МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Учебно-методическое пособие

Томск
Издательский Дом Томского государственного университета
2014

УДК 004.056.5
ББК 32.88-421
П291

П291 **Информационная безопасность** : учеб.-метод. пособие / сост. А.Е. Петелин. – Томск : Томский государственный университет, 2014. – 100 с.

Данное учебно-методическое пособие предназначено для организации самостоятельной работы студентов по курсу «Информационная безопасность». В дополнение к представленному теоретическому материалу приводятся вопросы для самоконтроля и две контрольные работы.

Для студентов факультета инновационных технологий Томского государственного университета.

УДК 004.056.5
ББК 32.88-421

Рецензент –
доктор физ.-мат. наук, профессор,
зав. кафедрой прикладной математики
Томского государственного архитектурно-строительного университета
С.Н. Колупаева

ПРЕДИСЛОВИЕ

Роль информации в современном мире крайне велика. В данный исторический период осуществляется переход от индустриального общества к информационному, в котором информация становится более важным ресурсом, чем материальные или энергетические ресурсы. Появилось много отраслей производства, которые практически не имеют материальной составляющей и состоят из одной информации (например, дизайн, создание программного обеспечения, реклама и пр.). В связи с постоянным ростом роли информационных систем в деятельности предприятий, учреждений, органов власти, а также в связи с постоянным ростом правонарушений в области информационных систем, широкому спектру специалистов необходимо уделять значительное внимание вопросам защиты информации.

Настоящее учебно-методическое пособие разработано для студентов факультета инновационных технологий Томского государственного университета, обучающихся по направлениям подготовки бакалавров 09.03.03 «Прикладная информатика».

Методические указания содержат краткие теоретические сведения об угрозах и каналах утечки информации (раздел 1), информационно-законодательного обеспечения Российской Федерации (раздел 2), способах обеспечения безопасности компьютерных систем (раздел 3), аудита информационной безопасности (раздел 4), управления рисками (раздел 5) и сведения об обеспечении информационной безопасности человека (раздел 6). В каждом разделе приводятся ссылки на рекомендуемую литературу, где тема соответствующего раздела освещена более обстоятельно.

В разделе 7 приводится список вопросов для самоконтроля знаний. В разделе 8 описано, как выбрать номер варианта контрольной работы. В разделах 9 и 10 представлены варианты контрольной работы № 1 и № 2, а также рекомендации по их выполнению и оформлению.

Замечания и предложения по совершенствованию учебно-методического пособия автор просит направлять на email: aepetelin@gmail.com

1. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ

Под *угрозой* безопасности информации понимают потенциальное нарушение безопасности, любое обстоятельство, которое может явиться причиной нанесения ущерба государству, юридическому или физическому лицу.

Выделяют три типа угроз: 1) нарушения конфиденциальности (информация становится известной не уполномоченному на это лицу); 2) нарушения целостности (несанкционированное изменение информации, в том числе её удаление); 3) нарушения доступности (блокирование доступа к информации).

При передаче информации используются: источник сигнала, среда распространения и приемник информации (рис. 1).

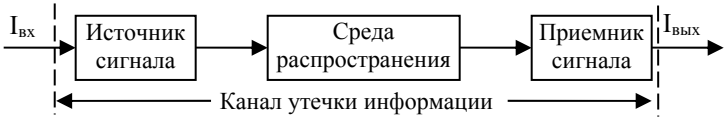

Рис. 1. Структура канала утечки информации [1]

На вход канала поступает информация от ее источника. Среда распространения – часть пространства, в которой перемещается носитель. Она характеризуется набором физических параметров, определяющих условия перемещения носителя с информацией: 1) физические препятствия для субъектов и материальных тел; 2) мера ослабления (или пропускания энергии) сигнала на единицу длины; 3) частотная характеристика (неравномерность ослабления частотных составляющих спектра сигнала); 4) вид и мощность помех для сигнала. Приемник сигнала выполняет функцию, обратную функции передатчика.

Если получатель информации санкционированный, то канал передачи информации называется *функциональным*, в противном случае – *каналом утечки информации*.

Обычно технические каналы утечки информации классифицируют по [1, 2]: 1) физической природе носителя информации (опти-

ческие, акустические, радиоэлектронные и материально-вещественные); 2) информативности (информативные, малоинформативные и неинформативные); 3) времени функционирования (постоянные, эпизодические и случайные) и 4) структуре (одноканальные и составные). Основным классификационным признаком технических каналов утечки информации является физическая природа носителя информации.

1.1. Оптический канал утечки информации

Носителем информации в *оптическом канале* является электромагнитное поле в диапазоне 0,46–0,76 мкм (видимый свет) и 0,76–13 мкм (инфракрасные излучения). Среда распространения в оптическом канале информации возможна трех видов: безвоздушное (космическое) пространство, атмосфера и оптические световоды.

Визуальное наблюдение является самым древним и очень эффективным методом сбора информации. Так, фотографировать можно на относительно большом расстоянии (в сотни километров от объекта наблюдения, например, из космоса) и при этом фотография обладает большой информационной емкостью. Примерно в 99 % случаев для получения информации применяется разнообразная оптика.

Спецслужбы давно и широко применяют различные оптические приборы для скрытного наблюдения и регистрации информации в дневных и ночных условиях при любой погоде. Для видеонаблюдения в дневное время применяются традиционные оптические приборы: бинокли, монокуляры, подзорные трубы, телескопы и др. Для ведения разведки ночью находят применение специальные телевизионные камеры, работающие при низком уровне освещённости, и приборы ночного видения.

В последнее время наблюдается значительный рост применения подвижных видеозаписывающих систем в основном двух типов [3]: 1) на основе камкодеров (видеокамеры со встроенным портативным видеомагнитофоном); 2) на основе кассетных видеомагнитофонов настольного типа и миниатюрных видеокамер. Для передачи видеоинформации она, как правило, кодируется кодером,

передается по проводным или беспроводным каналам связи, а затем раскодируется декодером и показывается на экране телевизора, монитора и пр. (рис. 2).

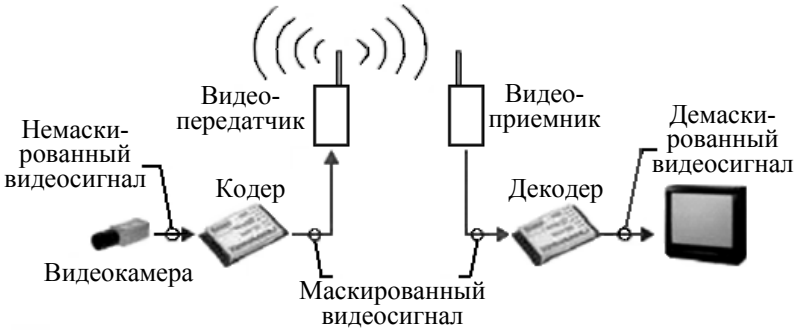

Рис. 2. Схема работы стандартного видеокомплекта

До недавнего времени атмосфера и безвоздушное пространство были единственной средой распространения световых волн. Но с разработкой волоконно-оптической технологии появились оптоволоконные линии связи, которые устойчивы к внешним помехам, имеют малое затухание и долговечны. Хотя возможность утечки информации из волоконно-оптического кабеля существенно ниже, чем из электрического, но при определенных условиях такая утечка возможна. Для съема информации в месте доступа к кабелю разрушают его защитную оболочку, прижимают фотодетектор приемника к очищенной площадке и изгибают кабель на угол, при котором часть световой энергии направляется на фотодетектор приемника.

1.2. Акустический канал утечки информации

Носителем информации в *акустическом канале* являются упругие волны в инфразвуковом (менее 16 Гц), звуковом (16 Гц – 20 кГц) и ультразвуковом (свыше 20 кГц) диапазонах частот. Источниками акустических колебаний являются [4]: механические колебательные системы (в т.ч. органы речи человека), способные

при определенных условиях осуществлять механические колебания; преобразователи акустичесиких колебаний в электрические и обратно – пьезоэлементы, микрофоны, телефоны, громкоговорители и пр. Дальность *акустического канала* утечки информации мала. Так, речь человека при обычной громкости может быть непосредственно подслушана злоумышленником на удалении единиц, в редких случаях – десятков метров. Для повышения дальности добывания речевой информации применяются два вида составного акустического канала утечки информации: акусторадиоэлектронной и акустооптический [5].

Акусторадиоэлектронный канал утечки информации состоит из акустического приемника, размещаемого злоумышленником в помещении с конфиденциальной информацией, и радиоэлектронного ретранслятора, обеспечивающего достаточную дальность для съема информации злоумышленником за пределами контролируемой зоны. Частным случаем акусторадиоэлектронного является акустоэлектрический канал утечки информации, который возникает вследствие преобразования информативного сигнала из акустического в электрический за счет «микрофонного» эффекта в электрических элементах вспомогательных технических средств и систем (звонков телефонных аппаратов, трансформаторов, катушек индуктивности и т. д.).

Акустоэлектрический канал утечки информации можно создать или непосредственным (гальваническим) подключением к линиям связи или с использованием «высокочастотного навязывания». В первом случае для подслушивания, например, телефонных разговоров используются специальные высокочувствительные низкочастотные усилители, подключенные к линиям связи (в этом случае дальность перехвата речевой информации, как правило, не превышает нескольких десятков метров). Метод «высокочастотного навязывания» в основном используется для перехвата разговоров, ведущихся в помещении, путем подключения к линии телефонного аппарата при положенной микротелефонной трубке, т. е. в ситуации, когда телефонный разговор не ведется и цепь питания микрофона разомкнута (дальность перехвата информации может достигать нескольких сот метров).

Несмотря на то, что цепь микрофона телефонного аппарата разомкнута рычажным переключателем, между цепью микрофона и выходом линии существует паразитная емкость $C_п$ порядка 5–15 пФ (рис. 3). На достаточно высоких частотах емкостное сопсопротивление этого переключателя будет относительно невысоким, поэтому навязываемые высокочастотные колебания через емкость $C_п$ будут приложены к микрофону. Если в это время на микрофон действует достаточное звуковое давление опасного сигнала (разговор в помещении, где расположен телефонный аппарат), то на выходе микрофона появится напряжение опасного сигнала. Происходит модуляция высокочастотных колебаний опасным речевым сигналом, которые перехватываются злоумышленником [6].

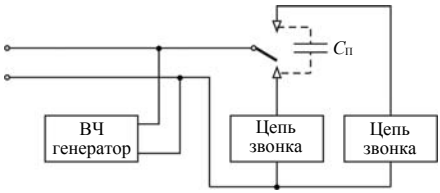

Рис. 3. Принцип реализации высокочастотного навязывания в телефонном аппарате

Акустооптический канал утечки информации образуется путем съема информации с плоской поверхности, колеблющейся под действием акустической волны с информацией, лазерным лучом в инфракрасном диапазоне. В качестве такой поверхности, как правило, используется внешнее стекло закрытого окна в помещении, в котором циркулирует конфиденциальная информация (рис. 4). В месте соприкосновения лазерного луча со стеклом происходит акустооптическое преобразование, т. е. модуляция лазерного луча акустическими сигналами от разговаривающих в помещении людей. Модулированный лазерный луч принимается оптическим приемником аппаратуры лазерного подслушивания, преобразуется в электрический сигнал, усиливается, фильтруется и демодулируется.

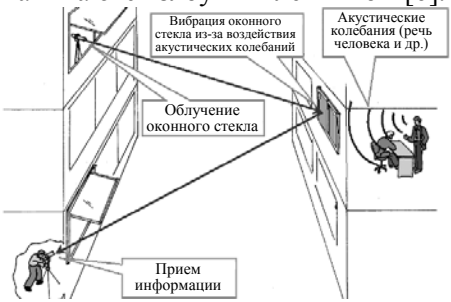

Рис. 4. Схема акустооптического канала утечки информации

1.3. Радиоэлектронный канал утечки информации

В *радиоэлектронном канале* утечки информации в качестве носителей используются электрические, магнитные и электромагнитные поля в радиодиапазоне, а также электрический ток. Вариантов условий для возникновения опасных сигналов очень много. Например, в усилительных каскадах любого радиоэлектронного средства (радиоприемника, телевизора, радиотелефона и др.) могут возникнуть условия для генерации сигналов на частотах вне звукового диапазона, которые модулируются электрическими сигналами акустоэлектрических преобразователей. Функции акустоэлектрических преобразователей могут выполнять элементы генераторов (катушки индуктивности, конденсаторы), являющиеся функциональными устройствами.

При обработке информации техническими средствами создаются побочные электромагнитные излучения, которые могут распространять обрабатываемую информацию с дальностью до 1 км [7, 8]. Наиболее опасными с этой точки зрения являются работающие ЭВМ, в особенности в пластмассовых неметаллизированных корпусах. Ориентировочные дальности обнаружения радиоизлучений элементов ЭВМ приведены в табл. 1.

Таблица 1

Дальность обнаружения радиоизлучений элементов ЭВМ

Элемент ЭВМ	Дальность обнаружения, м	
	электромагнитного	электрического
Системный блок	2–40	1–30
Монитор	25–120	10–55
Клавиатура	15–50	15–30
Печатающее устройство	5–35	10–80

Излучения элементов ЭВМ, конечно, уменьшаются при преодолении препятствий различной природы (квартирные перегородки, стены, окна и др.), но этого бывает недостаточно, и зло-

умышленник, находясь, допустим, в соседнем помещении, может считывать закрытую информацию с работающего ЭВМ.

1.4. Материально-вещественный канал утечки информации

Источниками и носителями информации в *материально-вещественном канале* являются субъекты (люди) и материальные объекты (макро- и микрочастицы), которые имеют четкие пространственные границы локализации. Утечка информации в этих каналах сопровождается физическим перемещением людей и материальных тел с информацией за пределы контролируемой зоны.

К основным источникам материально-вещественного канала утечки информации относятся: 1) черновики различных документов и макеты материалов, узлов, блоков, устройств, разрабатываемых в ходе научно-исследовательских и опытно-конструкторских работ, ведущихся в организации; 2) отходы делопроизводства и издательской деятельности на предприятии (организации), в том числе использованная копировальная бумага, забракованные листы при оформлении документов и их размножении; 3) нечитаемые дискеты ЭВМ из-за их физических дефектов и искажений загрузочных или других кодов; 4) бракованная продукция и ее элементы; 5) отходы производства в газообразном, жидком и твердом виде.

Перенос информации в материально-вещественном канале за пределы контролируемой зоны осуществляется: 1) сотрудниками организации и предприятия; 2) воздушными массами атмосферы; 3) жидкой средой; 4) излучениями радиоактивных веществ.

Потери носителей с ценной информацией возможны при отсутствии четкой системы учета носителей с закрытой информацией. Например, испорченный машинисткой лист отчета может быть выброшен ею в корзину, из которой он будет перенесен в бак для мусора, а далее при перегрузке бака или транспортировки мусора на свалку лист может быть унесен ветром и поднят злоумышленником.

Для предприятий химической, парфюмерной, фармацевтиче-

ской и других сфер разработки и производства продукции, технологические процессы которых сопровождаются использованием или получением различных газообразных или жидких веществ (материалов), возможны выбросы отходов, по свойствам которых злоумышленник может определить состав и другие характеристики продукции.

Многообразие рассмотренных каналов утечки информации предоставляет злоумышленнику большой выбор возможностей для добывания информации. При этом злоумышленник, как правило, использует *несколько каналов* утечки информации, что позволяет увеличить вероятность обнаружения и распознавания информации и повысить ее достоверность.

Заметим, что в настоящем учебно-методическом пособии приведено краткое описание каналов утечки информации. Более детально эта тема изложена в [1]. Там же, а также в [9], приводится довольно подробное описание технических средств предотвращения утечки информации.

1.5. Комплексный подход к защите информации

При организации комплексного подхода к защите информации в организации осуществляется выявление всевозможных угроз по совокупности каналов утечки информации и предотвращение возможных потерь по любой из выявленных угроз. Только комплексный подход может с достаточно большой вероятностью гарантировать информационную безопасность, но при этом организация комплексного подхода является дорогостоящей операцией, поскольку приходится учитывать большое множество угроз. Например, в офисе любой организации можно выделить не менее 30 источников угроз (рис. 5). На рис. 5 использованы следующие обозначения: 1 – утечка за счет структурного звука в стенах и перекрытиях; 2 – съем информации с ленты принтера, плохо стертых дискет и пр.; 3 – съем информации с использованием видеозакладок; 4 – программно-аппаратные закладки и ПК; 5 – радиозакладки в стенах и мебели; 6 – съем информации по системе вентиляции; 7 – лазерный съем акустической информации с окон; 8 – производ-

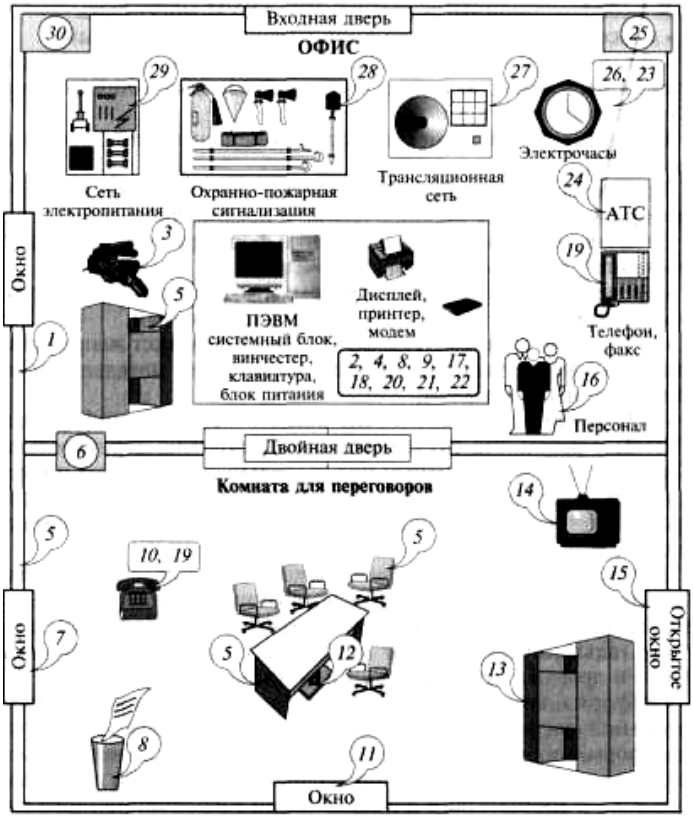

Рис. 5. Обобщенная схема каналов утечки информации в офисе организации [4]

ственные и технологические отходы; 9 – вредоносные программы; 10 – съем информации за счет наводок и «навязывания»; 11 – дистанционный съем видеоинформации (оптика); 12 – съем акустической информации с использованием диктофонов; 13 – хищение носителей информации; 14 – высокочастотный канал утечки в бытовой технике; 15 – съем информации направленным микрофоном; 16 – внутренние каналы утечки информации (через обслуживающий персонал); 17 – несанкционированное копирование; 18 – утечка за счет побочного излучения информации; 19 – съем инфор-

мации за счет использования «высокочастотного навязывания»; 20 – съем информации с клавиатуры по акустическому каналу; 21 – съем информации с дисплея по электромагнитному каналу; 22 – визуальный съем информации с дисплея и принтера; 23 – наводки по линии коммуникации и сторонние проводники; 24 – утечка через линии связи; 25 – утечка по цепям заземления; 26 – утечка по сети электрочасов; 27 – утечка по трансляционной сети и громкоговорящей связи; 28 – утечка по охранно-пожарной сигнализации; 29 – утечка по сети; 30 – утечка по сети отопления, газо- и водоснабжения, электропитания. При рассмотрении прилегающей территории можно выделить еще большее число источников угроз.

2. МЕХАНИЗМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Основными механизмами правового регулирования защиты информации являются нормативно-правовые акты в области информационной безопасности: акты федерального законодательства и нормативно-методические документы [10].

К актам федерального законодательства в РФ относятся [1]: Конституция РФ; законы федерального уровня (включая федеральные конституционные законы и кодексы); указы Президента РФ; постановления Правительства РФ; нормативные правовые акты федеральных министерств и ведомств; нормативные правовые акты субъектов РФ, органов местного самоуправления и т. д. Основным актом федерального законодательства в РФ является Конституция РФ.

2.1. Конституция Российской Федерации

Конституция РФ определяет базовые принципы отношений в информационной сфере. Этого вопроса касаются, в частности, следующие статьи [9, 11]:

– любые нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина, не могут применяться, если они не опубликованы официально для всеобщего

сведения (ст. 15, п. 3);

– каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (ст. 23);

– сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются (ст. 24);

– каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом, перечень сведений, составляющих государственную тайну, определяется федеральным законом (ст. 29);

– каждый имеет право на достоверную информацию о состоянии окружающей среды (ст. 42);

– интеллектуальная собственность охраняется законом (ст. 44);

– в Российской Федерации не должны издаваться законы, отменяющие или умаляющие права и свободы человека и гражданина (ст. 55).

2.2. Концепция национальной безопасности

Пока в Российской Федерации не существует ни отдельного органа исполнительной власти, создающего и проводящего информационную политику, ни, тем более, единого властного органа (по примеру США или Германии), который мог бы объединить все функции, связанные с обеспечением информационной безопасности. Реализация функций в настоящее время рассредоточена между несколькими государственными структурами.

Государственные структуры, ответственные за поддержку информационной безопасности в стране.

Контроль за обеспечением защиты государственной тайны в органах государственной власти, на предприятиях, в учреждениях и организациях осуществляют:

1. Комитет Государственной Думы по безопасности – структура в Государственной Думе Федерального собрания России, в ведении которой находятся рассмотрение и подготовка законопроектов по вопросам безопасности государства и граждан.

2. Совет безопасности России (Совбез России) – совещательный орган, осуществляющий подготовку решений Президента Российской Федерации по вопросам обеспечения защищённости жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, проведения единой государственной политики по обеспечению национальной безопасности.

3. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) – федеральный орган исполнительной власти России, осуществляющий реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности. В ведении ФСТЭК находится деятельность по технической защите конфиденциальной информации; деятельность по разработке и (или) производству средств защиты конфиденциальной информации.

Федеральная служба безопасности Российской Федерации (ФСБ России) – единая централизованная система органов федеральной службы безопасности, осуществляющая в пределах своих полномочий решение задач по обеспечению безопасности РФ. В ведении ФСБ России находятся:

– разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации, индивидуальными предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность;

– деятельность по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);

– деятельность по распространению шифровальных (криптографических) средств;

– деятельность по техническому обслуживанию шифровальных (криптографических) средств;

– предоставление услуг в области шифрования информации;

– разработка, производство шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных систем, телекоммуникационных систем;

– деятельность по выдаче сертификатов ключей электронных цифровых подписей, регистрации владельцев электронных цифровых подписей, оказанию услуг, связанных с использованием электронных цифровых подписей, и подтверждению подлинности электронных цифровых подписей;

4. Служба внешней разведки РФ (СВР России) – основной орган внешней разведки РФ. Осуществляет допуск предприятий к проведению работ, связанных с использованием сведений, составляющих государственную тайну за рубежом.

5. Министерство обороны РФ (Минобороны России) – федеральный орган исполнительной власти (федеральное министерство), проводящий государственную политику и осуществляющий государственное управление в области обороны, а также координирующий деятельность федеральных министерств, иных федеральных органов исполнительной власти и органов исполнительной власти субъектов РФ по вопросам обороны.

6. Министерство внутренних дел РФ (МВД России) – федеральный орган исполнительной власти, осуществляющий функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере внутренних дел, а также по выработке государственной политики в сфере миграции. МВД осуществляет лицензирование негосударственной (частной) охранной деятельности, негосударственной (частной) сыскной деятельности.

7. Министерство чрезвычайных ситуаций РФ (МЧС России) осуществляет лицензирование производства работ по монтажу, ремонту и обслуживанию средств обеспечения пожарной безопасности зданий и сооружений;

Контроль за ввозом в Российскую Федерацию и вывозом из Российской Федерации специальных технических средств, предназначенных для негласного получения информации, не уполномоченными на осуществление оперативно-розыскной деятельности

юридическими лицами обеспечивает Федеральная служба безопасности РФ и Федеральная таможенная служба РФ.

Лицензирование деятельности по ввозу указанных средств осуществляет Министерство экономического развития и торговли РФ на основании решений Центра Федеральной службы безопасности РФ по лицензированию, сертификации и защите государственной тайны.

Концепция и доктрина информационной безопасности Российской Федерации

Основы государственной политики РФ в области информатизации и обеспечения информационной безопасности сформулированы в Концепции национальной безопасности РФ и Доктрине информационной безопасности РФ [11, 12].

Концепция национальной безопасности Российской Федерации отражает систему взглядов на обеспечение в Российской Федерации безопасности личности, общества и государства от внешних и внутренних угроз во всех сферах жизнедеятельности. В ней сформулировано понятие национальных интересов России в информационной сфере. В Концепции отмечается усиление угроз национальной безопасности Российской Федерации в информационной сфере.

В Доктрине подчеркивается, что обеспечение информационной безопасности Российской Федерации в сфере экономики играет ключевую роль в обеспечении национальной безопасности Российской Федерации.

Утверждается, что 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.

В качестве основных мер по обеспечению информационной безопасности Российской Федерации в сфере экономики Доктриной провозглашаются:

– 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.

2.3. Нормативно-правовые акты Российской Федерации [11]

Гражданский кодекс Российской Федерации

Определяет правовое положение участников гражданского оборота, основания возникновения и порядок осуществления права собственности и других вещных прав, исключительных прав на результаты интеллектуальной деятельности (интеллектуальной собственности), регулирует договорные и иные обязательства, а также другие имущественные и связанные с ними личные неимущественные отношения, основанные на равенстве, автономии воли и имущественной самостоятельности их участников.

Статья 128. Виды объектов гражданских прав.

«К объектам гражданских прав относятся вещи, включая деньги и ценные бумаги, иное имущество, в том числе имущественные права; работы и услуги; информация; результаты интеллектуальной деятельности, в том числе исключительные права на них (интеллектуальная собственность)…».

Статья 138. Интеллектуальная собственность.

В случаях и в порядке, установленных настоящим Кодексом и другими законами, признается исключительное право (интеллектуальная собственность) гражданина или юридического лица на результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации юридического лица, индивидуализации продукции, выполняемых работ или услуг (фирменное наименование, товарный знак, знак обслуживания и т.п.).

Исключительные права делятся на несколько групп, для которых установлен различный правовой режим использования и защиты. Традиционно выделяют две основные группы: «промышленная» и «художественная» собственность, к которым примыкают «смежные» права исполнителей, производителей фонограмм, организаций эфирного и кабельного вещания. Технический прогресс способствует расширению сферы исключительных прав, включению в нее новых видов нематериальных объектов (топологий ИМС, программ для ЭВМ, баз данных и др.).

Исключительные права на объекты промышленной собственности удостоверяются охранными документами: патентами на изобретения и промышленные образцы, свидетельствами на полезные модели, товарные знаки, наименования мест происхождения. Охрана исключительных прав на художественную собственность (произведения литературы, науки и искусства), а также объекты смежных прав и топологий ИМС не требует государственной регистрации или иного оформления. Основанием для защиты служит сам факт создания произведения в форме, доступной для восприятия другими лицами, что не препятствует их регистрации по желанию правообладателя. В частности, патентное ведомство ведет соответствующие регистрационные реестры.

Статья 139. Служебная и коммерческая тайна

Информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании и обладатель информации принимает меры к охране ее конфиденциальности. Сведения, которые не могут составлять служебную или коммерческую тайну, определяются законом и иными правовыми актами.

Статья не раскрывает содержание сведений, составляющих служебную или коммерческую тайну, и не приводит их перечень. Установлен только один общий признак, которым должна обладать охраняемая информация, – «коммерческая ценность», т.е. способность быть объектом рыночного оборота. Условием предоставления защиты служит принятие правообладателем всех необходимых мер для обеспечения ее конфиденциальности. При соблюдении этих требований под правила статьи подпадают, таким образом, любые знания, включая практический опыт специалистов, применяемые не только в производстве, но и в других областях хозяйственной деятельности: торговле, маркетинге, менеджменте, иных управленческих услугах. Признание тех или иных сведений конфиденциальными является прерогативой правообладателя. Исключения из этой общей нормы устанавливаются законом или иным правовым актом.

Существенным новшеством в гражданском кодексе является введение имущественной ответственности лица перед своим работодателем за разглашение служебной или коммерческой тайны, что предполагает необходимость включения соответствующих условий в трудовое соглашение. Вместе с тем, санкции за нарушение служебной тайны устанавливаются также нормами законов о соответствующих видах деятельности.

Статья 771. Конфиденциальность сведений, составляющих предмет договора

Если иное не предусмотрено договорами на выполнение научно-исследовательских работ, опытно-конструкторских и технологических работ, стороны обязаны обеспечить конфиденциальность сведений, касающихся предмета договора, хода его исполнения и полученных результатов. Объем сведений, признаваемых конфиденциальными, определяется в договоре.

Каждая из сторон обязуется публиковать полученные при выполнении работы сведения, признанные конфиденциальными, только с согласия другой стороны.

Состав и объем конфиденциальной информации определяется сторонами. В нее включаются сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них, а также любые другие сведения научного, технического, экономического, организационного характера, которые могут быть отнесены к коммерческой тайне.

Нарушением обязательств по обеспечению конфиденциальности признается не только разглашение и прямая передача подобных сведений одной из сторон другим заинтересованным пользователям без согласия партнера, но и непринятие мер к их охране, исключающих свободный доступ к сведениям и возможность их утечки. Правила статьи относятся как к сведениям, которыми стороны обладают на момент заключения договора, так и к полученным в процессе выполнения работ.

Статья 857. Банковская тайна

Банк гарантирует тайну банковского счета и банковского вклада, операций по счету и сведений о клиенте. Сведения, составляющие банковскую тайну, могут быть предоставлены только самим

клиентам или их представителям. Государственным органам и их должностным лицам такие сведения могут быть предоставлены исключительно в случаях и в порядке, предусмотренных законом. В случае разглашения банком сведений, составляющих банковскую тайну, клиент, права которого нарушены, вправе потребовать от банка возмещения причиненных убытков.

В состав банковской тайны входят сведения о счетах и вкладах, операциях по счетам и вкладам, о клиентах и корреспондентах, а также иная информация, устанавливаемая кредитной организацией, если это не противоречит федеральному закону («О банках и банковской деятельности»). Следовательно, кредитная организация не обязана хранить в тайне сведения о контрагентах своих клиентов, а также другую информацию, не имеющую непосредственного отношения к банковскому счету (кроме сведений о клиенте), если она не взяла на себя такие обязательства. Тайна распространяется, однако, на движение вкладов (размер, время и сумма поступления или изъятия, от кого и по каким основаниям поступают суммы и пр.).

Статья 946. Тайна страхования

Страховщик не вправе разглашать полученные им в результате своей профессиональной деятельности сведения о страхователе, застрахованном лице и выгодоприобретателе, состоянии их здоровья, а также об имущественном положении этих лиц. За нарушение тайны страхования страховщик в зависимости от рода нарушенных прав и характера нарушения несет ответственность в соответствии с правилами, предусмотренными статьей 139 или статьей 150 настоящего Кодекса.

Налоговый кодекс Российской Федерации

Кодекс устанавливает систему налогов и сборов, взимаемых в федеральный бюджет, а также общие принципы налогообложения и сборов в Российской Федерации, в том числе: виды налогов и сборов, взимаемых в Российской Федерации.

Статья 32 Кодекса определяет обязанность налоговых органов бесплатно информировать (в том числе в письменной форме) налогоплательщиков о действующих налогах и сборах, законода-

тельстве о налогах и сборах и принятых в соответствии с ним нормативных правовых актах, порядке исчисления и уплаты налогов и сборов, правах и обязанностях налогоплательщиков, полномочиях налоговых органов и их должностных лиц, а также предоставлять формы налоговой отчетности и разъяснять порядок их заполнения.

Статья 102 Кодекса устанавливает понятие налоговой тайны. Налоговую тайну составляют любые полученные налоговым органом, органами внутренних дел, органом государственного внебюджетного фонда и таможенным органом сведения о налогоплательщике, за исключением сведений: разглашенных налогоплательщиком самостоятельно или с его согласия; об идентификационном номере налогоплательщика; о нарушениях законодательства о налогах и сборах и мерах ответственности за эти нарушения; предоставляемых налоговым (таможенным) или правоохранительным органам других государств в соответствии с международными договорами (соглашениями), одной из сторон которых является Российская Федерация.

Трудовой кодекс Российской Федерации

Кодекс устанавливает государственные гарантии трудовых прав и свобод граждан, благоприятных условий труда, защиты прав и интересов работников и работодателей.

Глава 14 Кодекса регулирует вопросы, связанные с защитой персональных данных работника.

Семейный кодекс Российской Федерации

Семейное законодательство устанавливает условия и порядок вступления в брак, прекращения брака и признания его недействительным, регулирует личные неимущественные и имущественные отношения между членами семьи: супругами, родителями и детьми (усыновителями и усыновленными), а в случаях и в пределах, предусмотренных семейным законодательством, между другими родственниками и иными лицами, а также определяет формы и порядок устройства в семью детей, оставшихся без попечения родителей.

Уголовный кодекс Российской Федерации

Устанавливает основание и принципы уголовной ответственности, определяет, какие опасные для личности, общества или государства деяния признаются преступлениями, и устанавливает виды наказаний и иные меры уголовно-правового характера за совершение преступлений. В Уголовном кодексе Российской Федерации вопросам безопасности информации и интеллектуальной собственности посвящены следующие главы и статьи.

Глава 19. Преступления против конституционных прав и свобод человека и гражданина

Статья 137. Нарушение неприкосновенности частной жизни. Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации, если эти деяния совершены из корыстной или иной личной заинтересованности и причинили вред правам и законным интересам граждан.

Статья 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан. То же деяние, совершенное лицом с использованием своего служебного положения или специальных технических средств, предназначенных для негласного получения информации. Незаконные производство, сбыт или приобретение в целях сбыта специальных технических средств, предназначенных для негласного получения информации.

Статья 140. Отказ в предоставлении гражданину информации. Неправомерный отказ должностного лица в предоставлении собранных в установленном порядке документов и материалов, непосредственно затрагивающих права и свободы гражданина, либо предоставление гражданину неполной или заведомо ложной информации, если эти деяния причинили вред правам и законным интересам граждан.

Статья 146. Нарушение авторских и смежных прав. Присвоение авторства (плагиат), если это деяние причинило крупный

ущерб (свыше 100 МРОТ) автору или иному правообладателю. Незаконное использование объектов авторского права или смежных прав, а равно приобретение, хранение, перевозка контрафактных экземпляров произведений или фонограмм в целях сбыта, совершенные в крупном размере. Деяния, предусмотренные частью второй настоящей статьи, если они совершены: неодн кратно; группой лиц по предварительному сговору или организованной группой; в особо крупном размере (свыше 500 МРОТ); лицом с использованием своего служебного положения.

Статья 147. Нарушение изобретательских и патентных прав. Незаконное использование изобретения, полезной модели или промышленного образца, разглашение без согласия автора или заявителя сущности изобретения, полезной модели или промышленного образца до официальной публикации сведений о них, присвоение авторства или принуждение к соавторству, если эти деяния причинили крупный ущерб. Те же деяния, совершенные неоднократно, либо группой лиц по предварительному сговору или организованной группой.

Статья 180. Незаконное использование товарного знака. Незаконное использование чужого товарного знака, знака обслуживания, наименования места происхождения товара или сходных с ними обозначений для однородных товаров, если это деяние совершено неоднократно или причинило крупный ущерб. Незаконное использование предупредительной маркировки в отношении не зарегистрированного в Российской Федерации товарного знака или наименования места происхождения товара, если это деяние совершено неоднократно или причинило крупный ущерб. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой.

Статья 186. Изготовление или сбыт поддельных денег или ценных бумаг. Изготовление в целях сбыта или сбыт поддельных банковских билетов Центрального банка Российской Федерации, металлической монеты, государственных ценных бумаг или других ценных бумаг в валюте Российской Федерации либо иностранной валюты или ценных бумаг в иностранной валюте. Те же

деяния, совершенные в крупном размере либо лицом, ранее судимым за изготовление или сбыт поддельных денег или ценных бумаг. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные организованной группой.

Статья 187. Изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов. Изготовление в целях сбыта или сбыт поддельных кредитных либо расчетных карт, а также иных платежных документов, не являющихся ценными бумагами. Те же деяния, совершенные неоднократно или организованной группой.

Статья 189. Незаконный экспорт технологий, научно-технической информации и услуг, сырья, материалов и оборудования, которые могут использоваться при создании оружия массового поражения, вооружения и военной техники. Незаконный экспорт технологий, научно-технической информации и услуг, сырья, материалов и оборудования, которые могут быть использованы при создании оружия массового поражения, средств его доставки, вооружения и военной техники и в отношении которых установлен специальный экспортный контроль.

Глава 28. Преступления в сфере компьютерной информации.

Статья 272. Неправомерный доступ к компьютерной информации. Неправомерный доступ к охраняемой законом компьютерной информации, т.е. информации на машинном носителе, в ЭВМ, системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой, либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети.

Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование

либо распространение таких программ или машинных носителей с такими программами. Те же деяния, повлекшие по неосторожности тяжкие последствия.

Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред. То же деяние, повлекшее по неосторожности тяжкие последствия.

Законы Российской Федерации

Закон «Об авторском праве и смежных правах»

Регулирует отношения, возникающие в связи с созданием и использованием произведений науки, литературы и искусства (авторское право), фонограмм исполнений, постановок, передач организаций эфирного или кабельного вещания (смежные права). Закон развивает основные принципы правового регулирования авторских и смежных прав. Закон отвечает международным стандартам в этой области и позволил России присоединиться к ряду международных договоров.

Статья 1 Закона устанавливает общую сферу его действия и определяет наличие двух различных категорий прав: 1) авторских прав, которые возникают в отношении произведений науки, литературы и искусства, и 2) смежных прав, объектами которых являются фонограммы, исполнения, постановки, передачи эфирного и кабельного вещания.

Статья 5 Закона определяет, что произведение получает охрану, если оно отвечает хотя бы одному критерию – критерию гражданства автора или критерию места первого обнародования. При этом под гражданством автора имеется в виду то гражданство (подданство), которое автор имеет на момент создания произведения, а если произведение было обнародовано – то на момент обнародования произведения. Последующее изменение гражданства не меняет правового статуса произведения.

Статьи 6–8 Закона определяют объекты авторского права. К ним относятся произведения науки, литературы и искусства, являющиеся результатом творческой деятельности, независимо от назначения и достоинства произведения, а также от способа его выражения. При этом авторское право распространяется как на обнародованные произведения, так и на необнародованные произведения, существующие в какой-либо объективной форме: письменной, устной, звуко- или видеозаписи, изображения, объемно-пространственной или в других формах.

Конкретными объектами авторского права в том числе являются: литературные произведения (включая программы для ЭВМ); аудиовизуальные произведения (кино-, теле- и видеофильмы, слайдфильмы, диафильмы и другие кино- и телепроизведения); фотографические произведения и произведения, полученные способами, аналогичными фотографии; географические, геологические и другие карты, планы, эскизы и пластические произведения, относящиеся к географии, топографии и к другим наукам; сборники (энциклопедии, антологии, базы данных) и другие составные произведения, представляющие собой по подбору или расположению материалов результат творческого труда.

Охрана программ для ЭВМ распространяется на все виды программ для ЭВМ (в том числе на операционные системы), которые могут быть выражены на любом языке и в любой форме, включая исходный текст и объектный код.

Авторское право не распространяется на идеи, методы, процессы, системы, способы, концепции, принципы, открытия, факты (это объект патентного законодательства).

Статьи 9–16 Закона содержат основное положение законодательства об авторском праве: авторское право на произведение науки, литературы и искусства возникает в силу факта его создания. Для возникновения и осуществления авторского права не требуется регистрации произведения, иного специального оформления произведения или соблюдения каких-либо формальностей.

Обладатель исключительных авторских прав для оповещения о своих правах вправе использовать знак охраны авторского права, который помещается на каждом экземпляре произведения и состо-

ит из: латинской буквы «С» в окружности; имени (наименования) обладателя исключительных авторских прав; года первого опубликования произведения.

Авторское право действует в течение всей жизни автора и 70 лет после его смерти. Право авторства, право на имя и право на защиту репутации автора охраняются бессрочно (статья 27).

Допускается без согласия автора и без выплаты авторского вознаграждения воспроизведение правомерно обнародованного произведения исключительно в личных целях, за исключением случаев, предусмотренных статьей 26 настоящего Закона и применительно к программам для ЭВМ и базам данных.

Допускается без согласия автора и без выплаты авторского вознаграждения, но с обязательным указанием имени автора, произведение которого используется, и источника заимствования: цитирование в оригинале и в переводе в научных, исследовательских, полемических, критических и информационных целях из правомерно обнародованных произведений; использование правомерно обнародованных произведений и отрывков из них в качестве иллюстраций в изданиях, в радио- и телепередачах, звуко- и видеозаписях учебного характера; воспроизведение в газетах, передача в эфир или сообщение по кабелю для всеобщего сведения правомерно опубликованных в газетах или журналах статей по текущим экономическим, политическим, социальным и религиозным вопросам; воспроизведение в газетах, передача в эфир или сообщение по кабелю для всеобщего сведения публично произнесенных политических речей обращений, докладов и других аналогичных произведений; воспроизведение или сообщение для всеобщего сведения в обзорах текущих событий средствами фотографии, путем передачи в эфир или сообщения для всеобщего сведения по кабелю произведений, которые становятся увиденными или услышанными в ходе таких событий.

Статья 25 Закона определяет порядок свободного воспроизведения программ для ЭВМ и баз данных и декомпилирования программ для ЭВМ. Лицо, правомерно владеющее экземпляром программы для ЭВМ или базы данных, вправе без получения разрешения автора или иного обладателя исключительных прав на

использование произведения и без выплаты дополнительного вознаграждения:

– внести в программу для ЭВМ или базу данных изменения, осуществляемые исключительно в целях ее функционирования на технических средствах пользователя, осуществлять любые действия, связанные с функционированием программы для ЭВМ или базы данных в соответствии с ее назначением, в том числе запись и хранение в памяти ЭВМ (одной ЭВМ или одного пользователя сети), а также исправление явных ошибок, если иное не предусмотрено договором с автором;

– изготовить копию программы для ЭВМ или базы данных при условии, что эта копия предназначена только для архивных целей и для замены правомерно приобретенного экземпляра в случаях, когда оригинал программы для ЭВМ или базы данных утерян, уничтожен или стал непригоден для использования. При этом копия программы для ЭВМ или базы данных не может быть использована для иных целей и должна быть уничтожена в случае, если владение экземпляром этой программы для ЭВМ или базы данных перестает быть правомерным.

Лицо, правомерно владеющее экземпляром программы для ЭВМ, вправе без согласия автора или иного обладателя исключительных прав и без выплаты дополнительного вознаграждения воспроизвести и преобразовать объектный код в исходный текст (декомпилировать программу для ЭВМ) или поручить иным лицам осуществить эти действия, если они необходимы для достижения способности к взаимодействию независимо разработанной этим лицом программы для ЭВМ с другими программами, которые могут взаимодействовать с декомпилируемой программой, при соблюдении следующих условий:

– информация, необходимая для достижения способности к взаимодействию, ранее не была доступна этому лицу из других источников;

– указанные действия осуществляются в отношении только тех частей декомпилируемой программы для ЭВМ, которые необходимы для достижения способности к взаимодействию;

– информация, полученная в результате декомпилирования, может использоваться лишь для достижения способности к взаимодей-

ствию независимо разработанной программы для ЭВМ с другими программами, не может передаваться иным лицам, за исключением случаев, если это необходимо для достижения способности к взаимодействию независимо разработанной программы для ЭВМ с другими программами, а также не может использоваться для разработки программы для ЭВМ, по своему виду существенно схожей с декомпилируемой программой для ЭВМ, или для осуществления любого другого действия, нарушающего авторское право.

Статья 17 Закона определяет исчерпывающий перечень лицензируемых видов деятельности (всего 103 наименования). К защите информации среди них относятся: 1) деятельность по распространению шифровальных (криптографических) средств; 2) деятельность по техническому обслуживанию шифровальных (криптографических) средств; 3) предоставление услуг в области шифрования информации; 4) разработка, производство шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных систем, телекоммуникационных систем; 5) деятельность по выдаче сертификатов ключей электронных цифровых подписей, регистрации владельцев электронных цифровых подписей, оказанию услуг, связанных с использованием электронных цифровых подписей, и подтверждению подлинности электронных цифровых подписей; 6) деятельность по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя); 7) деятельность по разработке и (или) производству средств защиты конфиденциальной информации; 8) деятельность по технической защите конфиденциальной информации; 9) разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации, индивидуальными предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность; 10) деятельность по проведению экспертизы промышленной безопасности; 11) производство работ

по монтажу, ремонту и обслуживанию средств обеспечения пожарной безопасности зданий и сооружений; 12) деятельность по эксплуатации электрических сетей (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя); 13) негосударственная (частная) охранная деятельность; 14) негосударственная (частная) сыскная деятельность; 15) публичный показ аудиовизуальных произведений, если указанная деятельность осуществляется в кинозале; 16) воспроизведение (изготовление экземпляров) аудиовизуальных произведений и фонограмм на любых видах носителей; 17) аудиторская деятельность.

Федеральный закон «О техническом регулировании».

Регулирует отношения, возникающие при разработке, принятии, применении и исполнении обязательных требований к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнению работ или оказанию услуг; разработке, принятии, применении и исполнении на добровольной основе требований к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнению работ или оказанию услуг; оценке соответствия.

В качестве основных принципов технического регулирования в Законе приняты следующие: независимость органов по аккредитации и сертификации от изготовителей, продавцов, исполнителей и приобретателей; единая система и правила аккредитации; единство правил и методов исследований (испытаний) и измерений при проведении процедур обязательной оценки соответствия; единство применения требований технических регламентов независимо от видов или особенностей сделок; недопустимость совмещения одним органом полномочий на аккредитацию и сертификацию и др.

Федеральный закон «О коммерческой тайне»

Регулирует отношения, связанные с установлением, изменением и прекращением режима коммерческой тайны в отношении информации, составляющей секрет производства (ноу-хау).

В законе однозначно определен перечень сведений, которые не могут составлять коммерческую тайну:

1. Содержащихся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры.

2. Содержащиеся в документах, дающих право на осуществление предпринимательской деятельности.

3. О составе имущества государственного или муниципального унитарного предприятия и об использовании ими средств соответствующих бюджетов.

4. О загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и безопасности населения в целом.

5. О численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости, и о наличии свободных рабочих мест.

6. О задолженности работодателей по выплате заработной платы и по иным социальным выплатам.

7. О нарушении законодательства и фактах привлечения к ответственности за совершение этих нарушений.

8. Об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности.

9. О размерах и структуре доходов некоммерческих организаций, о размерах и составе их имущества, об их расходах, о численности и об оплате труда их работников, об использовании безвозмездного труда граждан в деятельности некоммерческой организации.

10.О перечне лиц, имеющих право действовать без доверенности от имени юридического лица.

11.Обязательность раскрытия которых или недопустимость ограничения доступа к которым установлена иными федеральными законами.

Закон однозначно определяет круг лиц и организаций, кому необходимо предоставлять информацию, составляющую коммерческую тайну.

Такую информацию по мотивированному требованию необходимо предоставлять органу государственной власти, иного государственного органа, органа местного самоуправления. Информация предоставляется безвозмездно. Само мотивированное требование должно быть подписано уполномоченным лицом и содержать указание цели и правового основания затребования информации, срок предоставления информации. Если обладатель информации, составляющей коммерческую тайну, отказывается ее предоставлять, то соответствующие органы вправе потребовать ее предоставление по суду.

На всех документах, предоставляемых по требованию соответствующих органов, должен быть нанесен гриф «коммерческая тайна» с указанием ее обладателя (для юридических лиц – полное наименование и место нахождения, для индивидуальных предпринимателей – фамилия, имя, отчество и место жительства).

Обладатель информации, имеющей гриф «коммерческая тайна», должен принимать меры по ее охране. Эти меры должны включать: 1) перечень информации, составляющей коммерческую тайну; 2) установление порядка доступа и порядка обращения с такой информацией, а также способы контроля за установленным порядком; 3) учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана; 4) регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров; 5) нанесение на материальные носители (документы), содержащие информацию, составляющую коммерческую тайну, грифа «коммерческая тайна» с указанием обладателя этой информации.

Кроме этих мер обладатель информации, составляющей коммерческую тайну, вправе применять при необходимости средства и методы технической защиты конфиденциальности этой информации, другие, не противоречащие законодательству меры.

Для осуществления принимаемых мер работодатель обязан:

– ознакомить под расписку работника, доступ которого к информации, составляющей коммерческую тайну, необходим для выполнения своих обязанностей, с перечнем такой информации;

– ознакомить под расписку работника с установленным работодателем режимом коммерческой тайны и с мерами ответственности за его нарушения;

– создать работнику необходимые условия для соблюдения им установленного работодателем режима коммерческой тайны.

Доступ работника к информации, составляющей коммерческую тайну, осуществляется с его согласия, если это не предусмотрено его трудовыми обязанностями.

Работник обязан выполнять установленный работодателем режим коммерческой тайны и не разглашать информацию, составляющую коммерческую тайну, обладателями которой являются работодатель и его контрагенты, и без их согласия не использовать эту информацию в личных целях;

Трудовым договором с руководителем организации должны предусматриваться его обязательства по обеспечению охраны конфиденциальности информации, обладателем которой являются организация и ее контрагенты, и ответственность за обеспечение охраны ее конфиденциальности.

При увольнении работник обязан передать работодателю все имеющиеся в его распоряжении материальные носители с информацией, содержащей коммерческую тайну.

Работник имеет право обжаловать в судебном порядке незаконное установление режима коммерческой тайны в отношении информации, к которой он получил доступ в связи с исполнением им трудовых обязанностей.

Работник, который в связи с исполнением трудовых обязанностей получил доступ к информации, составляющей коммерческую тайну, обладателями которой являются работодатель и его контр-

агенты, в случае умышленного или неосторожного разглашения этой информации при отсутствии в действиях такого работника состава преступления несет дисциплинарную ответственность в соответствии с законодательством Российской Федерации.

Лицо, которое использовало информацию, составляющую коммерческую тайну, и не имело достаточных оснований считать использование данной информации незаконным, в том числе получило доступ к ней в результате случайности или ошибки, не может в соответствии с настоящим Федеральным законом быть привлечено к ответственности.

Закон «О государственной тайне».

Определяет основные понятия, полномочия органов государственной власти и должностных лиц в области отнесения сведений к государственной тайне и их защиты.

Статья 12 Закона определяет реквизиты носителей сведений, составляющих государственную тайну. На носители сведений, составляющих государственную тайну, наносятся реквизиты, включающие следующие данные:

– о степени секретности содержащихся в носителе сведений со ссылкой на соответствующий пункт действующего в данном государственном органе, на данном предприятии, в данных учреждении и организации перечня сведений, подлежащих засекречиванию;

– об органе государственной власти, о предприятии, об учреждении, организации, осуществивших засекречивание носителя;

– о регистрационном номере;

– о дате или условии рассекречивания сведений либо о событии, после наступления которого сведения будут рассекречены.

При невозможности нанесения таких реквизитов на носитель сведений, составляющих государственную тайну, они указываются в сопроводительной документации на этот носитель.

Федеральный закон «О связи».

Устанавливает правовые основы деятельности в области связи на территории Российской Федерации и на находящихся под юрисдикцией Российской Федерации территориях, определяет

полномочия органов государственной власти в области связи, а также права и обязанности лиц, участвующих в указанной деятельности или пользующихся услугами связи.

Статья 63 Закона устанавливает понятие тайны связи. На территории Российской Федерации гарантируется тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи. Ограничение права на тайну переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи, допускается только в случаях, предусмотренных федеральными законами. Операторы связи обязаны обеспечить соблюдение тайны связи.

Федеральный закон «Об информации, информационных технологиях и о защите информации».

Регулирует отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации, применении информационных технологий, обеспечении защиты информации.

Статья 5, п. 2. Информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).

Статья 6 посвящена обладателю информации. Им может быть гражданин (физическое лицо), юридическое лицо, Российская Федерация, субъект Российской Федерации, муниципальное образование. Обладатель информации вправе:

1) разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;

2) использовать информацию, в том числе распространять ее, по своему усмотрению;

3) передавать информацию другим лицам по договору или на ином установленном законом основании;

4) защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного

использования иными лицами;

5) осуществлять иные действия с информацией или разрешать осуществление таких действий.

Статья 8, п. 4. Доступ не может быть ограничен к:

– нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления;

– информации о состоянии окружающей среды;

– информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну);

– информации, накапливаемой в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах (ИС), созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией;

– иной информации, недопустимость ограничения доступа к которой установлена федеральными законами.

Статья 13, п. 3. Права обладателя информации, содержащейся в базах данных информационной системы, подлежат охране независимо от авторских и иных прав на такие базы данных (статья об информационных системах). Важны и обязанности обладателя информации:

– соблюдать права и законные интересы иных лиц;

– принимать меры по защите информации;

– ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

Статья 11 касается документированной информации.

Здесь важно отметить, что электронное сообщение, подписанное электронной цифровой подписью или иным аналогом собственноручной подписи, признается электронным документом, равнозначным документу, подписанному собственноручной подписью, в случаях, если федеральными законами или иными нормативными правовыми актами не устанавливается или не подразуме-

вается требование о составлении такого документа на бумажном носителе.

Статья 12 о государственном регулировании в сфере применения ИТ гласит в частности, что оно предусматривает:

– регулирование отношений, связанных с поиском, получением, передачей, производством и распространением информации с применением информационных технологий (информатизации);

– развитие информационных систем различного назначения для обеспечения граждан (физических лиц), организаций, государственных органов и органов местного самоуправления информацией, а также обеспечение взаимодействия таких систем;

– создание условий для эффективного использования в Российской Федерации информационно-телекоммуникационных сетей, в том числе сети Интернет и иных подобных информационно-телекоммуникационных сетей.

Федеральный закон «О персональных данных».

Регулирует отношения, связанные с обработкой персональных данных. Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии.

Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают:

– определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

– разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

– проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

– установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

– обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

– учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

– учет лиц, допущенных к работе с персональными данными в информационной системе;

– контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

– разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

– описание системы защиты персональных данных.

Основные подзаконные акты в области защиты информации

Количество подзаконных актов федерального уровня и уровня субъектов федерации, изданных во исполнение рассмотренных выше законов, выпущено более сотни. Кроме того, в них постоянно вносятся изменения и уточнения. Ниже представлено краткое

содержание только основных из таких подзаконных актов, определяющих либо основы деятельности в различных сферах, связанных с защитой информации, либо наиболее часто требующиеся на практике. Все такие акты разделены на три категории: указы Президента Российской Федерации, Постановления Правительства Российской Федерации и ведомственные документы. Более подробно о них можно посмотреть в учебнике [13].

Указы Президента Российской Федерации

№ 2334 «О дополнительных гарантиях прав граждан на информацию».

№ 334 «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации».

№ 21 «О мерах по упорядочению разработки, производства, реализации, приобретения в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы, а также использования специальных технических средств, предназначенных для негласного получения информации».

№ 116 «О мерах по противодействию терроризму».

№ 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

Постановления Правительства Российской Федерации

№ 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». Данным Постановлением утверждено Положение о лицензировании деятельности, связанной с работой со сведениями, составляющими государственную тайну. Государственными органами, ответственными за организацию и проведение специальных

экспертиз предприятий, являются Федеральная служба безопасности Российской Федерации, Государственная техническая комиссия при Президенте Российской Федерации, Служба внешней разведки Российской Федерации, другие министерства и ведомства Российской Федерации, руководители которых наделены полномочиями по отнесению к государственной тайне сведений в отношении подведомственных им предприятий.

№ 608 «О сертификации средств защиты информации». Данным Постановлением утверждено Положение о сертификации средств защиты информации, которое устанавливает порядок сертификации средств защиты информации в Российской Федерации и ее учреждениях за рубежом. Средствами защиты информации являются технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

№ 214 «Об утверждении Положения о ввозе в Российскую Федерацию и вывозе из Российской Федерации специальных технических средств, предназначенных для негласного получения информации, и списка видов специальных технических средств, предназначенных для негласного получения информации, ввоз и вывоз которых подлежат лицензированию».

№ 135 «О лицензировании отдельных видов деятельности». Устанавливает перечень федеральных органов исполнительной власти, осуществляющих лицензирование в определенных областях, а также виды деятельности, лицензируемые органами исполнительной власти субъектов Российской Федерации.

№ 290 «О лицензировании деятельности по технической защите конфиденциальной информации». Положение определяет порядок лицензирования деятельности юридических и физических лиц по технической защите конфиденциальной информации.

3. БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СИСТЕМ

Несмотря на наличие технических каналов утечки информации, прежде всего нужно позаботиться об обеспечении безопасности на

уровне компьютерных систем [14]. К примеру, бессмысленно обеспечивать контроль над излучением элементов ЭВМ, если компьютер может использовать любой желающий.

3.1. Модели безопасности компьютерных систем

Создание безопасности компьютерных систем сводится к разработке набора правил, определяющих множество допустимых действий в системе (политики безопасности). Системы, функционирующие в соответствии со строго определенным набором формализованных правил и реализующие какую-либо политику безопасности, называются моделями безопасности. К наиболее эффективным и используемым в настоящее время моделям безопасности относятся модели систем: 1) дискреционного; 2) мандатного; 3) ролевого разграничения доступа [14, 15]. При описании моделей безопасности используют понятия субъект и объект. Под субъектом понимается индивид или группа индивидов, объект – защищаемая информация, чаще всего представленная в виде файлов, реже – в виде настроек различных систем и пр.

Модель систем дискреционного разграничения доступа

Данная модель характеризуется разграничением доступа между поименованными субъектами и объектами. Для каждого субъекта должно быть задано явное и недвусмысленное перечисление допустимых операций (читать, писать и т. д.) над конкретным объектом. Субъект с определенным правом доступа к объекту может передать это право любому другому субъекту.

Возможны, по меньшей мере, два подхода к построению дискреционного управления доступом [15]: 1) каждый объект системы имеет привязанного к нему субъекта (владельца), который устанавливает права доступа к данному объекту; 2) система имеет одного выделенного субъекта – суперпользователя, который имеет право устанавливать права владения для всех остальных субъектов системы.

Возможны и смешанные варианты построения, когда одновременно в системе присутствуют как владельцы, устанавливающие

права доступа к своим объектам, так и суперпользователь, имеющий возможность изменения прав для любого объекта и/или изменения его владельца. Именно такой смешанный вариант реализован в большинстве операционных систем (UNIX или Windows семейства NT), он же в основном используется и в Интернете, в частности, в социальных сетях. Если в социальной сети пользователь загрузил какую-либо информацию (фото, документы и пр.), то что бы он с ней ни делал, как бы ни скрывал, существует суперпользователь (администратор социальной сети), который может этой информацией воспользоваться. При этом удаление пользователем информации ничего не изменит, поскольку удаляемая информация, как правило, по умолчанию сохраняется в резервной базе данных, доступ к которой также имеет суперпользователь.

Модель систем мандатного разграничения доступа

В данной модели каждому субъекту и объекту присваиваются классификационные метки, отражающие место данного субъекта (объекта) в соответствующей иерархии. Посредством этих меток субъектам и объектам назначаются классификационные уровни (уровни уязвимости, категории секретности и т. п.), являющиеся комбинациями иерархических и неиерархических категорий. Для доступа субъекта к объекту первый должен предоставить системе классификационные метки этого объекта. При санкционированном занесении в список пользователей нового субъекта осуществляется присвоение ему классификационных меток. Внешние классификационные метки (субъектов, объектов) должны точно соответствовать внутренним меткам. Мандатный принцип контроля доступа должен быть применен ко всем объектам при явном и скрытом доступе со стороны любого из субъектов. При организации мандатного принципа контроля возможны следующие подходы [15]:

– субъект может читать объект, только если иерархическая классификация субъекта не меньше, чем иерархическая классификация объекта, и неиерархические категории субъекта включают в себя все иерархические категории объекта;

– субъект осуществляет запись в объект, только если классификационный уровень субъекта не больше, чем классификационный

уровень объекта, и все иерархические категории субъекта включаются в неиерархические категории объекта.

При реализации мандатных правил создается диспетчер доступа – средство, осуществляющее перехват всех обращений субъектов к объектам, а также разграничение доступа в соответствии с заданным принципом разграничения доступа. При этом решение о санкционированности запроса на доступ должно приниматься только при одновременном его разрешении и дискреционными, и мандатными правилами разграничения доступа.

Модель систем ролевого разграничения доступа

Ролевое разграничение доступа представляет собой развитие политики дискреционного разграничения доступа, при этом права доступа субъектов системы на объекты группируются с учетом специфики их применения, образуя роли – совокупность прав доступа на объекты компьютерной системы. Задание ролей позволяет определить более четкие и понятные для пользователей компьютерной системы правила разграничения доступа. Такой подход часто используется в системах, для пользователей которых четко определен круг их должностных полномочий и обязанностей.

Ролевое разграничение доступа отличается от дискреционного разграничения доступа также тем, что его правила определяют порядок предоставления прав доступа субъектам компьютерной системы не статически, а в зависимости от сессии его работы и от имеющихся (или отсутствующих) у него ролей в каждый момент времени.

3.2. Угрозы безопасности компьютерных систем и сетей

Любая программа, наносящая какой-либо вред компьютеру, на котором она запускается, или другим компьютерам в сети называется вредоносной программой. Наиболее распространенными типами вредоносных программ являются вирусы, черви и трояны. Чуть менее распространенными – условно опасные программы, хакерские утилиты и злые шутки.

Компьютерный вирус – это программа, способная создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети и/или файлы, системные области компьютера и прочие выполняемые объекты. При этом дубликаты сохраняют способность к дальнейшему распространению. Жизненный цикл вируса состоит из:

1. Проникновения на чужой компьютер. Проникать может как через мобильные носители, так и сетевые соединения. В отличие от червей, вирусы не используют сетевые ресурсы – заражение вирусом возможно, только если пользователь сам каким-либо образом его активировал.

2. Активации. По типу активации вирусы делятся на: **загрузочные вирусы** (заражают загрузочные сектора жестких дисков и мобильных носителей) и **файловые вирусы** (заражают файлы. Отдельно по типу среды обитания в этой группе также выделяют). В свою очередь файловые вирусы делятся на:

- **классические файловые вирусы** – они различными способами внедряются в исполняемые файлы, создают файлы-двойники, свои копии в различных каталогах жесткого диска или используют особенности организации файловой системы;
- **макровирусы**, написанные на макросах какого-либо приложения (например, Microsoft Word);
- **скрипт-вирусы**, написанные в виде скриптов для определенной командной оболочки – например, bat-файлы для DOS или JS-скрипты для Windows Scripting Host (WSH).

3. Поиска объектов заражения. Вирусы жестко привязаны к операционной системе или программной оболочке, для которой каждый конкретный вирус был написан. Это означает, что вирус для Microsoft Windows не будет работать и заражать файлы на компьютере с другой установленной операционной системой, например Unix. Точно также макровирус для Microsoft Word 2003 скорее всего не будет работать в приложении Microsoft Excel 97.

4. Подготовки копий. Для маскировки вирусов могут использоваться такие технологии как: шифрование – в этом случае вирус состоит из двух частей: сам вирус и шифратор, метаморфизм – при применении этого метода вирусные копии создаются путем заме-

ны некоторых команд на аналогичные, перестановки местами частей кода, вставки между ними дополнительных, обычно ничего не делающих команд. Соответственно в зависимости от используемых методов вирусы можно делить на *шифрованные*, *метаморфные* и *полиморфные*, использующие комбинацию двух типов маскировки.

5. Внедрения копий. Внедрение копий осуществляется при определенных событиях или действиях пользователя, например, 26 числа каждого четного месяца или при загрузке браузера или при перезагрузке компьютера и пр.

Червь – это вредоносная программа, распространяющаяся по сетевым каналам и способная к самостоятельному преодолению систем защиты компьютерных сетей, а также к созданию и дальнейшему распространению своих копий, не обязательно совпадающих с оригиналом.

Жизненный цикл червей аналогичен жизненному циклу вирусов. В зависимости от способа проникновения черви делятся на:

– *сетевые черви* – используют для распространения локальные сети и Интернет;

– *почтовые черви* – распространяются с помощью почтовых программ;

– *IM-черви* используют системы мгновенного обмена сообщениями;

– *IRC-черви* распространяются по каналам IRC;

– *P2P-черви* – при помощи пиринговых файлообменных сетей.

По методу активации все черви можно разделить на две большие группы – на тех, которые требуют активного участия пользователя (для чего, как правило, используются обманные методы) и тех, кто его не требуют (используются ошибки в настройке или бреши в системе безопасности операционной системы). В последнее время наметилась тенденция к совмещению этих двух технологий – такие черви наиболее опасны и часто вызывают глобальные эпидемии.

Трояны или программы класса троянский конь, в отличие от вирусов и червей, не обязаны уметь размножаться. Это программы, написанные только с одной целью – нанести ущерб целевому

компьютеру путем выполнения несанкционированных пользователем действий: кражи, порчи или удаления конфиденциальных данных, нарушения работоспособности компьютера или использования его ресурсов в неблаговидных целях.

Жизненный цикл троянов:

1. Проникновение в систему. Проникать в систему могут самостоятельно или в кооперации с вирусом или червем. В первом случае обычно используется маскировка, когда троян выдает себя за полезное приложение, которое пользователь самостоятельно копирует себе на диск.

2. Активация. По активации троян похож на червя – либо требует активных действий от пользователя или же через уязвимости в программном обеспечении самостоятельно заражает систему.

3. Выполнение вредоносных действий. По типу вредоносной нагрузки трояны классифицируются на:

– *клавиатурные шпионы* – постоянно находясь в оперативной памяти, записывают все данные, поступающие от клавиатуры с целью последующей их передачи своему автору;

– *похитители паролей* – предназначены для кражи паролей путем поиска на зараженном компьютере специальных файлов, которые их содержат;

– *утилиты скрытого удаленного управления* – это трояны, которые обеспечивают несанкционированный удаленный контроль над инфицированным компьютером (возможность скрыто загружать, отсылать, запускать или уничтожать файлы).

– *анонимные SMTP-сервера и прокси-сервера* – такие трояны на зараженном компьютере организовывают несанкционированную отправку электронной почты, что часто используется для рассылки спама.

– *утилиты дозвона* – в скрытом от пользователя режиме инициируют подключение к платным сервисам Интернет.

– *модификаторы настроек браузера* – меняют стартовую страницу в браузере, страницу поиска или еще какие-либо настройки, открывают дополнительные окна, имитируют нажатия на рекламные баннеры и т. п.

– *логические бомбы* – характеризуются способностью при сраба-

тывании заложенных в них условий (в конкретный день, время суток, определенное действие пользователя или команды извне) выполнять какое-либо действие, например, удаление файлов.

Условно опасные программы – программы, о которых нельзя однозначно сказать, что они вредоносны. Такие программы обычно становятся опасными только при определенных условиях или действиях пользователя. К ним относятся:

– *Riskware* – вполне легальные программы, которые сами по себе не опасны, но обладают функционалом, позволяющим злоумышленнику использовать их с вредоносными целями. К riskware относятся обычные утилиты удаленного управления, которыми часто пользуются администраторы крупных сетей, программы для загрузки файлов из Интернет, утилиты восстановления забытых паролей и другие.

– *Adware* (рекламные утилиты) – условно-бесплатные программы, которые в качестве платы за свое использование демонстрируют пользователю рекламу, чаще всего в виде графических баннеров. После официальной оплаты и регистрации обычно показ рекламы заканчивается и программы начинают работать в обычном режиме. После регистрации такие программы могут автоматически не удаляться и продолжать свою работу в скрытом режиме.

– *Pornware* – утилиты, так или иначе связанные с показом информации порнографического характера. Эти программы самостоятельно дозваниваются до порнографических телефонных служб, загружают из Интернет порнографические материалы или утилиты, предлагающие услуги по поиску и показу такой информации. Обычно это делается с целью насильственного показа рекламы платных порнографических сайтов или служб.

Хакерские утилиты – к этому виду программ относятся программы скрытия кода зараженных файлов от антивирусной проверки (шифровальщики файлов), автоматизации создания сетевых червей, компьютерных вирусов и троянских программ (конструкторы вирусов), наборы программ, которые используют хакеры для скрытого взятия под контроль взломанной системы и другие подобные утилиты. То есть такие специфические программы, которые обычно используют только хакеры.

Злые шутки – программы, которые намеренно вводят пользователя в заблуждение путем показа уведомлений, например, уведомления о форматировании диска или обнаружении вирусов, хотя на самом деле ничего не происходит. Текст таких сообщений целиком и полностью отражает фантазию автора.

3.3. Классификация программно-технических методов и средств защиты информации

Хорошая защита информации обходится дорого, плохая же защита никому не нужна (принцип сплошной защиты), ибо наличие в ней лишь одной уязвимости означает полную бесполезность всей защиты в целом.

Для того чтобы создать на предприятии (организации и пр.) безопасную информационную систему, необходимо, прежде всего, обеспечить работоспособность всех классов программно-технических методов и средств защиты информации [16]: 1) средства защиты от несанкционированного доступа (средства авторизации, мандатное управление доступом, избирательное управление доступом, управление доступом на основе ролей, аудит); 2) системы анализа и моделирования информационных потоков; 3) системы мониторинга сетей (системы обнаружения и предотвращения вторжений, системы предотвращения утечек конфиденциальной информации); 4) анализаторы протоколов; 5) антивирусные средства; 6) межсетевые экраны; 7) криптографические средства (шифрование, цифровая подпись); 8) системы резервного копирования; 9) системы бесперебойного питания (источники бесперебойного питания, резервирование нагрузки, генераторы напряжения); 10) системы аутентификации (пароль, ключ доступа (физический или электронный), сертификат, биометрия); 11) средства предотвращения взлома корпусов и краж оборудования; 12) средства контроля доступа в помещение; 13) инструментальные средства анализа систем защиты (мониторинговый программный продукт).

3.4. Безопасность на уровне операционных систем

Несомненно, для защиты компьютерных систем необходима и антивирусная защита, и усиленные меры идентификации и аутентификации пользователей, но в первую очередь необходимо все же обеспечить защиту с помощью встроенных средств операционной системы (ОС). Рассмотрим настройку средств безопасности одной из распространенных ОС Windows XP.

Настройка средств безопасности осуществляется в соответствии с политикой безопасности – шаблоном, по которому можно выбирать и конфигурировать различные типы механизмов защиты, поддерживаемых операционной системой или ее приложениями, в соответствии с некоторой моделью разграничения доступа (раздел 3.1). В политике безопасности предписано каждого пользователя системы классифицировать по группам, что осуществляется посредством создания *учетных записей пользователей* – записей, содержащих все сведения, определяющие пользователей в ОС. К этим сведениям относятся: имя пользователя и пароль, требуемые для входа пользователя в систему, имена групп, членом которых пользователь является, а также права и разрешения, которые он имеет при работе в системе и доступе к ее ресурсам.

Существует как минимум пять групп пользователей: 1) администраторы (имеют полный доступ на управление компьютером), 2) операторы архива (могут архивировать и восстанавливать файлы на компьютере, независимо от всех разрешений, которыми защищены эти файлы, не могут изменять параметры безопасности); 3) опытные пользователи (могут создавать учетные записи и группы пользователей, изменять и удалять созданные ими учетные записи и группы пользователей, создавать локальные группы и удалять пользователей из локальных групп, которые они создали, удалять пользователей из групп «Опытные пользователи», «Пользователи» и «Гости»); 4) пользователи (могут выполнять наиболее распространенные задачи, например, запуск приложений, использование локальных и сетевых принтеров и т. д.); 5) гости (для пользователей, не имеющих собственных учетных записей на компьютере).

При добавлении учетной записи пользователя его, как правило,

относят к некоторой группе, тем самым пользователю предоставляются все разрешения и права, назначенные этой группе. На одном компьютере может быть создано неограниченное число учетных записей. Для добавления на компьютер нового пользователя или изменения учетной записи существующего пользователя необходимо войти в систему с учетной записью «Администратор» (или члена группы «Администраторы»), зайти в Пуск → Панель управления → Администрирование → Управление компьютером → Служебные программы → Локальные пользователи и группы → Пользователи и в окне со списком пользователей осуществить нужную операцию.

Средствами реализации учетных записей пользователей обеспечивается защита от несанкционированного доступа к информации злоумышленника при его непосредственном контакте с системой. Но существуют угрозы, связанные с несанкционированным доступом к информации по сети. Такой доступ, как правило, осуществляется посредством: вирусов, кейлогеров (программа, считывающая нажатие клавиш) и радминов (программа, предназначенная для удаленного администрирования, но при этом может использоваться для доступа к скрытой информации).

Важно помнить, что как бы хорошо ни была защищена ОС, в ней периодически находятся уязвимые места, которыми может воспользоваться злоумышленник. Но разработчики ОС довольно часто выпускают «заплатки» – исправления выявленных недостатков ОС, которые устанавливаются на систему пользователя путем обновления ОС. В ОС Windows существует средство автоматического обновления, которое позволяет в автоматическом режиме устанавливать самые «свежие» обновления. Для включения автоматического обновления необходимо перейти к Пуск → Панель управления → Центр обеспечения безопасности Windows → Автоматическое обновление и выбрать пункт «Автоматически (рекомендуется)», выбрать день недели и время выполнения обновления.

Для обеспечения защиты от вредоносных программ используется специальное антивирусное программное обеспечение: Dr. Web, Kaspersky, McAfee, AVZ, Agnitum, Avast, Avira, BitDefender, Emsisoft, Eset, F-Secure, Panda, Sophos, Symantec и др.

Каждый из них обладает своими достоинствами и недостатками, выбор конкретного антивирусного программного обеспечения остается за пользователем. Если опыта работы с антивирусными программами у пользователя недостаточно, рекомендуется выбор осуществить исходя из рейтинга антивирусных программ, например, здесь [17]. Существует ряд ресурсов (virustotal.com, virscan.org, urlvoid.com, vms.drweb.com/online и пр.), на которых можно выполнить проверку файлов или других ресурсов на наличие вредоносных программ с помощью нескольких антивирусных программ.

В стратегии защиты от несанкционированного доступа к информационным ресурсам компьютерной сети особое внимание уделяется обеспечению безопасности ее границ. Целостность периметра компьютерной сети обеспечивается использованием тех или иных базовых технологий межсетевого экранирования в точке подключения защищаемой сети к внешней неконтролируемой сети. В качестве внешней сети чаще всего выступает Интернет, точки доступа – сервер сети. Систему разграничения компьютерных сетей с различными политиками безопасности, реализующую правила информационного обмена между ними, называют межсетевым экраном (встречаются также термины фаервол или брандмауэр).

Межсетевой экран повышает безопасность объектов внутренней сети за счет игнорирования несанкционированных запросов из внешней среды [18]. Кроме того, экранирование позволяет контролировать информационные потоки, исходящие во внешнюю среду, что способствует поддержанию во внутренней области режима конфиденциальности. Кроме функций разграничения доступа, брандмауэр может обеспечивать выполнение дополнительных функций безопасности: аутентификацию, контроль целостности, фильтрацию содержимого, обнаружение атак, регистрацию событий. Если говорить просто, брандмауэр нужен для того, чтобы «не пропустить» вредоносные программы, тогда как антивирусные системы служат, прежде всего, для выявления уже имеющихся вредоносных программ [19].

В ОС Windows существует встроенный брандмауэр, который можно включить в Пуск → Панель управления → Центр обеспе-

чения безопасности Windows → Брандмауэр Windows. Данный брандмауэр можно использовать, если на компьютере нет особо важной информации (паролей кредитных карт и пр.), в противном случае все же рекомендуется установить брандмауэр внешних производителей, например [20–22]: COMODO, Zone Alarm, Agnitum Outpost.

Очень часто вредоносные программы выдаются под видом полезных программ. В этом случае брандмауэры оказываются бесполезными, поскольку пользователь (с правами администратора), устанавливая потенциально опасную программу, игнорирует всякие предупреждения межсетевого экрана. Заметим, что устанавливаемые программы проверяет также антивирусное программное обеспечение, но и оно может оказаться бесполезным. Как показывает практика, антивирусам свойственно «пропускать» некоторые вредоносные программы, особенно рекламные вставки и программы-шпионы (программы, которые скрытным образом устанавливаются на компьютер с целью сбора информации о конфигурации компьютера, пользователе, пользовательской активности без согласия последнего). Поэтому для обеспечения комплексной защиты просто необходима программа, специально предназначенная для выявления рекламных вставок и программ-шпионов (программа-антишпион).

К наиболее известным программам-антишпионам относятся: Spybot Search&Destroy, Ad-Aware, Spyware Terminator, SyperAntiSpyware (программы можно найти на soft.oszone.net и biblprog.org.ua). Антишпионы не конфликтуют с антивирусами, поэтому их можно и нужно устанавливать вместе, но при этом конфликтуют между собой, поэтому необходимо остановиться на какой-то конкретной программе-антишпионе [18]. Выполнять сканирование системы как программой-антишпионом, так и антивирусным программным обеспечением рекомендуется не реже одного раза в месяц.

Для работы любой вредоносной программы требуется её запустить, как правило, это делает сам пользователь (например, по невнимательности), или программа может быть прописана в автозагрузку ОС, тогда она будет автоматически запускаться при

загрузке ОС. Как правило, для работы вредоносных программ используется второй подход. Поэтому следует периодически проверять и настраивать автозагрузку, для этого на вкладке *Автозагрузка* утилиты *Настройка системы* (Пуск → Выполнить…, ввести msconfig, нажать ОК), необходимо убрать все подозрительные программы, а также программы, в автозапуске которых нет необходимости (рис. 6).

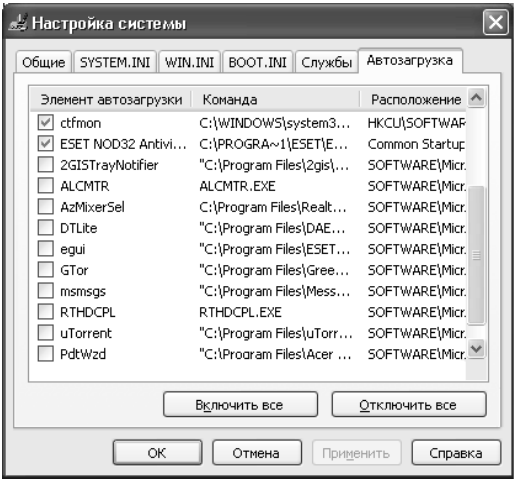

Рис. 6. Утилита *Настройка системы*

В любом случае, загружается ли вредоносная программа с помощью автозагрузки или каким-либо другим способом, при её работе она интерпретируется ОС как процесс и, соответственно, отображается во вкладке *Процессы* утилиты *Диспетчер задач Windows* (рис. 7), которая вызывается нажатием сочетания клавиш Alt+Ctrl+Del. С ее помощью можно в режиме реального времени отслеживать выполняющиеся приложения и запущенные процессы, оценивать загруженность системных ресурсов компьютера и сети. Используя Диспетчер задач, можно остановить выполнение любого выполняющегося процесса, в том числе вредоносную программу, но необходимо четко понимать и уметь отличать легальные процессы (например, системные или запущенные программы) от подозрительных, для чего можно поискать информацию о выполняемом

процессе в Интернете (twirpx.com/file/40641/, http://wiki.compowiki.info/ProcessyWin dows и пр.).

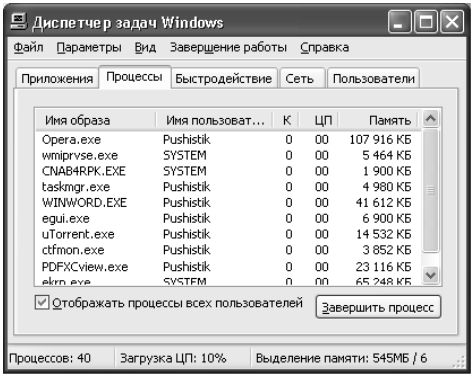

Рис. 7. Диспетчер задач Windows

Вся информация о конфигурации системы, настройках приложений и пр. в ОС Windows хранится в одном месте – в реестре ОС (Пуск → Выполнить…, ввести regedit, нажать OK), поэтому большинство вредоносных программ в той или иной степени пытаются заполучить доступ к реестру. Одно из потенциально опасных мест в реестре – это ключ Userinit из раздела HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\Current Version\Winlogon. По умолчанию этот ключ содержит запись C:\WINDOWS\system32\userinit.exe (рис. 8). Если в указанном ключе содержатся дополнительные записи, то это могут быть вредоносные программы, и их необходимо удалить.

Существует множество других потенциально опасных мест в реестре, выявить которые без средств автоматизации очень сложно. Для выявления в реестре опасных записей, ошибок реестра и пр. используются такие программы как: Spybot Search&Destroy, Ad-Aware, Reg Organizer и др. Программа Reg Organizer помимо очистки реестра также может выполнять очистку и исправление ошибок на жестком диске [18]. Данную операцию необходимо выполнять, поскольку излишняя «замусоренность» диска и наличие ошибок могут приводить к возникновению потенциально опасных ситуаций (периодическому зависанию компьютера, появлению со-

общений об ошибках и пр.).

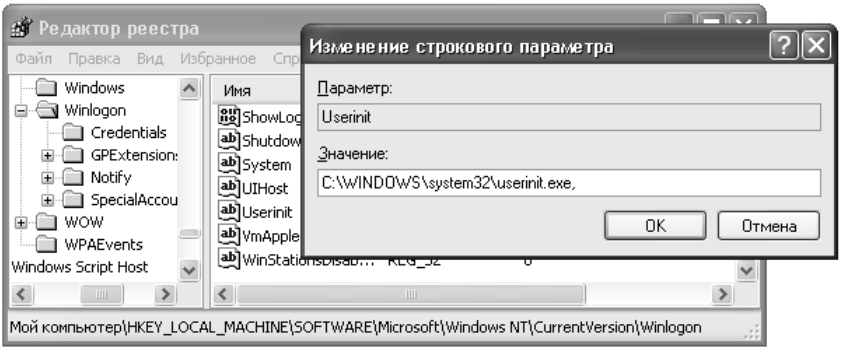

Рис. 8. Редактор реестра

В случае сбоя системы (вследствие проникновения вредоносной программы или других действий) можно восстановить её работоспособность, загрузив работоспособную версию реестра, но для этого необходимо заблаговременно создать рабочую копию реестра путем его экспорта (меню Файл\Экспорт…) в редакторе реестра. Создавать рабочую копию реестра рекомендуется перед каждой проверкой реестра и не реже одного раза в месяц. Для устранения сбоя системы также можно использовать процедуру *Восстановление системы* (Пуск → Все программы → Стандартные → Служебные → Восстановление системы), которая должна быть включена до момента сбоя. Для настройки процедуры восстановления необходимо воспользоваться вкладкой *Восстановление системы* в свойствах системы (Пуск → Панель управления → Система).

Вредоносные программы, как правило, проникают в систему двумя способами: через внешние носители информации (флешнакопители, CD, DVD и пр.) и через сеть Интернет. Первый способ заражения в основном осуществляется за счет автозагрузки носителя (используются файлы autorun.inf и autorun.ini на внешнем носителе), поэтому для обеспечения безопасности автозагрузку внешних носителей необходимо отключить (Пуск → Выполнить… → gpedit.msc → Конфигурация компьютера → Административные шаблоны → Система → Отключить автозапуск →

Включен → на всех дисководах), и перед каждым использованием носителя информации сканировать его антивирусным программным обеспечением.

Вероятность проникновения вредоносных программ в систему из сети Интернет во многом зависит от выбора браузера (Internet Explorer, Mozilla Firefox, Opera, Google Chrome, Apple Safari и пр.), его настроек и расширений (дополнений, плагинов). Статистика используемости браузеров разнится, но в основном лидируют браузеры Mozilla Firefox и Opera.

Все расширения браузера Mozilla Firefox касательно безопасности можно найти здесь [23], браузера Opera здесь [24]. Наиболее важные расширения в области безопасности для Mozilla Firefox: *Adblock Plus* – блокирует ненужную рекламу, *NoScript* – блокирует исполнение JavaScript, апплетов Java, Flash и других потенциально опасных компонент HTML-страниц до тех пор, пока пользователь не разрешит их исполнение, *WOT* – определяет степень опасности ресурсов (репутацию) в сети Internet; для Opera: *Opera AdBlock* – блокирует ненужную рекламу, *VirusTotal* – интегрирует браузер с известным одноимённым веб-сервисом, способным провести проверку просматриваемого в данный момент сайта (а также любого файла с компьютера пользователя) на наличие каких-либо угроз, *WOT* – аналогичен одноименному плагину для Mozilla Firefox.

Одним из часто встречаемых типов вредоносных программ являются макровирусы – вредоносные программы, написанные на макросах (используемых для автоматического выполнения операций в некоторых прикладных программах обработки данных: текстовых редакторах, электронных таблицах и т. д.). Макровирусы наиболее распространены в приложениях Microsoft Office: World, Excel и пр. Для борьбы с макровирусами в Microsoft Office необходимо в настройках (Сервис → Параметры → Безопасность → Защита от макросов) установить уровень безопасности не ниже высокого (высокий или очень высокий). Данная настройка позволяет избежать автоматического запуска (например, при открытии файла приложения) потенциально опасного макроса.

Количество вредоносных программ с каждым годом растет, они становятся все более изощренными. Уже сейчас для обеспечения

безопасности недостаточно только антивирусных программ, необходима комплексная организация мер безопасности, включающая установку межсетевых экранов, создание и настройку учетных записей пользователей, настройку автозагрузки и многое другое. Меры обеспечения безопасности, описанные выше, являются основными и должны быть использованы каждым, кто хочет обезопасить себя от компьютерных угроз.

Одним из основных компонентов подсистемы безопасности ОС Windows является Диспетчер учетных записей [25]. Он обеспечивает взаимодействие других компонентов подсистемы безопасности Windows с базой данных учетных записей (Security Account Database, SAM), в которой хранятся имена и пароли пользователей. С помощью SAM Диспетчер производит идентификацию и аутентификацию пользователей при интерактивном входе в систему или при доступе по сети.

База данных SAM представляет собой один из кустов системного реестра Windows. Этот куст находится в ветви HKEY_LOCAL_MACHINE\SAM. Как и остальные кусты реестра, он хранится в отдельном файле в папке \winnt\system32\config. Из этого файла при загрузке ОС строится та часть реестра, которую будет контролировать Диспетчер учетных записей. Основная часть информации в SAM хранится в двоичном виде. Доступ на чтение и запись к данному разделу реестра для обычных пользователей и групп Windows запрещен.

Пароли в Windows хранятся в SAM не в открытом текстовом виде, а обрабатываются специальной процедурой – хешированием. В отличие от шифрования хеширование является необратимой операцией, поэтому, даже если известна хешированная форма пароля, восстановить его в исходном текстовом виде с помощью алгоритма нельзя ни пользователю, ни администратору.

Для совместимости с другими клиентами и серверами фирмы Microsoft (Windows for Workgroups, Lan Manager) в SAM хранится также хешированное и зашифрованное представление пароля пользователя в стандарте системы Lan Manager. Этот пароль гораздо менее устойчив к взлому [26], чем пароль Windows.

Доступ к файлу \winnt\System32\Config\SAM для обычных

пользовательских программ заблокирован. Тем не менее, с помощью программы NTBACKUP любой обладатель права Back up files and directories может скопировать его в составе реестра на резервный магнитный носитель. Резервную копию реестра также позволяет создать программа REGBACK из Windows Resource Kit. Кроме того, взломщик может попытаться переписать копию файла SAM из папки \winnt\System32\Config или сжатую архивную копию (файл SAM._ из папки \winnt\Repair). Чтобы прочитать добытую физическую копию файла SAM, ее можно загрузить в реестр Windows на любом другом доступном компьютере (командой Load Hive в программе RegEdit32).

Для защиты SAM в основном используются следующие методы:

Ограничение физического доступа к основным серверам сети. Основные рекомендации: не применять попеременную (dual-boot) загрузку; форматировать все разделы под файловую систему NTFS; установить пароль BIOS на запуск компьютера, отключив при этом возможность загрузки со сменных магнитных носителей; тщательно планировать формирование групп пользователей, имеющих право интерактивного доступа к серверам и контроллерам доменов.

Защита SAM от несанкционированного доступа. Доступ пользователей ко всем копиям базы данных SAM необходимо строго ограничивать. Ограничения должны касаться даже тех пользователей, которые имеют права администратора, и членов групп Backup Operators и Server Operators. Необходимо запретить запуск на сервере непроверенных программ и просмотр полученных через Internet сомнительных Web-страниц.

Резервный файл SAM.SAV создается при установке или при обновлении ОС и может быть после этого сразу удален. Папку \winnt\Repair надо средствами файловой системы NTFS закрыть для доступа всех пользователей, включая администратора. Разрешать доступ к этой папке следует только на время работы программы RDISK, которая создает в ней новые архивные копии кустов реестра Windows NT. Принять меры к физическому сокрытию архивных копий и загрузочных дискет.

Отмена кэширования паролей на компьютерах домена. По

умолчанию имена и хешированные пароли последних десяти пользователей домена, регистрировавшихся ранее на данном компьютере, сохраняются в его локальном реестре. Локальный администратор данного компьютера в состоянии извлечь эту информацию из реестра, и, если среди десяти пользователей обнаружится администратор домена, его пароль может быть взломан. Поэтому администратором домена кэширование информации на локальном компьютере должно быть отменено.

Дополнительное шифрование хешированных паролей в SAM. Для этого можно применить программу SYSKEY фирмы Microsoft, которую могут запустить только члены локальной группы Administrators данного компьютера. Уникальный 128-битный ключ для дополнительного шифрования паролей, созданный программой SYSKEY, после ее работы автоматически сохраняется в реестре для последующего применения. Чтобы усилить защищенность паролей, этот ключ перед записью в реестр зашифровывается еще раз другим (тоже 128-битным ключом). Последний называется системным ключом или ключом запуска. Программа SYSKEY предлагает два способа его хранения: в реестре данного компьютера, на отдельной дискете, либо вообще его не хранить. В последнем случае он будет вычисляться каждый раз при запуске системы на основе пароля, набираемого на клавиатуре системным администратором. Пароль указывается в диалоговом окне программы SYSKEY, которое будет выводиться перед появлением приглашения Press Ctrl-Alt-Del to log on.

Защита учетных записей от подбора. Простейший способ защитить пароли пользователей от вскрытия методом подбора вариантов – включить блокировку учетных записей после определенного количества неудачных попыток входа в систему. Такая блокировка существенно уменьшает возможность подбора пароля той или иной учетной записи пользователя как при интерактивной регистрации, так и при сетевом доступе. Исключением здесь является учетная запись Administrator. Программа PASSPROP из Windows NT Resource Kit позволяет установить специальный режим блокировки для учетной записи Administrator. Для этого ее надо запустить с ключом /ADMINLOCKOUT. Если после этого произойдет

блокировка учетной записи, администратор сможет войти в систему интерактивно на любом из контроллеров домена, но любые попытки регистрации этого пользователя по сети будут отвергнуты.

Чтобы дополнительно защитить от подбора пароль администратора, рекомендуется изменить имя в его учетной записи. После этого можно создать нового пользователя с именем Administrator, предоставив ему минимальные права. Переименованную учетную запись в дальнейшем лучше вообще не применять, а для системных администраторов можно создать отдельные учетные записи и поместить их в локальную группу Administrators или в глобальную группу Domain Admins. Можно также лишить пользователей этих групп права доступа к компьютеру по сети, особенно если это контроллер домена.

Выбор паролей и их фильтрация. Для повышения устойчивости паролей пользователей к взлому рекомендуется принять ряд мер. Во-первых, с помощью программы User Manager for Domains необходимо установить минимальную длину пароля (например, не меньше 6 символов). Во-вторых, следует установить режим устаревания паролей, чтобы пользователи их периодически обновляли, чем выше риск атаки, тем короче должен быть срок устаревания. Принудить пользователей вводить устойчивые к взлому пароли поможет уже упоминавшаяся выше программа PASSPROP. После ее запуска с ключом /COMPLEX «правильными» будут признаваться только пароли, сочетающие или буквы в разном регистре, или буквы с цифрами, или буквы со специальными символами, или цифры с символами.

Для защиты особо ценной информации (файл паролей и пр.) применяются дополнительные меры предосторожности:

1. Отдельным пользователям или группе пользователей запретить выполнять некоторые действия (читать, изменять, записывать и пр.) с закрытой информацией. Для этого нужно открыть произвольную папку в Проводнике, выбрать Сервис → Свойства папки, перейти на вкладку Вид и убрать выделение напротив строки *Использовать простой общий доступ к файлам (рекомендуется)*, после чего в диалоговом окне свойств любой папки появляется вкладка *Безопасность*, которая и предназначена для создания пароля.

2. Для доступа на определенный диск или папку, в которой находится информация, с помощью специальных программ (Folder Crypt, Folder Password Protect, extCryptor, File and Folder Privacy, FFGuard, DAFFTIN Cryppie и др.) наложить пароль. Функция защиты информации паролем имеется не только в специальных программах, но и во многих стандартных архиваторах, например, в архиваторе WinRar. Для того, чтобы наложить на файл архива пароль, необходимо в настройках архивации на вкладке *Дополнительно* нажать *Установить пароль*. Пароль должен быть сложным – в него должны быть включены буквы, цифры и спецсимволы («.№;%:?*() +/, и т. д.), но при этом он должен быть запоминающимся.

3. Хранить информацию на специальных флэш-устройствах, используемых для защиты конфиденциальной информации. Среди таких устройств можно выделить: флэш-накопители Cruzer Enterprise от SanDisk, на которых используется одновременно и шифрование и парольная защита (на программном уровне); флэш-накопители Elecom с системой идентификации паролем PASS, использующие парольную защиту (на программном уровне) и позволяющие владельцу определять, на каких компьютерах разрешено просматривать данные; флэш-накопители Samurai, на которых также используется парольная защита (на аппаратном уровне) и активирующаяся при попытке несанкционированного доступа система уничтожения записанной информации. Устанавливаемый на флэш-накопители пароль должен быть сложным (см. п. 2).

4. АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аудит информационной безопасности – независимая оценка текущего состояния системы информационной безопасности, устанавливающая уровень ее соответствия определенным критериям, и предоставление результатов в виде рекомендаций.

Целью аудита информационной безопасности является проведение экспертизы соответствия системы информационной безопасности определенным требованиям и оценки системы управления безопасностью.

Аудитом информационной безопасности занимаются специальные организации аудиторов в области информационной безопасности, например, подразделения государственной технической комиссии при Президенте РФ или независимые негосударственные организации.

В области аудита безопасности информации выделяют следующие основные направления деятельности:

1. Аттестация объектов информатизации по требованиям безопасности информации, к которой относятся: а) аттестация автоматизированных систем, средств связи, обработки и передачи информации; б) аттестация помещений, предназначенных для ведения конфиденциальных переговоров; в) аттестация технических средств, установленных в выделенных помещениях.

2. Контроль защищенности информации ограниченного доступа – выявление технических каналов утечки информации и способов несанкционированного доступа к ней, а также контроль эффективности применяемых средств защиты информации.

3. Специальные исследования технических средств (персональные ЭВМ, средства связи и обработки информации, локальные вычислительные системы и пр.) на наличие побочных электромагнитных излучений и наводок.

В зависимости от направления деятельности в области аудита информационной безопасности выделяют активный аудит, экспертный аудит и аудит на соответствие стандартам.

Активный аудит представляет собой исследование состояния защищенности информационной системы (ИС) с точки зрения злоумышленника, обладающего высокой квалификацией в области информационных технологий [9]. Суть активного аудита состоит в том, что бы, используя специальное программное обеспечение (в том числе системы анализа защищенности [8]) и специальные методы, смоделировать как можно большее количество сетевых атак, которые может выполнить злоумышленник, и осуществить сбор информации обо всех уязвимостях системы, степени их критичности и методах устранения, сведений о широкодоступной информации (доступной любому потенциальному нарушителю). По окончании активного аудита выдаются рекомендации по модернизации системы

сетевой защиты, которые позволяют устранить опасные уязвимости.

Активный аудит делится на «внешний» активный аудит и «внутренний» активный аудит. При «внешнем» активном аудите специалисты моделируют действия «внешнего» злоумышленника: определение доступных из внешних сетей IP-адресов; сканирование данных адресов с целью определения работающих сервисов и служб, определение назначения отсканированных хостов; определение версий сервисов и служб сканируемых хостов; изучение маршрутов прохождения трафика к хостам и др. «внутренний» активный аудит по составу работ аналогичен «внешнему», однако при его проведении с помощью специальных программных средств моделируются действия «внутреннего» злоумышленника (невнимательного рабочего, уволенного сотрудника и пр.).

Экспертный аудит представляет сравнение состояния информационной безопасности с «идеальным» описанием, которое базируется на требованиях, предъявленных руководством в процессе проведения аудита и на описании «идеальной» системы безопасности, основанной на аккумулированном мировом и частном опыте. Экспертный аудит состоит: 1) из сбора исходных данных об информационной системе, об её функциях и особенностях, используемых технологиях автоматизированной обработки и передачи данных (с учетом ближайших перспектив развития); 2) сбора информации об имеющихся организационно-распорядительных документах по обеспечению информационной безопасности и их анализа; 3) определения точек ответственности систем, устройств и серверов информационной системы; 4) формирования перечня подсистем каждого подразделения компании с категорированием критичной информации и схемами информационных потоков. Выделяют три этапа экспертного аудита:

1. Анализ проекта информационной системы, топологии сети и технологии обработки информации, в ходе которого выявляются, например, такие недостатки существующей топологии сети, которые снижают уровень защищенности информационной системы.

2. Анализ информационных потоков организации. На данном этапе определяются типы информационных потоков информационной системы организации и составляется их диаграмма, где для

каждого информационного потока указывается его ценность (в том числе, ценность передаваемой информации) и используемые методы обеспечения безопасности, отражающие уровень защищенности информационного потока.

3. Анализ организационно-распорядительных документов, таких как политика безопасности, план защиты и различного рода инструкции, которые оцениваются на предмет достаточности и непротиворечивости декларируемым целям и мерам информационной безопасности.

Аудит на соответствие стандартам – это деятельность, при которой информационная безопасность сравнивается с неким абстрактным описанием, приводимым в стандартах. К основным стандартам, на соответствие которым проводится аудит, относятся: 1) руководящие документы Гостехкомиссии РФ: «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», «Специальные требования и рекомендации по технической защите конфиденциальной информации» (СТР-К), «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий» (ГОСТ Р ИСО/МЭК 15408-2002 или «Общие критерии»), «Защита информации. Испытание программных средств на наличие компьютерных вирусов. Типовое руководство» (ГОСТ Р 51188–98), «Информационные технологии. Практические правила управления информационной безопасностью» (ГОСТ Р ИСО/МЭК 17799) и др.; 2) зарубежные и международные стандарты: «Информационные технологии – Технологии безопасности – Практические правила менеджмента информационной безопасности» (ISO/IEC 17799:2005), «Информационные технологии – Технологии безопасности – Практические правила менеджмента информационной безопасности» (ISO/IEC 27002), Руководство по менеджменту рисков ИБ (ISO/IEC 27005), WebTrust и др.

Проведение аудита разделяется на следующие этапы: 1) сбор исходных данных об информационной системе предприятия, функциях и особенностях, об используемых технологиях автоматизированной обработки и передачи данных (с учетом бли-

жайших перспектив развития); 2) сбор информации об имеющихся организационно-распорядительных документах по обеспечению информационной безопасности и их анализ; 3) выявление критичных информационных потоков и свойств циркулирующей информации в информационной системе с точки зрения обеспечения ее конфиденциальности, целостности и доступности; 4) формирование перечня подсистем каждого подразделения предприятия с категорированием критичной информации и схемами информационных потоков; 5) подготовка предложений по совершенствованию системы обеспечения информационной безопасности.

Официальный отчет, подготовленный в результате проведения аудита на соответствие стандарту, включает: 1) степень соответствия проверяемой информационной системы выбранным стандартам; 2) степень соответствия собственным внутренним требованиям компании в области информационной безопасности; 3) количество и категории полученных несоответствий и замечаний; 4) рекомендации по построению или модификации системы обеспечения информационной безопасности, позволяющие привести её в соответствие с рассматриваемым стандартом; 5) подробная ссылка на основные документы заказчика, включая политику безопасности, описания процедур обеспечения информационной безопасности, дополнительные обязательные и необязательные стандарты и нормы, применяемые к данной компании.

Аудит объединяет несколько различных форм работ, основанных на единых принципах и методологии, но различающихся по содержанию конечной цели и объемам проводимых испытаний. Форма проводимого обследования (аудита) зависит, в первую очередь, от жизненного цикла обследуемого проекта (табл. 2).

Результатом аттестации является официальный документ – Аттестат соответствия, выдаваемый уполномоченным (аккредитованным в Системе аттестации «Системы сертификации по требованиям безопасности информации РОСС RU.0001.01БИ00») органом по аттестации и подтверждающий, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации.

Таблица 2

Соответствие видов аудита периодам жизненного цикла обследуемого объекта [27], 1 – первичный, 2 – технический, 3 – аттестация, 4 – сюрвей, 5 – контрольный

Периоды жизненного цикла обследуемого объекта	Виды обследования (аудита)				
	1	2	3	4	5
Принятие решения о создании корпоративной ИС	x				
Определение требований к создаваемой корпоративной ИС		x			
Проектирование и ввод в эксплуатацию корпоративной ИС			x	x	
Штатная эксплуатация средств корпоративной ИС					x
Ремонт (плановый и внеплановый), устранение неисправностей			x		x
Нештатные ситуации, приводящие к ущербу				x	x
Устранение последствий нештатных ситуаций					x
Принятие решений о модернизации корпоративной ИС	x	x	x		
Модернизация корпоративной ИС				x	
Эксплуатация модернизированной ИС					x
Вывод из эксплуатации и замена корпоративной ИС					x

Сюрвей – специфическая форма аудита, который проводится на этапе подготовки к страхованию информационных рисков, либо после наступления страхового случая с целью проведения оценки возможности нанесения субъектам материального и иного случайного или преднамеренного ущерба в результате нарушения безопасности информации (оценка информационных рисков) и подтверждения соответствия принятого комплекса мер и средств противодействия угрозам установленным страховщиком в страховом полисе требованиям, либо проверки условий наступления страхового случая, оговоренного в страховом полисе. Особенностью такого аудита является то, что он проводится на обследуемом

объекте в интересах третьего лица – страховой компании. Результатом является специальный документ – Сюрвей-рипорт, который представляется страховщику и содержит материалы по оценке риска, предшествующие заключению договора страхования. На разных этапах обследования используются различные методы: технические, аналитические, экспертные, расчетные. При этом, результаты, полученные одними методами, могут дублироваться (дополняться) результатами, полученными другими методами. Совокупность всех применяемых методов позволяет дать объективную оценку состояния обеспечения безопасности информации на обследуемом объекте.

Основными группами методов при обследовании являются:

– Экспертно-аналитические методы предусматривают проверку соответствия обследуемого объекта установленным требованиям по безопасности информации на основании экспертной оценки полноты и достаточности представленных документов по обеспечению необходимых мер защиты информации, а также соответствия реальных условий эксплуатации оборудования предъявляемым требованиям по размещению, монтажу и эксплуатации технических и программных средств.

– Экспертно-инструментальные методы предполагают проведение проверки функций или комплекса функций защиты информации с помощью специального инструментария (тестирующих средств) и средств мониторинга, а также путем пробного запуска средств защиты информации и наблюдения реакции за их выполнением. В процессе испытаний технических и программных средств используются тестирующие средства, принятые в установленном порядке.

– Моделирование действий злоумышленника («дружественный взлом» системы защиты информации) применяются после анализа результатов, полученных в ходе использования первых двух групп методов, они необходимы как для контроля данных результатов. Этим методом подтверждаются также реальные возможности потенциальных злоумышленников (как внутренних, легально допущенных к работе с тем или иным уровнем привилегий в ИС, так и внешних – в случае подключения ИС к глобальным информацион-

ным сетям). Кроме того, подобные методы могут использоваться для получения дополнительной исходной информации об объекте, которую не удалось получить другими методами.

Важным моментом является то, что применение методов моделирования действий злоумышленника ограниченно. При использовании данных методов необходимо учитывать, что при осуществлении тестовой атаки, используемое в ИС оборудование может быть выведено из строя, информационные ресурсы утрачены или искажены.

5. УПРАВЛЕНИЕ РИСКАМИ

В случае, когда обрабатываемые данные или используемые информационные системы являются нестандартными, использование стандартов безопасности не представляется возможным. В этом случае для обеспечения безопасности необходимо организовать работу по управлению рисками потери информации.

С количественной точки зрения размер риска является функцией вероятности реализации определенной угрозы (использующей некоторые уязвимости), а также величины возможного ущерба. Суть работы по управлению рисками состоит в том, чтобы оценить их размер, выработать эффективные и экономичные меры по уменьшению этого размера и затем убедиться, что риски заключены в приемлемые рамки.

Управление рисками включает в себя два вида деятельности, которые чередуются циклически: 1) (пере)оценку (измерение) рисков; 2) выбор эффективных и экономичных защитных средств (нейтрализация рисков).

По отношению к выявленным рискам возможны следующие действия: 1) ликвидация риска (например, за счет устранения причины); 2) уменьшение риска (например, за счет использования дополнительных защитных средств); 3) принятие риска (и выработка плана действия в соответствующих условиях); 4) переадресация риска (например, путем заключения страхового соглашения).

Процесс управления рисками можно подразделить на следующие этапы: 1) выбор анализируемых объектов и уровня детализации их

рассмотрения; 2) выбор методологии оценки рисков; 3) идентификация активов; 4) анализ угроз и их последствий, определение уязвимостей в защите; 5) оценка рисков; 6) выбор защитных мер; 7) реализация и проверка выбранных мер; 8) оценка остаточного риска. Этапы 6 и 7 относятся к выбору защитных средств (нейтрализации рисков), остальные – к оценке рисков.

Управление рисками, как и любую другую деятельность в области информационной безопасности, необходимо интегрировать в жизненный цикл информационной системы. В таком случае эффект оказывается наибольшим, а затраты – минимальными.

На этапе инициации известные риски следует учесть при выработке требований к системе вообще и средствам безопасности в частности. На этапе закупки (разработки) выявленные риски способны помочь при выборе архитектурных решений, играющих ключевую роль в обеспечении безопасности. На этапе установки выявленные риски следует учитывать при конфигурировании, тестировании и проверке ранее сформулированных требований, а полный цикл управления рисками должен предшествовать внедрению системы в эксплуатацию. На этапе эксплуатации управление рисками должно сопровождать все существенные изменения в системе. При выведении системы из эксплуатации управление рисками помогает убедиться в том, что миграция данных происходит безопасным образом.

Управление рисками – процесс повторяющийся. Все этапы управления рисков связаны между собой, по завершении любого из них может выявиться необходимость возврата к предыдущему.

Первый шаг в анализе угроз – их идентификация. Анализируемые виды угроз следует выбрать из соображений здравого смысла, но в пределах выбранных видов провести максимально полное рассмотрение. Целесообразно выявлять не только сами угрозы, но и источники их возникновения – это поможет в выборе дополнительных средств защиты. Например, нелегальный вход в систему может стать следствием воспроизведения начального диалога, подбора пароля или подключения к сети неавторизованного оборудования.

После идентификации угрозы необходимо оценить вероятность

ее осуществления. Допустимо использовать при этом трехбалльную шкалу (низкая (1), средняя (2) и высокая (3) вероятность). Кроме вероятности осуществления, важен размер потенциального ущерба. Например, пожары бывают нечасто, но ущерб от каждого из них, как правило, велик. Тяжесть ущерба также можно оценить по трехбалльной шкале.

Оценивая вероятность осуществления угроз, целесообразно исходить не только из среднестатистических данных, но учитывать также специфику конкретных информационных систем. Если в подвале дома, занимаемого организацией, располагается сауна, а сам дом имеет деревянные перекрытия, то вероятность пожара, к сожалению, оказывается существенно выше средней.

После того, как накоплены исходные данные и оценена степень неопределенности, можно переходить к обработке информации, то есть собственно к оценке рисков. Вполне допустимо применить такой простой метод, как умножение вероятности осуществления угрозы на предполагаемый ущерб.

Если какие-либо риски оказались недопустимо высокими, необходимо их нейтрализовать, реализовав дополнительные защитные меры. Как правило, для ликвидации или нейтрализации уязвимости, сделавшей реальной опасную угрозу, существует несколько механизмов безопасности, отличающихся эффективностью и стоимостью. Например, если велика вероятность нелегального входа в систему, можно приказать пользователям выбирать длинные пароли и пр.

Оценивая стоимость защитных мер, приходится, разумеется, учитывать не только прямые расходы на закупку оборудования и/или программ, но и расходы на внедрение новинки и, в частности, на обучение и переподготовку персонала. Эту стоимость также можно выразить по трехбалльной шкале и затем сопоставить ее с разностью между вычисленным и приемлемым риском.

6. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЧЕЛОВЕКА [28]

В наш цифровой век жизнь многих людей отражается в различного рода информационных системах: фиксируются телефонные звонки, сообщения в социальных сетях и форумах, оплата счетов, покупки, поездки, собирается информация о приобретаемой недвижимости и пр. Только видеокамеры, например, устанавливаются в магазинах, жилых массивах, автомобильных парковках, офисных зданиях, домов, и занимают лишь небольшую толику средств наблюдения и сбора информации. Конечно, использование видеокамер снижает уровень преступности, но они же фиксируют также события личной жизни.

Угрозы неприкосновенности частной жизни

В последнее время принимают опасные масштабы следующие угрозы неприкосновенности частной жизни граждан:

1. Потеря контроля над процессом. Правительства многих стран и деловые круги, делая ставку на компьютерные технологии, заменили миллиарды бумажных папок электронными системами обработки данных. В результате возник мир, в котором ничтожная ошибка, сделанная чиновником, может повлечь разрушительные последствия для чьей-то личной жизни.

2. Систематическая фиксация всего происходящего. Мы находимся на пороге нового мира, в котором каждое сделанное нами приобретение, каждое посещенное нами место, каждое сказанное или прочитанное нами слово будет записываться для последующего анализа.

3. Тотальное прослушивание окружающего мира. Серьезную угрозу свободе представляет постоянный мониторинг общественных мест при помощи микрофонов, видеокамер, систем спутникового наблюдения и других устройств дистанционного контроля в сочетании с новейшими достижениями в области обработки информации. Вскоре в больших городах большинство людей просто не сможет найти себе места, чтобы уединиться.

4. Нецелевое использование медицинских записей. Медицинские записи традиционно считаются видом конфиденциальной информации. Обязательство хранить медицинскую тайну – одно из ключевых требований к медицинскому работнику, но обеспечение конфиденциальности пациента может идти вразрез с интересами индустрии медицинского страхования.

5. Бесконтрольная реклама. Рекламные буклеты в почте, рекламные сообщения по e-mail, реклама по факсу и телефону представляют собой широкомасштабную и бесконтрольную рекламную компанию. Маркетологи всё чаще используют персональную информацию для навязчивых рекламных предложений, которые трудно отделить от подборок новостей, личных писем и другой некоммерческой корреспонденции.

6. Персональная информация как товар. Идентифицирующая личность информации: имя, профессия, хобби и другие мелочи делающие человека уникальным – всё это превратилось в ценный объект владения, которым обладают бизнесмены, постоянно использующие его для получения прибыли и захвата рынка.

7. Микроуправление интеллектуальной собственностью. Корпорации очень бдительно следят за правомерностью использования своей интеллектуальной собственности. Но с пиратством чрезвычайно сложно бороться, когда технология позволяет любому потребителю стать распространителем интеллектуальной собственности. Чтобы предотвратить её хищение, правообладатели задействуют самые изощренные методы слежки за клиентами. А поскольку технология уже существует, маловероятно, что её применение будет ограничено лишь защитой от пиратства.

Кодекс справедливого использования информации

В 1972 году в США Элиот Ричардсон (бывший в то время советником президента Никсона по вопросам здравоохранения, образования и социального обеспечения) создал комиссию по изучению влияния компьютерных технологий на приватность. После нескольких лет слушаний в конгрессе США комиссия пришла к выводу, что повод для тревоги имеется. В результате отчета Ричардсона, был разработан билль о правах в компьютерную эпо-

ху, получивший название «Кодекс справедливого использования информации». Этот кодекс остается одним из самых значимых трудов в области обеспечения приватности при использовании компьютеров на сегодняшний день. Кодекс базируется на пяти принципах:

1. Не должно существовать систем, накапливающих персональную информацию, сам факт существования которых является секретом.
2. Каждый человек должен иметь возможность контролировать, какая информация о нем храниться в системе и каким образом она используется.
3. Каждый человек должен иметь возможность не допустить использования собранной о нем информации для одной конкретной цели, с другой неоговоренной целью.
4. Каждый человек должен иметь возможность корректировать информацию о себе.
5. Каждая организация, занимающаяся созданием, сопровождением, использованием или распространением массивов информации, содержащих персональные данные, должна обеспечить использование этих данных только в целях, для которых они собраны, и принять меры против их использования не по назначению.

Влияние средств массовой информации на человека

Массовая информация – предназначенные для неограниченного круга лиц печатные, аудио-, аудиовизуальные и иные сообщения и материалы.

Средство массовой информации (СМИ) – периодическое печатное издание, радио-, теле-, видеопрограмма, кинохроника и иная форма периодического распространения массовой информации.

Как правило, СМИ разделяют на два типа: печатные и электронные.

К электронным относятся СМИ, использующие электронные каналы передачи – радио и телевидение. Электронные СМИ более оперативны, в них существует явление «прямого эфира» – моментальной передачи информации о событиях. Недостаток электронных СМИ – привязанность ко времени эфира. Из-за ограниченного

количества каналов радио и телевидение обычно более строго регулируются государством, чем печатные СМИ.

К печатным относят те СМИ, которые производят при помощи печатного станка – газеты, журналы. У печатных СМИ свои преимущества: к газетной или журнальной статье можно вернуться спустя день или столетие. В отличие от электронных СМИ, печатные требуют грамотности от тех, кому они адресованы, но текст дает больший простор для воображения, нежели визуальный ряд или звук.

Методы влияния СМИ на человеческое сознание

СМИ через воздействие на общество в целом воздействуют на каждого человека в отдельности, формируя определенные одинаковые эмоции и действия. Таким образом, благодаря СМИ формируется общественное мнение.

Общественное мнение – состояние массового сознания, заключающее в себе скрытое или явное отношение разных социальных общностей к проблемам и событиям действительности.

В практике СМИ сегодня широко используются методы подсознательного воздействия, когда отношение общества к тем или иным явлениям окружающего мира формируется с помощью стереотипных представлений.

Пресса стандартизует сообщение, т.е. особым образом «подводит» информацию под стереотип, всеобщее мнение. Человек должен воспринимать сообщение без усилий и безоговорочно, без внутренней борьбы и критического анализа. С помощью стереотипов легко манипулировать сознанием человека. СМИ приучают мыслить человека стереотипами и снижают интеллектуальный уровень сообщения так, что превратились в инструмент оглупления.

Задача прессы – создать прочное, устойчивое отношение к данному явлению благодаря использованию внушения. Один из приемов внушения – создание информационного резонанса.

Информационный (общественный) резонанс – одновременное повышенное искусственное привлечение средствами СМИ общественного внимания к тому или иному социальному или политическому событию, сопряженное с замалчиванием других событий, имеющих равную информационную значимость.

Будучи искусственно созданным, информационный резонанс выдаётся за проявление коллективной воли общества и используется заинтересованными лицами для формирования «нужного» общественного мнения, внедрения в общественное сознание под видом объективной информации желательного для указанных лиц содержания. Информационный резонанс может использоваться теми или иными группами для давления на судебные органы, исполнительную и законодательную власть, правительство, общественные организации и политические партии.

Можно выделить следующие методы влияния СМИ на человеческое сознание:

1. Метод создания образа врага. Нередко используется для создания негативной общественной реакции, в основе механизма заложена идея дегуманизации – враг представляется непохожим на вас: он другой национальности, вида, умственных особенностей, кроме того, он агрессивен и ничего хорошего от него ждать нельзя.
2. Метод семантического манипулирования. Предполагает тщательный отбор и специальную компоновку понятий, вызывающих либо позитивные, либо негативные ассоциации.
3. Метод отвлечения. Общество не терпит информационного вакуума, поэтому чтобы отвлечь аудиторию от одной информации, необходимо переключить её внимание на другую, поданную в максимально сенсационном виде. Цель новой информации – создать отвлекающую альтернативу и снизить актуальность предыдущей информации.
4. Метод дробления (фрагментации). По мере усложнения телевизионных программ длительность каждого их элемента сокращается во времени, т.е. информация, поданная мелкими порциями, не позволяет ею эффективно воспользоваться.
5. Немедленность подачи информации. Чувство срочности создает ощущение чрезвычайной важности передаваемой информации. Быстро чередующиеся сообщения мешают составлению верных оценок и суждений.
6. Мифотворчество. Мифы очень жизнеспособны, и их жизненность объясняется тем, что опираясь на реальные факты и события, они воспринимаются как истина, догмат. Истинные же факты

зачастую воспринимаются людьми за небылицы. Именно так воспринимались рассказы афганцев о том, что они участвовали в настоящей войне, поскольку пропагандой в массовом сознании был закреплен миф об ограниченном введении советских войск в Афганистан.

7. Имидж. Имидж создает реальную социально-психологическую установку, определяющую поведение людей по отношению к объекту. И, поскольку воздействует на психику человека, следовательно, легко воспринимается, запоминается и потому часто используется в рекламе, имидж можно эффективно использовать как средство пропаганды, как инструмент управления сознанием. СМИ формирует огромное множество имиджей политиков, актеров, музыкантов, режиссеров. Создатели рекламы утверждают, что «люди курят не сигареты, а их образ», «женщины покупают не косметику, а желание быть красивой» и т.д.

Сложно определить наиболее эффективный метод, поскольку каждый из них оказывает определенное целенаправленное влияние. Все эти средства внушения оказывают огромнейшее влияние на человеческое сознание, заставляя самого человека действовать и думать определенным образом.

Влияние телевидения на детей

Можно выделить физическое и психологическое влияние телевидения на ребенка:

– Физическое влияние. Во-первых, перед экраном ребенок долгое время сидит неподвижно, что нарушает его естественную двигательную активность, которая в этом возрасте необходима для нормального гармонического развития. Во-вторых, в первые 4 года у человека развиваются острота зрения, а первые 10 лет – тонкая моторика, управляющая глазной мускулатурой. Когда ребенок смотрит телевизор мышцы глаз не тренируются, их активность снижается примерно на 90%, происходит изменение активности токов головного мозга и наступает так называемое «альфа-состояние» – состояние близкое к трансу. В-третьих, дети, которые проводят много времени перед телевизором, заболевают ожирением. Просто

бездельничая, человек снижает больше калорий, чем проведя это же время у телевизора.

– Психическое влияние. Дети, часто смотрящие телевизор, хуже умеют читать, хуже отличают реальное от вымысла; у них хуже развито воображение; они с большим страхом воспринимают мир; им свойственна повышенная тревожность сознания в сочетании с большой агрессивностью. Все это приводит к тому, что когда ребенок идет в школу, он меньше приспособлен к жизни, у многих детей наблюдается отставание в речи. Всё это – результат дефицита личного общения (В 1996 году английский логопед Сали Уорд опубликовала результаты своих десятилетних исследований. Она установила, что 20% обследованных детей в возрасте 9 месяцев отстают в развитии, если их родители используют телевизор как няньку. Если дети продолжают смотреть телевизор, к 3-летнему возрасту задержка составляет уже целый год).

Влияние сцен насилия по телевидению на поведение человека

Статистика свидетельствует, что если ребенок по 3-4 часа в день смотрит взрослые телепередачи, то еще до окончания начальной школы он увидит около 8 тысяч убийств. А ведь дети не способны критически воспринимать получаемую информацию и дистанцироваться от неё. Поэтому, когда ребенок видит сцены насилия в кино или телепередаче, это вызывает у него сильнейшие агрессивные импульсы. Частые просмотры телепрограмм со сценами насилия могут способствовать преступных наклонностей, а также предрасположенности к насилию. Мальчики восьми лет, обнаружившие самые сильные пристрастия к кинофильмам с кровавыми драконами и убийствами, с большой вероятностью окажутся среди совершивших тяжкие преступления по достижении ими 30-летнего возраста.

Специалисты считают, что факт влияния просмотра теленасилия на агрессивность уже может считаться доказанным и это влияние осуществляется, по крайней мере, пятью путями:

1. С помощью имитирующего научения (при наблюдении). Дети склонны имитировать поведение именно агрессивных персонажей, действия которых представляются в фильме или передаче как со-

циально приемлемые или имеют положительное подкрепление. В этом случае ребенок принимает данную модель и идентифицирует себя с ней.

2. Теленасилие делает детей нечувствительными к насилию в жизни. Чем больше ребенок смотрит теленасилия, тем более положительную установку на агрессивное поведение он принимает. Более того, дети, которые увлечены теленасилием, склонны подозревать других в использовании агрессивных действий, что является эмоциональным искажением, также увеличивающим вероятность использования ими агрессивного поведения.

3. Оправдание насилия на экранах телевизора. Ребенок с высоким уровнем агрессивности прибегает к теленасилию для того, чтобы избавиться от чувства вины и получить оправдание своей собственной агрессивности. Таким образом, впоследствии он становиться еще более склонным к примерению агрессивного поведения для разрешения возникающих социальных проблем.

4. Теленасилие содержит в себе ключевые стимулы, пробуждающие агрессивные мысли, фантазии, чувства и действия. Это объясняет известный факт, обнаруженный в ходе психологических экспериментов: когда дети наблюдали один вид агрессивного поведения, а затем демонстрировали агрессивное поведение другого рода. Даже совершенно посторонние объекты, связываемые ребенком с агрессией, могут впоследствии служить стимулом для запуска насильственного поведения.

5. Дети, увлеченные теленасилием, обнаруживали более низкий уровень физиологического возбуждения в ответ на показ сцен насилия, чем контрольная группа детей. В связи с этим они стремятся к постоянному поддержанию этого уровня, вновь обращаясь к теленасилию.

Отдельно следует выделить просмотр мультфильмов:

– Многократное повторение сцен садизма в западных мультфильмах вызывает у детей фиксацию агрессии и способствует выработке соответствующих моделей поведения.

– Агрессия в мультфильмах сопровождается красивыми, яркими картинками, например, рисуется красивая сцена, которая сопровождается убийством.

– Часто персонажи западных мультфильмов уродливы и внешне отвратительны. Ребенок идентифицирует себя с такими персонажами.

Влияние рекламы на детей

Реклама является средством манипулирования личностью, призванным скорректировать её потребности и вкусы в соответствии с нуждами рекламодателя (а не потребителя), и тем самым задать нужную траекторию движения денежных средств.

Согласно исследованиям, ребенок в возрасте до 8 лет не способен критически воспринимать рекламу и склонен относиться к ней с полным доверием. Если учесть, что в числе наиболее рекламируемых продуктов – конфеты, сахоросодержащие хлопья, сладкие напитки и всякого рода закуски, таким образом, реклама формирует неверное представление о здоровом сбалансированном питании.

Последствия влияния рекламы на детей:

– Удар по кошельку родителей. Каждый родитель знает, что стоит ему зайти в магазин с ребенком, ему придется там что-то купить: шоколадку, жевательную резинку, игрушку и т.п., потому что ребенок не успокоится до тех пор, пока его желание не будет удовлетворено.

– Формирование стереотипов поведения и личностных ценностей. По телевиденью показываю, как люди становятся миллионерами за полчаса, а звезды эстрады рождаются за четыре недели, пища готовиться моментально, а новорожденные кричат всего пять секунд. У детей создается установка, что любую программу можно решить только при помощи покупки товара, лишая их самостоятельности выбора и применения собственных сил. К тому же, формирование потребительских привычек толкает детей на постоянные траты, не объясняя, где брать деньги на эти покупки.

– Реклама вредит здоровью подрастающего поколения, особенно реклама вредных продуктов типа чипсов, фаст-фуда и сладко газированной воды, которые приводят к нарушению обмена веществ.

– Реклама приводит к различного рода зависимостям, особенно если речь идет о рекламе коротких SMS-сервисов, где подросток спокойно может поиграть в рулетку, и как отмечают психологи,

после двух-трех сеансов может начать развиваться игровая зависимость, с которой потом очень трудно бороться.

– Реклама ведет к ранней сексуальности. Полуобнаженные модели, на которых старается равняться молодое поколение и поведение которых принимает за эталон, присутствуют во многих рекламных роликах даже самых безобидных товаров.

7. КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Структура каналов передачи информации.
2. Классификация технических каналов информации.
3. Оптический канал утечки информации.
4. Акустический канал утечки информации.
5. Радиоэлектронный канал утечки информации.
6. Материально-вещественный канал утечки информации.
7. Классификация моделей безопасности информационных систем.
8. Классификация программно-технических методов и средств защиты информации
9. Применение принципа сплошной защиты.
10. Модель систем дискреционного разграничения доступа.
11. Модель систем мандатного разграничения доступа.
12. Модель систем ролевого разграничения доступа.
13. Политика безопасности в защите информации на уровне операционных систем.
14. Структурные уровни политики безопасности.
15. Учетные записи.
16. Антивирусное программное обеспечение.
17. Брандмауэр как способ защиты сети от угроз безопасности.
18. Средства «Автозагрузка» и «Диспетчер задач» в ОС Windows.
19. Реестр ОС Windows.
20. Средство «Восстановление» системы ОС Windows.
21. Макровирусы.
22. Способы установки паролей.

23. Аудит информационной безопасности. Цели аудита информационной безопасности.
24. Основные направления деятельности аудита информационной безопасности.
25. Активный аудит информационной безопасности.
26. Экспертный аудит информационной безопасности.
27. Аудит на соответствие стандартам.
28. Акты федерального законодательства РФ.
29. Нормативно-методические документы в области информационной безопасности.
30. Органы государственной власти РФ, обеспечивающие создание, изменение и исполнение механизмов защиты информации.
31. Управление рисками.
32. Влияние СМИ на человека.
33. Влияние просмотра рекламы и сцен насилия на ребенка.
34. Приемы рекламного воздействия

8. ВЫБОР ВАРИАНТА КОНТРОЛЬНЫХ РАБОТ

Пусть M – число, состоящее из трех последних цифр шифра. Тогда номер вашего варианта N определяется по формуле

$$N = \begin{cases} M, \textit{если } M \le 30, \\ M - 30, \textit{если } 30 < M \le 60, \\ M - 60, \textit{если } 60 < M \le 90, \\ M - 90, \textit{если } 90 < M \le 120. \end{cases}$$

Например, шифру 461-078 ($M = 78$) соответствует 18-й вариант; шифру 462-034 ($M = 34$) соответствует 4-й вариант.

9. КОНТРОЛЬНАЯ РАБОТА № 1

Контрольная работа № 1 включает тридцать вариантов по шесть заданий (табл. 3). В ответе на каждое из первых пяти заданий указывается наименование программного обеспечения (ПО). В первом задании рассматривается ПО архивации данных, во втором – разнообразные утилиты, предназначенные преимущественно для обеспечения наиболее полного контроля над системой, предотвращения повреждения жесткого диска и потери данных, в третьем задании – антивирусное ПО, в четвертом – межсетевые экраны, в пятом – ПО восстановления данных после удаления или повреждения жесткого диска. В шестом задании требуется ответить на три контрольных вопроса из раздела 5. Для подготовки ответов по этим заданиям можно использовать литературу [29–40].

Для выполнения заданий необходимо подготовить в редакторе MS Word или OO Writer документ, содержащий для каждого задания следующие характеристики указанного в задании ПО: наименование; описание (назначение, отличия от аналогов: преимущества и недостатки и т. д.); схема распространения (свободное или платное, если платное, то существует ли бесплатная пробная версия).

Подготовленные документы необходимо представить в отдельном файле, названном Вашей фамилией, номера контрольной и номера варианта контрольной работы (например, «Иванов_кр1_25.doc»), записанном на дискете или лазерном диске.

9.1. Варианты контрольной работы № 1

Варианты контрольной работы № 1 выбираются по схеме, описанной в разделе 8, и представлены в таблице 3.

Таблица 3

Варианты контрольной работы № 1

Вариант 1	
1. WinRar.	4. Jetico Personal Firewall.
2. TrojanKiller.	5. Advanced rar repair.
3. Sophos.	6. Контрольные вопросы 1, 9, 19.

Продолжение табл. 3

Вариант 2	
1. WinZip.	4. Safety Net.
2. RansomHide.	5. Undelete.
3. Trend Micro.	6. Контрольные вопросы 2, 12, 28.
Вариант 3	
1. ACB.	4. DefenseWall.
2. File Folder Protector.	5. BadCopy Pro.
3. F-Secure.	6. Контрольные вопросы 3, 10, 24.
Вариант 4	
1. 7-Zip.	4. PC tools Firewall.
2. XenAntiSpyware.	5. ZeroAssumptionRecovery.
3. Kaspersky.	6. Контрольные вопросы 4, 13, 27.
Вариант 5	
1. WaveZip.	4. ZoneAlarm Firewall.
2. Folder Guard Pro.	5. R.saver.
3. BitDefender.	6. Контрольные вопросы 5, 14, 21.
Вариант 6	
1. WavPack.	4. GeSWall.
2. Anti-keylogger.	5. Pandora Recovery.
3. Dr. Web.	6. Контрольные вопросы 6, 15, 30.
Вариант 7	
1. ZipMagic.	4. RusRoute Firewall.
2. Spybot – Search&Destroy.	5. MjM Free Photo Recovery.
3. ESET NOD32.	6. Контрольные вопросы 7, 17, 25.
Вариант 8	
1. ACE.	4. Outpost Firewall.
2. Anti-Porn.	5. FileRecoveryAngel.
3. Symantec.	6. Контрольные вопросы 8, 16, 28.
Вариант 9	
1. ARJ.	4. AVS Firewall.
2. Odin HDD Encryption.	5. CardRecovery.
3. McAfee.	6. Контрольные вопросы 9, 20, 23.
Вариант 10	
1. JAR.	4. Rising Personal Firewall.
2. AVG antispyware.	5. PC Inspector File Recovery.
3. Panda Security.	6. Контрольные вопросы 5, 13, 32.

Продолжение табл. 3

Вариант 11	
1. COMPRESSIA.	4. Webroot Desktop Firewall.
2. Superantispyware.	5. Recover My Files.
3. Avira.	6. Контрольные вопросы 2, 11, 29.
Вариант 12	
1. DZip.	4. Online Solutions Security Suite.
2. Ultima Steganography.	5. O&O UnErase.
3. AVG.	6. Контрольные вопросы 6, 19, 24.
Вариант 13	
1. ABC.	4. Online Armor.
2. Asterisk Key.	5. AnyFound Photo Recovery.
3. Norton Antivirus.	6. Контрольные вопросы 4, 15, 21.
Вариант 14	
1. ANN.	4. Sunbelt Personal Firewall.
2. NeoSpy.	5. Undelete Plus.
3. Avast.	6. Контрольные вопросы 1, 14, 33.
Вариант 15	
1. ZZIP.	4. CA Internet Security Suite Plus.
2. ChildWebGuardian.	5. R-Studio.
3. BullGuard Internet Security.	6. Контрольные вопросы 3, 12, 26.
Вариант 16	
1. WinUHA.	4. Trend Micro Internet Security.
2. Spyware Terminator.	5. EasyRecovery.
3. ZoneAlarm Antivirus.	6. Контрольные вопросы 7, 16, 28.
Вариант 17	
1. WinRK.	4. ZoneAlarm Free Firewall.
2. File Securer.	5. GetDataBack.
3. G Data AntiVirus.	6. Контрольные вопросы 8, 17, 23.
Вариант 18	
1. PKZIP.	4. Kaspersky Internet Security.
2. Access Administrator Pro.	5. Power Quest Lost & Found.
3. Outpost.	6. Контрольные вопросы 8, 19, 29.
Вариант 19	
1. PPMY.	4. Privatefirewall.
2. WinPatrol.	5. Ontrack Easy Recovery.
3. ArcaVir.	6. Контрольные вопросы 1, 11, 34.

Продолжение табл. 3

Вариант 20	
1. UHBC.	4. Jetico Personal Firewall.
2. Passware RARkey.	5. Stellar Phoenix Digital Media Recovery.
3. Rising Internet Security.	6. Контрольные вопросы 2, 13, 24.
Вариант 21	
1. UltimateZip.	4. Webroot Desktop Firewall.
2. Windows Firewall Control.	5. SoftPerfect File Recovery.
3. Simple Antivirus.	6. Контрольные вопросы 7, 21, 30.
Вариант 22	
1. StuffIt Deluxe.	4. Look'n'Stop Personal Firewall.
2. SUPERAntiSpyware.	5. Acronis Recovery Expert.
3. eScan AntiVirus.	6. Контрольные вопросы 3, 14, 25.
Вариант 23	
1. WinTar.	4. Sygate Firewall.
2. Pwdcrack.	5. Tokiwa DATARECOVERY.
3. Webroot AntiVirus.	6. Контрольные вопросы 6, 10, 20.
Вариант 24	
1. FreeArc.	4. FortKnox Firewall.
2. Notebak Alarm.	5. Avira UnErase Personal.
3. Fortinet.	6. Контрольные вопросы 4, 15, 22.
Вариант 25	
1. PeaZip.	4. VisNetic Firewall.
2. RogueRemover.	5. ADRC Data Recovery Software Tools.
3. BullGuard.	6. Контрольные вопросы 5, 16, 29.
Вариант 26	
1. QuickZip.	4. NetLimiter.
2. Emsisoft Anti-Malware.	5. DiskInternals Uneraser.
3. Norman.	6. Контрольные вопросы 9, 11, 22.
Вариант 27	
1. ZipGenius.	4. R-Firewall.
2. HWMonitor.	5. AusLogics Emergency Recovery.
3. Comodo AntiVirus.	6. Контрольные вопросы 6, 17, 25.
Вариант 28	
1. ALZip.	4. Kerio Control Firewall.
2. Mail Washer.	5. FreeUndelete.
3. AhnLab.	6. Контрольные вопросы 3, 10, 20.

Продолжение табл. 3

Вариант 29	
1. Izarc.	4. Tiny Firewall.
2. AdGuard.	5. Glary Undelete.
3. ArcaVir.	6. Контрольные вопросы 4, 19, 23.
Вариант 30	
1. jZip.	4. jFirewall.
2. Ad-Aware SE Personal.	5. R-Undelete.
3. MoonSecure.	6. Контрольные вопросы 5, 12, 27.

9.2. Рекомендации к выполнению контрольной работы № 1

Приведем пример, как может выглядеть документ для заданий 1–5 контрольной работы (ответы на вопросы из шестого задания рассматривать не будем, т. к. они кратко были изложены в первых четырех разделах). Предположим, мы имели следующие задания.

Вариант 31	
1. PowerArchiver.	4. Comodo Firewall.
2. CloseFolder.	5. Recuva.
3. Microsoft Security Essentials.	

1. *Наименование*: PowerArchiver (рис. 9).

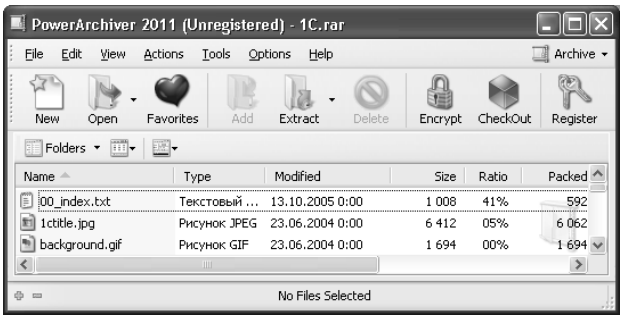

Рис. 9. Интерфейс программы PowerArchiver

Описание: Архиватор для Microsoft Windows. Имеет встроенную поддержку создания/извлечения множества различных типов ар-

хивов, в том числе ZIP, CAB, LHA (LZH), TAR, TAR.GZ, TAR.BZ2, BH (BlakHole), RAR, ARJ, ARC, ACE, ZOO, GZ, BZIP2 и т. д. Имеется возможность открывать различные форматы образов дисков: ISO, BIN, IMG и NRG. Существует встроенная утилита для просмотра файлов TXT, RTF, BMP, ICO, WMF, EMF, GIF, JPG (JPEG), Adobe Photoshop, Autodesk и др. Размеры файлов ограничены только возможностями ОС. Имеется возможность производить восстановление поврежденных ZIP архивов и выполнять проверку их на наличие вирусов, шифровать файлы и архивы, создавать самораспаковывающиеся и многотомные архивы и конвертировать архивы из одного формата в другой. Существует поддержка с FTP, длинных имен файлов, Drag-n-Drop, интеграция в Windows shell, развитая система помощи, удобный интерфейс с поддержкой скинов, интеграция с проводником Windows для быстрого создания и распаковывания архивов, мощная функция поиска по архивам, поддержка 15 языков. Первоначальное название программы было EasyZip.

Схема распространения: PowerArchiver является платным ПО с 30-дневной бесплатной пробной версией. При покупке персональной лицензии предоставляется доступ ко всем обновлениям последующих версий программы, при бизнес-лицензии – только двух последующих стабильных релизов.

2. *Наименование*: CloseFolder (рис. 10).

   Описание: Программа, которая позволяет блокировать доступ к папкам. Преимуществом CloseFolder является то, что после удаления этой программы или после переноса папки на другой компьютер она все равно будет закрыта. Имеется возможность установки пароля на запуск программы, блокировки папки из контекстного меню и блокировки папок по списку.

   Схема распространения: программа CloseFolder является платным ПО, имеется тридцатидневная бесплатная пробная версия.

Рис. 10. Интерфейс программы CloseFolder

3. *Наименование*: Microsoft Security Essentials (рис. 11).

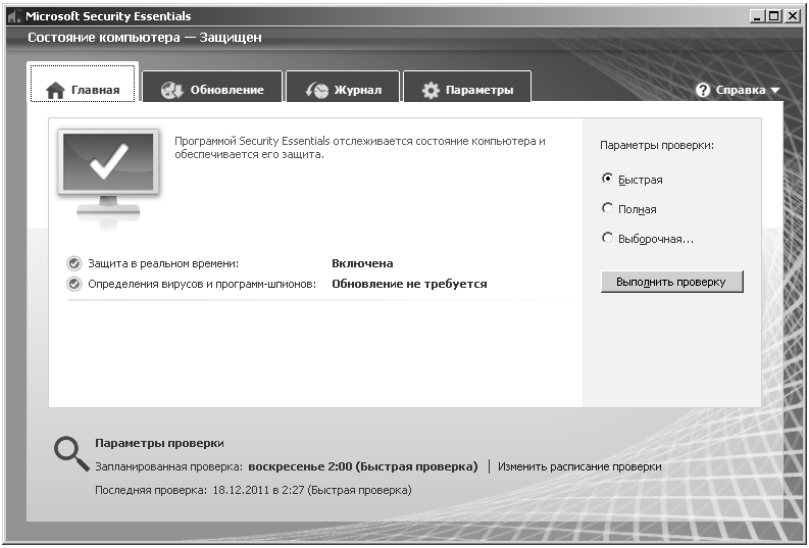

Рис. 11. Интерфейс программы Microsoft Security Essentials

Описание: Пакет антивирусных приложений от компании Microsoft, предназначенный обеспечивать борьбу с различными вирусами, шпионскими программами, руткитами и троянскими программами. Антивирус Microsoft Security Essentials пришёл на замену Windows Live OneCare (коммерческая антивирусная программа от Microsoft), а также бесплатному Windows Defender, который защищал пользователей от рекламного и шпионского программного обеспечения. Microsoft Security Essentials включает защиту в реальном времени. Является экономной по отношению к оперативной памяти, имеет простой в использовании пользовательский интерфейс. Существует интеграция с брандмауэром Windows. Поддерживается служба динамических подписей, которая дает возможность проверки, несет ли угрозу подозрительная программа (перед запуском подозрительной программы Microsoft Security Essentials эмулирует ее поведение, чтобы выяснить ее дальнейшие действия). В версию Microsoft Security Essentials 2011 года включена функ-

ция защиты сети. К достоинствам также можно отнести маленький установочный пакет (около 7 Мб) и быструю скорость установки, к недостаткам – достаточно продолжительное первое обновление (от 5 до 15 минут). В Microsoft Security Essentials включен ряд новых и усовершенствованных технологий для обнаружения пакетов программ rootkit, от которых особенно сложно защититься. В 2011 году журнал PC Advisor антивирус Microsoft Security Essentials 2.0 включил в список «Пять лучших бесплатных пакетов безопасности», который также содержал: Avast! 6 Free Edition, Comodo Antivirus 5.4, AVG Antivirus 2011 и BitDefender Total Security 2012 Beta.

Схема распространения: Microsoft Security Essentials является бесплатным ПО для домашнего использования при условии легальной копии Windows. Лицензия предусматривает, что в случае нелегальности версии операционной системы, последняя будет заблокирована. Малые предприятия также имеют право устанавливать Microsoft Security Essentials для бесплатного использования, но только на 10 компьютерах. Однако лицензионное соглашение отрицает использование антивируса в учебных заведениях, предприятиях и правительственных органах. Лицензия запрещает пользователям производить реверс-инжиниринг, взлом, декомпиляцию и дизассемблирование Microsoft Security Essentials или публиковать, а также раскрывать результаты тестирования и любые другие оценочные испытания программного продукта третьим лицам без предварительного письменного согласия с корпорацией Microsoft.

4. *Наименование*: Comodo Firewall (рис. 12).

   Описание: Персональный файервол (или межсетевой экран, или брандмауер) компании Comodo для Microsoft Windows. Comodo Firewall входит в состав набора инструментов Comodo Internet Security для защиты компьютера. Comodo Firewall проверяет обширный список из более чем двух миллионов безопасных приложений. Если приложения нет в безопасном списке, то Comodo Firewall сообщает о возможной угрозе, прежде чем разрешить приложению доступ к вашему ПК, что позволяет предотвратить проникновение и распространение на компьюте-

ре вредоносных программ. Список безопасных программ может быть настроен пользователем. Существует автоматическое обновление фаервола. Позволяет осуществлять проактивную защиту (систему отражения локальных угроз), защиту от интернет-атак, защиту от переполнения буфера, защиту от несанкционированного доступа, защиту важных системных файлов и записей реестра от внутренних атак, обнаружение переполнения буфера. В течение 2010 года Comodo Firewall был на первом месте во множествах тестов, посвящённых проблемам защиты персонального компьютера программами класса Firewall, и признан лучшим фаерволом.

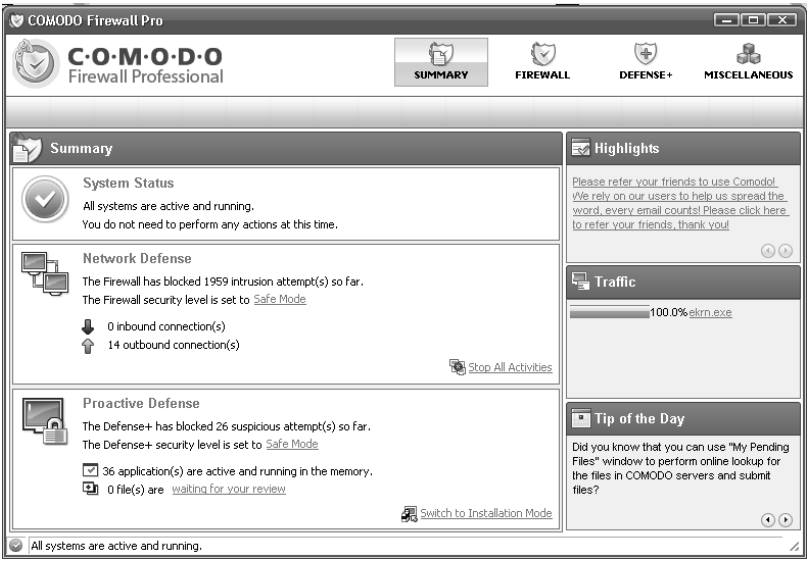

Рис. 12. Интерфейс программы Comodo Firewall

Схема распространения: Comodo Firewall является бесплатным ПО (не путать с пакетом Comodo Internet Security, который является коммерческим продуктом с бесплатной 30-дневной версией).

5. *Наименование*: Recuva (рис. 13).

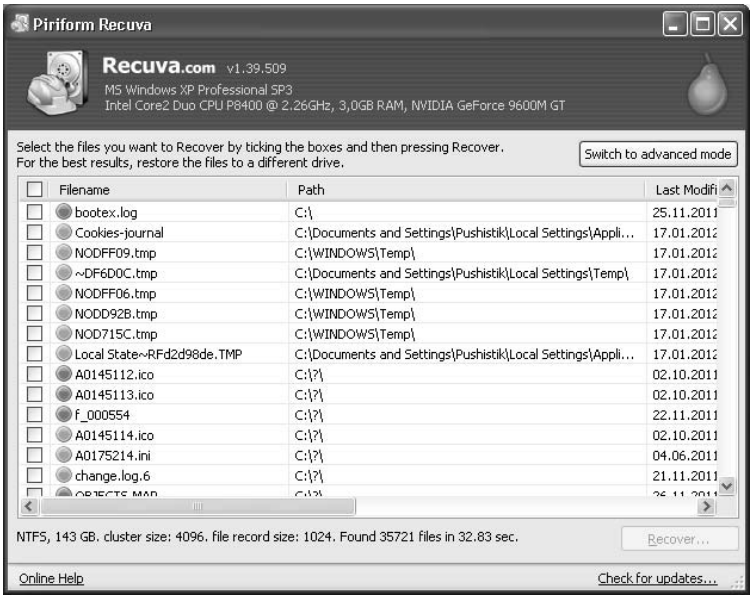

Рис. 13. Интерфейс программы Recuva

Описание: Специальная утилита, которая предназначена для восстановления удаленных или потерянных данных. Существует возможность восстановления данных с поврежденных и отформатированных носителей информации, восстановления удалённых сообщений из почтового ящика (поддерживает Microsoft Outlook Express, Mozilla Thunderbird и Windows Live Mail), удалённой музыки с iPod или MP3 плееров, структуры папок, несохранённых документов Microsoft Word. Recuva позволяет надежно удалить файлы, которые пользователи хотят стереть навсегда (без возможности восстановления), искать неудаленные файлы с поврежденных носителей. В Recuva поддерживается многоязычность интерфейса (в том числе, русская версия) и поддержка всех операционных систем Windows.
Схема распространения: Recuva является бесплатным ПО.

10. КОНТРОЛЬНАЯ РАБОТА № 2

Во второй контрольной работе необходимо подготовить в реферативной форме развернутый (на 25–30 страниц) ответ на соответствующую варианту задания тематику. Текст реферата представить в отдельном файле, названном Вашей фамилией, номера контрольной и номера варианта контрольной работы (например, «Иванов_кр2_25.doc»), записанном на дискете или лазерном диске.

Варианты контрольной работы № 2 выбираются по схеме, описанной в разделе 8, и выбираются из следующего списка:

1. Атаки на схемы типа Бонеха-Франклина для обнаружения внутренних нарушителей.
2. Различные подходы построения безопасных служб установки точного времени в электронном документообороте.
3. Механизм электронных водяных знаков.
4. Схемы электронных платежных систем и методы их защиты.
5. Вопросы информационной безопасности аутсорсинга.
6. Модели внутреннего нарушителя информационной безопасности.
7. Безопасность в беспроводных сетях.
8. Особенности сбора исходной информации системами обнаружения атак.
9. Коммерческие средства аутентификации пользователей телекоммуникационных сетей.
10. Методология разработки политики информационной безопасности предприятия.
11. Общий порядок проведения лицензирования в области защиты информации и контроль за деятельностью лицензиатов.
12. Виды и схемы сертификации средств защиты информации, проведения сертификации и контроля.
13. Виды и особенности проведения аттестации помещений по требованиям безопасности информации.
14. Испытания объектов на соответствие требованиям по защите информации от несанкционированного доступа, от утечки по акустическим каналам и каналам ПЭМИН.
15. Примеры взломов сетей и Web-узлов через Internet.

16. Причины уязвимости сети Internet.
17. Классификация злоумышленников.
18. Идентификация и аутентификация – понятия и виды.
19. Ролевое управление доступом и управление доступом в Java-среде.
20. Типовая структура и основные функции службы безопасности.
21. Способы предотвращения утечки информации по материально-вещественному каналу утечки информации.
22. Принцип защиты от деструктивных действий и размножения компьютерных вирусов, а также технология гарантированного восстановления системы после заражения вирусом.
23. Методы и средства защиты информации в системах управления базами данных.
24. Методы и средства защиты конфиденциальной информации на крупных коммерческих и правительственных сайтах.
25. Рейтинг средств межсетевого экранирования и антивирусного обеспечения.
26. Определение слабых мест в защите сервисов: FTP, TFTP, SSH, Finger, HTTP, IMAP, SMTP, NetDIOS/SMB, RPC.
27. Проверка наличия в web-сервисах уязвимых сценариев, на базе BasicScript, JavaScript, Perl и ActiveXo.
28. Обеспечение взаимодействия между субъектами, защищающими и использующими информацию ограниченного доступа, подбор и обучение персонала.
29. Методы и модели оценки эффективности комплексной системы защиты информации.
30. Методы влияния СМИ на общественное мнение. Информационная война.

ЛИТЕРАТУРА

1. Ярочкин В.И. Информационная безопасность: учебник для вузов по гуманит. и социал.-экон. спец. – М.: Академический Проект: Трикста, 2005. – 543 с.
2. Торокин А.А. Инженерно-техническая защита информации:

учебн. пособие для студентов, обучающихся по специальности в области информ. безопасности. – М.: Гелиос АРВ, 2005. – 960 с.
3. Зайцев А.П., Шелупанов А.А. Техническая защита информации: учебн. пособие. – М.: Горячая линия-Телеком, 2007. – 616 с.
4. Грибунин В.Г., Чудовский В.В. Комплексная система защиты информации на предприятии: учеб. пособие для студ. высш. учеб. заведений. – М.: Издательский центр "Академия", 2009. – 416 с.
5. Хореев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Том 1. Технические каналы утечки информации. – М.: НПЦ «Аналитика», 2008. – 436 с.
6. Несанкционированный доступ в электромагнитных каналах [электронный ресурс] / URL: http://www.twirpx.com/file/4269/.
7. Хорев П.Б. Методы и средства защиты информации в компьютерных системах: учебное пособие для вузов по направлению 230100 (654600) «Информатика и вычислительная техника». – М.: Академия, 2007. – 255 с.
8. Расторгуев С.П. Основы информационной безопасности: учебное пособие для вузов по спец. «Компьютер. Безопасность», «Комплекс. обеспечение информ. безопасности автоматиз. систем» и «Информ. безопасность телекоммуникац. систем». – М.: Академия, 2007 – 186 с.
9. Партыка Т.Л., Попов И.И. Информационная безопасность: учебное пособие для средн. проф. образования по спец. информатики и вычислительной техники. – М.: ФОРУМ, 2011. – 431 с.
10. Правовое регулирование защиты информации в России [электронный ресурс] / URL: http://www.e-nigma.ru/stat/dip_1/.
11. Варфоломеев А.А. Основы информационной безопасности: учебн. пособие. – М.: РУДН, 2008. – 412 с.
12. Земор Ж. Курс криптографии. – М. – Ижевск: НИЦ «Регулярная и хаотическая динамика»; Институт компьютерных исследований, 2006. – 256 с.
13. Тихонов В.А., Райх В.В. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты: учебное пособие. – М.: Гелиос АРВ, 2006. – 528 с.

14. Девянин П.Н. Модели безопасности компьютерных систем: учебн. пособие для студ. высш. учеб. заведений. – М.: Академия, 2005. – 144 с.
15. Макашов Д. Модели безопасности компьютерных систем [электронный ресурс] // URL: itsec.ru/articles2/Inf_security/models.
16. Информационная безопасность [электронный ресурс] / URL: http://ru.wikipedia.org/wiki/Информационная_безопасность.
17. Информационно-аналитический центр Anti-Malware [электронный ресурс] / URL: anti-malware.ru/tests_history.
18. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации: учебное пособие для вузов по спец. 230201 «Информационные системы и технологии». – М.: Академия, 2007. – 331 с.
19. Андрончик А.Н., Богданов В.В., Домуховский Н.А. [и др.]. Защита информации в компьютерных сетях. Практический курс: учебное пособие – Екатеринбург: УГТУ-УПИ, 2008. – 248 с.
20. Alexfedoruk Комплексная защита от вирусов [электронный ресурс] / URL:http://litvik.ru/2/13/uchebniki_manuals/18118-alexfedoruk-kom pleksnaya-zaschita-ot-virusov.html.
21. IP [электронный ресурс] / URL: 2ip.ru/article/.
22. WindowsFAQ [электронный ресурс] / URL: windowsfaq.ru/content/view/328/46/1/1
23. Mozilla Corporations [электронный ресурс] / URL: https://addons.mozilla.org/ru/firefox/search/?q=&cat=1%2C12
24. Расширения Opera [электронный ресурс] / URL: https://addons.opera.com/addons/extensions/
25. Кастер Х. Основы Windows NT и NTFS. – М.: Изд. отдел «Русская редакция» ТОО «Channel Trading Ltd.», 1996. – 440 с.
26. Люцарев В.С., Ермаков К.В., Рудный Е.Б. [и др.] Безопасность компьютерных сетей на основе Windows NT. – М.: Изд. отдел «Русская редакция» ТОО «Channel Trading Ltd.», 1998. – 304 с.
27. Демин С.Л., Вайнштейн Ю.В. Основы информационной безопасности: методические указания. Красноярск, 2007. – 19 с.
28. Гафнер В.В. Информационная безопасность: учеб. пособие. – Ростов н/Д: Феникс, 2010. – 324 с.
29. Ватолин Д., Ратушняк А., Смирнов М. [и др.] Методы сжатия

данных. Устройство архиваторов, сжатие изображений и видео. – М.: ДИАЛОГ-МИФИ, 2002. – 384 с.
30. Гультяев, А.К. Восстановление данных. – СПб.: Питер, 2006. – 379 с.
31. Ведеев, Д. Защита данных в компьютерных сетях. Открытые системы. – М.: Спартак, 2004. – 120 с.
32. Архиваторы [электронный ресурс] / URL: www.compress.ru/article.aspx?id=9776&iid=412.
33. Всё о сжатии данных, изображений и видео [электронный ресурс] / URL: http://compression.ru/.
34. Всё для Windows, мобил, КПК, смартфонов [электронный ресурс] / URL: http://panlom.hut.ru/.
35. Подробная документация по настройке Windows XP, Windows Vista, Windows 7 и Windows 8 [электронный ресурс] / URL: http://windxp.com.ru/secret.htm.
36. WOZZ.RU сайт о безопасности в сети [электронный ресурс] / URL: http://wozz.ru/.
37. Комплексная защита от вредоносных программ [электронный ресурс] / URL: http://www.comss.ru/.
38. Antivirus-Software [электронный ресурс] / URL: http://www.antivirus-software.ru/.
39. Информационная безопасность [электронный ресурс] / URL: http://www.securrity.ru/.
40. Securelist [электронный ресурс] / URL: www.viruslist.ru/.

СОДЕРЖАНИЕ

Корректор А.Н. Воробьева

Подписано к печати 02.07.2014 г. Формат $60\times84^{1}/_{16}$.
Бумага для офисной техники. Гарнитура Times.
Усл. печ. л. 5,8.
Тираж 50 экз. Заказ № 451.

Отпечатано на оборудовании
Издательского Дома
Томского государственного университета
634050, г. Томск, пр. Ленина, 36
Тел. 8+(382-2)–53-15-28