. индивидуальные субъекты должны идентифицироваться;
4. вычислительная система в своем составе должна иметь аппаратные/программные механизмы, допускающие независимую оценку на предмет того, что система обеспечивает выполнение изложенных требований;
5. гарантированно защищенные механизмы, реализующие перечисленные требования, должны быть постоянно защищены от «взламывания» и/или несанкционированного внесения изменений.

4. В стандарте США «Оранжевой книге» фундаментальное требование, которое относится к группе Подотчетность:

1. управляющие доступом метки должны быть связаны с объектами;
2. необходимо иметь явную и хорошо определенную систему обеспечения безопасности;
3. гарантированно защищенные механизмы, реализующие перечисленные требования, должны быть постоянно защищены от «взламывания» и/или несанкционированного внесения изменений;

4. вычислительная система в своем составе должна иметь аппаратные/программные механизмы, допускающие независимую оценку на предмет того, что система обеспечивает выполнение изложенных требований;
5. контрольная информация должна храниться отдельно и защищаться так, чтобы со стороны ответственной за это группы имелась возможность отслеживать действия, влияющие на безопасность.

5. В стандарте США «Оранжевой книге» фундаментальное требование, которое относится к группе Гарантии:

1. управляющие доступом метки должны быть связаны с объектами;
2. необходимо иметь явную и хорошо определенную систему обеспечения безопасности;
3. индивидуальные субъекты должны идентифицироваться;
4. вычислительная система в своем составе должна иметь аппаратные/программные механизмы, допускающие независимую оценку на предмет того, что система обеспечивает выполнение изложенных требований;
5. контрольная информация должна храниться отдельно и защищаться так, чтобы со стороны ответственной за это группы имелась возможность отслеживать действия, влияющие на безопасность.

6. В стандарте США «Оранжевой книге» фундаментальное требование, которое относится к группе Гарантии:

1. управляющие доступом метки должны быть связаны с объектами;
2. защищенные механизмы, реализующие перечисленные требования, должны быть постоянно защищены от «взламывания» и/или несанкционированного внесения изменений;
3. индивидуальные субъекты должны идентифицироваться;
4. необходимо иметь явную и хорошо определенную систему обеспечения безопасности;
5. контрольная информация должна храниться отдельно и защищаться так, чтобы со стороны ответственной за это группы имелась возможность отслеживать действия, влияющие на безопасность.

7. В стандарте США «Оранжевой книге» минимальная защита – это группа:

1. A;
2. B;
3. C;
4. D;
5. E.

8. В стандарте США «Оранжевой книге» индивидуальная защита – это группа:

1. A;
2. B;
3. C;
4. D;
5. E.

9. В стандарте США «Оранжевой книге» мандатная защита – это группа:

1. A;
2. B;
3. C;
4. D;
5. E.

10. В стандарте США «Оранжевой книге» верифицированная защита – это группа:

1. A;
2. B;
3. C;
4. D;
5. E.

11. В стандарте США «Оранжевой книге» системы, подвергнутые оцениванию, но не отвечающие требованиям более высоких классов, – это группа:

1. A;
2. B;
3. C;
4. D;
5. E.

12. В стандарте США «Оранжевой книге» системы, обеспечивающие разделение пользователей и данных, – это группа:

1. A1;
2. B1;
3. B2;
4. C1;
5. C2.

13. В стандарте США «Оранжевой книге» системы, осуществляющие не только разделение пользователей, но и разделение их по осуществляемым действиям, – это группа:

1. A1;
2. B1;
3. B2;
4. C1;
5. C2.

14. В стандарте США «Оранжевой книге» системы, дополнительно должны быть формальные модели механизмов обеспечения безопасности, присваивания имен защищаемым данным и средства мандатного управления доступом ко всем поименованным субъектам и объектам, группа:

1. A1;
2. B1;
3. B2;
4. C1;
5. C2.

15. В стандарте США «Оранжевой книге» системы, дополнительно должны быть формальные модели механизмов обеспечения безопасности, присваивания имен защищаемым данным и средства мандатного управления доступом ко всем поименованным субъектам и объектам, – это группа:

1. A1;
2. B1;
3. B2;
4. C1;
5. C2.

16. В стандарте США «Оранжевой книге» системы, построенные на основе ясно определенной формально задокументированной модели, с мандатным управлением доступом ко всем субъектам и объектам, располагающие усиленными средствами тестирования и средствами управления со стороны администратора системы, – это группа:

1. A1;
2. B1;
3. B2;
4. C1;
5. C2.

17. В стандарте США «Оранжевой книге» системы, монитор обращений которых контролирует все запросы на доступ субъектов к объектам, не допускающие несанкционированных изменений, – это группа:

1. A1;
2. B1;
3. B2;
4. B3;
5. C1.

18. В стандарте США «Оранжевой книге» управление системой осуществляется по строго определенным процедурам, обязательно введение должности администратора безопасности, – это группа:

1. A1;
2. B1;
3. B2;
4. C1;
5. C2.

19. В руководящем документе Гостехкомиссии системы, в которых работает один пользователь, допущенный ко всей обрабатываемой информации, размещенной на носителях одного уровня конфиденциальности, – относятся к группе:

1. первой;
2. второй;
3. третьей;
4. четвертой;
5. пятой.

20. В руководящем документе Гостехкомиссии системы, в которых работает несколько пользователей, которые имеют одинаковые права доступа ко всей информации, обрабатываемой и/или хранимой на носителях различного уровня конфиденциальности, – относятся к группе:

1. первой;
2. второй;
3. третьей;
4. четвертой;
5. пятой.

21. В руководящем документе Гостехкомиссии многопользовательские системы, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности, причем различные пользователи имеют различные права на доступ к информации, – относятся к группе:

1. первой;
2. второй;
3. третьей;
4. четвертой;
5. пятой.

Для итогового контроля необходимо проведение:

- коллоквиумов для закрепления знаний, полученных из лекционного материала;
- аудиторных практических заданий;
- написание эссе;
- зачета и экзамена (как семестровый и итоговый контроль знаний по окончанию изучения всей дисциплины).

Глоссарий

Алгоритмический контроль – заключается в том, что задача, решенная по какому-либо алгоритму, проверяется повторно по сокращенному алгоритму с достаточной степенью точности.

Атака – действие, предпринимаемое нарушителем в поиске и использовании той или иной уязвимости. Угрозы могу быть разделены на угрозы не зависящие от деятельности человека, и искусственные угрозы, связанные с деятельностью человека.

Аутентификация – установление подлинности, заключается в проверке, является ли проверяемый объект (субъект) в самом деле тем, за кого себя выдает.

Биометрические технологии – идентификация человека по уникальным, присущим только ему биологическим признакам.

Владелец информации – субъект, осуществляющий владение и пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации.

Владелец сертификата ключа подписи – физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы).

Вредоносные программы – программы, к которым относятся: классические файловые вирусы, сетевые черви, троянские программы, спам, хакерские утилиты и прочие программы, наносящие заведомый

вред компьютеру, на котором они запускаются на выполнение, или другим компьютерам в сети.

Дешифровывание – процесс, при котором из шифротекста извлекается открытый текст.

Доступ к информации – получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств.

Естественные угрозы – угрозы, вызванные воздействиями на АСОИ и ее элементы объективных физических процессов или стихийных природных явлений, не зависящих от человека.

Закрытый ключ электронной цифровой подписи – уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи.

Защита информации – деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Защита информации от агентурной разведки – деятельность по предотвращению получения защищаемой информации агентурной разведкой.

Защита информации от иностранной технической разведки – деятельность по предотвращению получения защищаемой информации иностранной разведкой с помощью технических средств.

Защита информации от аварийных ситуаций – создание средств предупреждения, контроля и организационных мер по исключению НСД на комплексе средств автоматизации в условиях отказов его функционирования, отказов системы защиты информации, сис-

тем жизнеобеспечения людей на объекте размещения и при возникновении стихийных бедствий.

Защита информации от иностранной разведки – деятельность по предотвращению получения защищаемой информации иностранной разведкой.

Защита информации от непреднамеренного воздействия – деятельность по предотвращению воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений или иных нецеленаправленных на изменение информации воздействий, связанных с функционированием технических средств, систем или с деятельностью людей, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Защита информации от несанкционированного воздействия – деятельность по предотвращению воздействия на защищаемую информацию с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Защита информации от несанкционированного доступа – деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации. Заинтересованными субъектами, осуществляющими несанкционированный доступ к защищаемой информации, могут выступать: государство, юридическое лицо,

		группа физических лиц, в том числе общественная организация, отдельное физическое лицо.
Защита информации от разглашения	–	деятельность по предотвращению несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.
Защита информации от утечки	–	деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа к защищаемой информации и от получения защищаемой информации [иностранными] разведками.
Защищаемая информация	–	информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации. Собственниками информации могут быть – государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.
Злоумышленник	–	нарушитель, намеренно идущий на нарушение из корыстных побуждений.
Идентификация	–	присвоение какому-либо объекту или субъекту уникального образа, имени или числа.
Интернет	–	объединение в масштабе всей планеты группы сетей, которое использует единый протокол для передачи данных.
Информационная безопасность РФ	–	состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.
Информационная система	–	совокупность документов и массивов документов и информационных технологий.

Информационная система общего пользования – информационная система, которая открыта для использования всеми физическими и юридическими лицами и в услугах которой этим лицам не может быть отказано.

Информационные процессы – процессы сбора, накопления, обработки хранения, распределения и поиска информации.

Информационные ресурсы – документы или массив документов, существующие отдельно или в составе информационной системы.

Информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.
Информация является одним из объектов гражданского права том числе и прав собственности, владения, пользования.

Искусственные угрозы – угрозы АСОИ, вызванные деятельностью человека. Среди них, исходя из мотивации действий, можно выделить непреднамеренные и преднамеренные.

Категорирование защищаемой информации – установление градаций важности защиты защищаемой информации.

Классические вирусы – это программы, распространяющие свои копии по ресурсам локального компьютера.

Ключ – используется в процессе шифровки и дешифровки.

Кодирование информации – осуществляется заменой слов и предложений исходной информации кодами.

Компьютерные преступления против государственных и общественных интересов – преступления, направленные против государственной и общественной безопасности (например, угрожающие обороноспособности государства, злоупотребления с автоматизированными системами голосования и т.д.).

Компьютерные преступления против личных прав и частной сферы – незаконный сбор данных о лице, разглашение частной информации (например, банковской или врачебной тайны, информации о расходах и т.д.).

Контроль доступа к аппаратуре – означает, что внутренний монтаж аппаратуры и технологические органы и пульты управления закрыты крышками, дверцами или кожухами, на которые установлены датчики.

Контроль организации защиты информации – проверка соответствия состояния организации, наличия и содержания документов требованиям правовых, организационно-распорядительных и нормативных документов по защите информации.

Контроль состояния защиты информации – проверка соответствия организации и эффективности защиты информации установленным требованиям и/или нормам в области защиты информации.

Контроль эффективности защиты информации – проверка соответствия эффективности мероприятий по защите информации установленным требованиям или нормам эффективности защиты информации.

Конфиденциальность информации – известность ее содержания только имеющим соответствующие полномочия субъектам.

Корпоративная информационная система – информационная система, участниками которой может быть ограниченный круг лиц, определенный ее владельцем или соглашением участников этой информационной системы.

Кракер – лицо, изучающее систему с целью ее взлома. Именно кракеры реализуют свои криминальные наклонности в похищении информации и написании вирусов, разрушающих ПО. Они применяют различные способы атак на компьютерную систему, используя принципы построения протоколов сетевого

обмена. Кракеры разрабатывают специальное программное обеспечение, засылая его на взломанную машину.

Криптоанализ – исследование возможности расшифровки информации без ключа.

Криптография – построение и исследование математических методов преобразования информации.

Мероприятие по защите информации – совокупность действий по разработке и/или практическому применению способов и средств защиты информации.

Мероприятие по контролю эффективности защиты информации – совокупность действий по разработке и/или практическому применению методов, способов и средств контроля эффективности защиты информации.

Метод контроля эффективности защиты информации – порядок и правила применения определенных принципов и средств контроля эффективности защиты информации.

Нарушитель – лицо, предпринявшее попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства.

Непреднамеренное воздействие на защищенную информацию – воздействие на нее из-за ошибок пользователя, сбой техники или программных средств, природных явлений и т.д.

Несанкционированное воздействие – на защищенную информацию – воздействие с нарушением правил ее изменения.

Несанкционированный доступ – получение защищенной информации заинтересованным субъектом с нарушением правилом доступа к ней.

Нормы эффективности защиты информации – значения показателей эффективности защиты информации, установленные нормативными документами.

Носитель информации – физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов.

Объект защиты – информация или носитель информации или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации.

Ограничение доступа – создание некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям.

Одноалфавитная подстановка – прямая замена символов шифруемого сообщения другими буквами того же самого или другого алфавита.

Орган защиты информации – административный орган, осуществляющий организацию защиты информации.

Организационные мероприятия по защите информации *в АСОИ* – разработка и реализация административных и организационно-технических мер при подготовке и эксплуатации системы.

Организационный контроль эффективности защиты информации – проверка полноты и обоснованности мероприятий по защите информации требованиям нормативных документов по защите информации.

Организация защиты информации – содержание и порядок действий по обеспечению защиты информации.

Открытый ключ электронной цифровой подписи – уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе.

Подтверждение подлинности электронной цифровой подписи в электронном документе – положительный результат проверки соответствующим сертифицированным средством электронной цифровой подписи с использованием сертификата ключа подписи принадлежности электронной цифровой подписи в электронном документе владельцу сертификата ключа подписи и отсутствия искажений в подписанном данной электронной цифровой подписью электронном документе.

Показатель эффективности защиты информации – мера или характеристика для оценки эффективности защиты информации.

Пользователь (потребитель) информации – субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением.

Пользователь сертификата ключа подписи – физическое лицо, использующее полученные в удостоверяющем центре сведения о сертификате ключа подписи для проверки принадлежности электронной цифровой подписи владельцу сертификата ключа подписи.

Правило доступа к информации – совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям.

Право доступа к информации – совокупность правил доступа к информации, установленных правовыми документами или собственником, владельцем информации.

Преднамеренные (умышленные) угрозы – связаны с корыстными устремлениями людей (злоумышленников).

Предоставление привилегий на доступ – к информации заключается в том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы.

Разграничение доступа – в вычислительной системе – разделение информации, циркулирующей в ней, на части и организация доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями.

Сертификат ключа подписи – документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и которые выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи.

Сертификат средств электронной цифровой подписи – документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной цифровой подписи установленным требованиям.

Сетевые черви – программы, распространяющие свои копии по локальным и/или глобальным сетям.

Сжатие информации – метод криптографического преобразования информации.

Система защиты информации – совокупность органов и/или исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации.

Скамеры – мошенники, рассылающие свои послания в надежде поймать на наживку наивных и жадных. Интернет-телефония становится все более популярной. На сегодня зарегистрировано уже довольно много случаев обращения мошенников к пользователям Skype – сервисом IP-телефонии, позволяющим пользователям связываться посредством компьютер-компьютер и компьютер-телефон.

Собственник информации – субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами.

Спамеры – те, от кого приходят в наши почтовые ящики не запрошенные массовые рассылки.

Способ защиты информации – порядок и правила применения определенных принципов и средств защиты информации.

Средства электронной цифровой подписи – аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций – создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей.

Средство защиты информации – техническое, программное средство, вещество и/или материал, предназначенные или используемые для защиты информации.

Средство контроля эффективности защиты информации – техническое, программное средство, вещество и/или материал, предназначенные или используемые для контроля эффективности защиты информации.

Стеганография – метод скрытой передачи информации.

Стойкость метода – тот минимальный объем зашифрованного текста, статистическим анализом которого можно вскрыть исходный текст. Таким образом стойкость шифра определяет допустимый объем информации, зашифровываемый при использовании одного ключа.

Субъект доступа к информации – участник правоотношений в информационных процессах. Информационные процессы – процессы создания, обработки, хранения, защиты от внутренних и внешних угроз, передачи, получения, использования и уничтожения информации.

Тестовый контроль – применяется для проверки работоспособности комплекса средств автоматизации при помощи испытательных программ.

Техника защиты информации – средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации.

Технический контроль эффективности защиты информации – контроль эффективности защиты информации, проводимый с использованием средств контроля.

Троянский конь – программы, осуществляющие различные несанкционированные пользователем действия: сбор информации и ее передачу злоумышленнику, ее разрушение или злонаме-

ренную модификацию, нарушение работоспособности компьютера, использование ресурсов компьютера.

Трудоемкость метода – число элементарных операций, необходимых для шифрования одного символа исходного текста.

Угроза информационной безопасности в компьютерной системе – события или действия, которые могут вызвать изменения функционирования КС, связанные с нарушением защищенности информации, обрабатываемой в ней.

Удаленная атака – несанкционированное информационное воздействие на распределенную вычислительную систему, программно осуществляемое по каналам связи.

Утечка информации – неконтролируемое распространение защищенной информации путем ее разглашения, несанкционированного доступа.

Уязвимость информации – возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создадутся условия для реальной угрозы безопасности в ней.

Фишеры *(от англ. fisher – рыбак)* – сравнительно недавно появившаяся разновидность Интернет-мошенников, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию: различные пароли, пин-коды, данные, используя фальшивые электронные адреса и поддельные веб-сайты и т.п.

Фишинг *(ловля на удочку)* – это распространение поддельных сообщений от имени банков или финансовых компаний. Целью такого сообщения является сбор логинов, паролей и пин-кодов пользователей.

Фракеры – приверженцы электронного журнала Phrack, осуществляют взлом интрасети в познавательных целях для получения информации

о топологии сетей, используемых в них программно-аппаратных средствах и информационных ресурсах, а также реализованных методах защиты. Эти сведения могут тем или иным способом (покупка, хищение и т.п.), попасть к заинтересованным в них лицам, которые и осуществят НСД.

Хакер – в XIX веке называли плохих игроков в гольф, своего рода дилетантов.

Цель защиты информации – предотвращение ущерба собственнику, владельцу, пользователю информации в результате возможной утечки информации и/или несанкционированного и непреднамеренного воздействия на информацию.

Черный пиар – акция, которая имеет цель опорочить ту или иную фирму, компанию, политического кандидата и т.п.

Шифрование – изменение исходного текста так, чтобы скрыть от посторонних его содержание.

Шифрование информации – преобразование информации, в результате, которого содержание информации становится непонятным для субъекта, не имеющего соответствующего доступа. Результат шифрования называется **шифротекстом**.

Шифротекст – зашифрованное сообщение.

Экономические компьютерные преступления – являются наиболее распространенными. Они совершаются по корыстным мотивам и включают в себя компьютерное мошенничество, кражу программ («компьютерное пиратство»), кражу услуг и машинного времени, экономический шпионаж.

Электронная цифровая подпись – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием за-

крытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

Электронная цифровая подпись *(англ. digital signature)* – это цифровой код (последовательность символов), присоединяемый к электронному сообщению для идентификации отправителя.

Электронный документ – документ, в котором информация представлена в электронно-цифровой форме.

Эффективность защиты информации – степень соответствия результатов защиты информации поставленной цели.

Эффективность защиты информации – степень соответствия результатов защиты поставленной цели. Объектом защиты может быть информация, ее носитель, информационный процесс, в отношении которого необходимо производить защиту в соответствии с поставленными целями.

Список литературы

Законодательные и нормативно-методические акты и материалы

1. Гостехкомиссия России. Руководящий документ. «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».
2. Гостехкомиссия России. Руководящий документ. «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты секретной информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники».
3. Гостехкомиссия России. Руководящий документ. «Защита от несанкционированного доступа к информации термины и определения».
4. Гостехкомиссия России. Руководящий документ. «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации».
5. Гостехкомиссия России. Руководящий документ. «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации».
6. Гражданский кодекс Российской Федерации. – Ч. 1 и 2.
7. Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента РФ № Пр-1895 от 9 сентября 2000 г.
8. Закон РФ «О государственной тайне».
9. Закон РФ «О федеральных органах правительственной связи и информации».
10. Федеральный Закон от 04. 07. 1996 г. № 85-ФЗ «Об участии в международном информационном обмене».
11. Федеральный Закон от 20. 02. 1995 г. № 24-ФЗ «Об информации, информатизации и защите информации».
12. Закон РФ от 27 ноября 1992 г. № 4015-1 «Об организации страхового дела в Российской Федерации».
13. Закон РФ от 10.01.2002 № 1-ФЗ «Об электронной цифровой подписи».
14. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к ин-

формации. Гостехкомиссия России. Сборник руководящих документов по защите информации от несанкционированного доступа. – М., 1998.
15. Концепция развития страхования в Российской Федерации. Утверждена распоряжением Правительства РФ 25. 09. 2002 г.
16. Критерии оценки безопасности компьютерных систем МО США («Оранжевая книга») TCSTC (Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28-STD, 1983).
17. Методика ОСАО «Ингосстрах» Расчет и экономическое обоснование тарифных ставок по страхованию информационных систем. – М. 2001 г.
18. Постановление от 26.06.95 № 608 «О сертификации средств защиты информации».
19. Постановление Правительства от 24.12.94 № 1418 «О лицензировании отдельных видов деятельности».
20. Правила страхования информационных систем ОСАО «Ингосстрах».– М., 2001.
21. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от НСД. Показатели защищенности от НСД к информации. – М.: Гостехкомиссия РФ, 1996.
22. Стандарт ISO:17799-00 (Стандарт Великобритании BS 7799-95 «Практические правила управления информационной безопасностью»).

Монографии, учебная литература

1. Автоматизированные информационные технологии в экономике/Под ред. И.Т. Трубилина. – М.: Финансы и статистика, 2003.
2. Аналитико-статистический обзор о деятельности 155 страховых компаний России по итогам 2002 г. – М.: Центр экономического анализа агентства «Интерфакс», 2003.
3. Архипов А.П., Гомелля В.Б. Основы страхового дела: Учеб. пособие. – М.: Маркет ДС, 2002.
4. Беззубцев О.А. О мерах по защите информационных технологий, используемых в государственном управлении // Бизнес и безопасность в России. – 2003. – №1.
5. Вихорев С.В., Кобцев Р.Ю. Как узнать – откуда напасть, или откуда исходит угроза безопасности информации // Конфидент. – 2002. – № 2.

6. Волковский В.И. Угрозы информационной безопасности: последствия неизбежны. // Бизнес и безопасность в России. – 2002. – № 1.
7. Волковский В.И. Экономическая безопасность и информация. //Бизнес и безопасность в России. – 2002. – № 2.
8. Гайковия В.Ю., Першин А.Ю.Безопасность электронных банковских систем. – М.: Единая Европа, 1994.
9. Гульбин Ю. Преступления в сфере компьютерной информации // Российская юстиция. – 1997 – № 10.
10. Данилина Н.М., Кузьмин А.С., Пярин В.А. Как застраховать информационные риски // Бизнес и безопасность в России. – 2001. – № 3.
11. Емельянов А.А. Имитационное моделирование в управлении рисками. – СПб.: Инжэкон, 2000.
12. Емельянов А.А., Власова Е.А., Дума Р.В. Имитационное моделирование экономических процессов: Учеб. пособие / Под ред. А.А. Емельянова. – М.:
13. Завгородний В.И. Комплексная защита информации в компьютерных системах: Учеб. пособие – М.: Логос, 2001.
14. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2000.
15. Косарев А.В. Информационная безопасность: оценка размеров риска // Современные образовательные технологии подготовки специалистов в экономических вузах России. Ч.4. – М.: Финансовая академия, 2001.
16. Кравченко С.В. Информационная безопасность предприятия и защита коммерческой тайны // Экономика и производство. – 1999. – № 3.
17. Мельников В.В. Безопасность информации в автоматизированных системах. – М.: Финансы и Статистика, 2003.
18. Мур М. Откуда исходит угроза. // Эксперт, Цифровой мир. – 2002. – №7(23).
19. Панасенко С.П., Батура В.П. Основы криптографии для экономистов: Учеб.пособие / Под ред. Л.Г. Гагариной. – М.: Финансы и статистика, 2005.
20. Петров А.А. Компьютерная безопасность: криптографические методы защиты. – М.: ДМК Пресс, 2000.
21. Родионов И.И, Гиляревский Р.С., Цветкова В.А., Залаев Г.З. Рынок информационных услуг и продуктов. – М.: МК-Периодика, 2002.

22. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М.: Радио и связь, 2001.
23. Симонов С., Колдышев П. Обеспечение информационной безопасности в вычислительных комплексах //Jet Info. Информационный бюллетень. – 2002. – № 4 (107).
24. Щербаков А.Ю. Компьютерная безопасность: теория и практика. – М.: Нолидж, 2001.
25. Фролов К.В. и др. Безопасность России. – М.: МГФ «Знание», 2005 г.
26. Герасименко В.А., Малюк А.А. «Основы защиты информации», ППО «Известия», 1997 г.
27. Милославская Н.Г., Толстой А.И. Интрасети: доступ в Internet, защита. – М.: ООО «ЮНИТИ-ДАНА», Москва, 2000.
28. Проскурин В.Г., Крутов С.В. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах. – М.: Радио и связь, 2000.
29. Белкин П.Ю. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных. – М.: Радио и связь, 1999 г.
30. Касперский Е.В. Компьютерные вирусы: что это такое и как с ними бороться. – М.: «СК Пресс», 1998.
31. Фролов А.В., Фролов Г.В. Осторожно: компьютерные вирусы. – М.: Диалог-МИФИ, 1996.
32. Горбатов В.С. Фатьянов А.А. Правовые основы защиты информации. – М.: МИФИ, 1999.