Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное
учреждение высшего профессионального образования
«Комсомольский-на-Амуре государственный технический университет»

В. А. Челухин

КОМПЛЕКСНОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Утверждено в качестве учебного пособия
Ученым советом Федерального государственного бюджетного
образовательного учреждения высшего профессионального образования
«Комсомольский-на-Амуре государственный технический университет»

Комсомольск-на-Амуре
2014

УДК 002:004.056(07)
ББК 32.973я7
Ч-405

Рецензенты:

ЗАО «Предприятие Русич-ДВ», канд. техн. наук, доцент,
главный научный сотрудник А. И. Руднев;
Г. Ф. Вильдяйкин канд. техн. наук, доцент,
член-корреспондент АЭН РФ, лицензиат ФСТЭК РФ,
заместитель генерального директора ОАО "Амурская ЭРА"

Челухин, В. А.

Ч-405 Комплексное обеспечение информационной безопасности автоматизированных систем : учеб. пособие / В. А. Челухин. – Комсомольск-на-Амуре : ФГБОУ ВПО «КнАГТУ», 2014. – 207 с.

ISBN 978-5-7765-1137-0

Рассматриваются основные вопросы комплексного обеспечения информационной безопасности. Подробно разбираются методы и средства защиты информации от несанкционированного вмешательства. Комплексно рассмотрены все аспекты обеспечения информационной безопасности автоматизированных систем – правово-юридические, организационные, аппаратные и программные. Изучены принципы защиты от вирусов и защиты информации от несанкционированных действий по использованию конфиденциальной информации.

УДК 002:004.056(07)
ББК 32.973я7

ISBN 978-5-7765-1137-0

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

В современном мире информационный ресурс стал одним из наиболее мощных рычагов экономического развития. Сегодня информация приравнивается к важнейшим ресурсам наряду с сырьем и энергией. В развитых странах большинство работающих заняты не в сфере производства, а в той или иной степени занимаются обработкой информации. В современном деловом мире происходит процесс миграции материальных активов в сторону информационных. По мере развития организации усложняется ее информационная система, основной задачей которой является обеспечение максимальной эффективности ведения бизнеса в постоянно меняющихся условиях конкуренции на рынке.

Широкое внедрение персональных компьютеров вывело уровень информатизации деловой жизни на качественно новую ступень. Ныне трудно представить себе фирму или предприятие (включая самые мелкие), которые не были бы вооружены современными средствами обработки и передачи информации. В компьютерах и на серверах, на носителях данных накапливаются значительные объемы информации, представляющей большую ценность для ее владельца.

Однако создание индустрии переработки информации, давая объективные предпосылки для грандиозного повышения эффективности жизнедеятельности человечества, порождает целый ряд сложных и крупномасштабных проблем. Одной из таких проблем является надежное обеспечение сохранности и установленного статуса использования информации, циркулирующей и обрабатываемой в информационных системах.

Рассматривая информацию как товар, можно сказать, что информационная безопасность в целом может привести к значительной экономии средств, в то время как ущерб, нанесенный ей, приводит к значительным материальным затратам. Например, раскрытие технологии изготовления оригинального продукта приведет к появлению аналогичного продукта, но от другого производителя, и как следствие нарушения информационной безопасности, владелец технологии, а может быть и автор, потеряют часть рынка.

С другой стороны, информация является субъектом управления, и ее изменение может привести к катастрофическим последствиям в объекте управления.

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

В настоящее время промышленно развитые страны переживают новый исторический этап научно-технической революции, связанный с возрастанием роли информации в общественном производстве. Сложившаяся ранее система отношений, получившая условное название "индустриального общества", переходит в исторически новое "информационное общество", общество, основанное на информации.

Информационное общество – объективно возникшая в ходе исторического процесса стадия общественного развития. Она предполагает качественно новый, более высокий уровень производительных сил (в сравнении с индустриальным обществом). При переходе от индустриального общества к информационному резко возрастает значение информации, её накопления и использования во всех сферах социальной практики, что ведет к усилению динамизма социальных процессов и ускорению общественного прогресса, интеграции всего человечества.

Исторически развитие средств и методов защиты информации условно можно разделить на три этапа.

Первый из этих подходов условно может быть назван примитивным. Он характерен для начального периода развития работ по защите информации. Отличительными особенностями этого подхода являются попытки решения проблемы защиты путем разового включения несложных механизмов защиты в состав системы. Основное внимание уделялось обеспечению ее физической целостности. Нарушение информации на этом первоначальном этапе рассматривалось как результат воздействия естественных факторов, главными из которых являются отказы, сбои и ошибки элементной базы. Проблемы защиты от несанкционированного получения информации в большинстве случаев не возникало. Это объяснялось автономностью работы ЭВМ первых поколений, индивидуальностью реализации процедур обработки, представление информации в памяти ЭВМ и на машинных носителях в закодированном виде.

По мере роста масштабов автоматизации обработки информации уязвимость информации со стороны злоумышленников стала быстро расти. Ущерб от подобных действий нередко принимал внушительные размеры и приводил к серьезным сбоям и уничтожению информации. Возникла проблема угроз безопасности информации вследствие заражения систем компьютерными вирусами. Поэтому на рубеже 70-80-х гг. на смену примитивному пришел полусистемный подход, который характеризовался существенным расширением используемых средств защиты, особенно программных и юридических.

Наконец, в последние годы на смену полусистемному пришёл комплексный подход к организации защиты информации. Для этого подхода характерен взгляд на защиту информации как на непрерывный процесс, осуществляемый на всех этапах жизненного цикла автоматизированных

систем – проектировании, создании, эксплуатации. Причем все используемые средства и методы объединены в единую систему, в которой немалую роль играет созданная на этом этапе нормативно-правовая база защиты информации. К указанным средствам относятся законы, стандарты и другие нормативно-правовые акты, регламентирующие правила обращения с защищаемой информацией и являющиеся обязательными для соблюдения.

Отчетливо просматривается тенденция выработки и реализации концепции защиты, направленной на решение трех классов задач – задач анализа, синтеза и управления.

Задача анализа заключается в объективной оценке потенциальных угроз информации и возможного ущерба от их проявления.

Задачи синтеза – определение наиболее эффективных форм и способов организации механизмов защиты.

Задачей управления является обеспечение рационального использования созданных механизмов защиты в процессе обработки защищаемой информации.

Кроме того, достаточно явно наблюдаются и следующие тенденции - обострение конкуренции и снижение лояльности сотрудников зачастую приводит к увеличению рисков, связанных с информационной безопасностью (ИБ). Нестабильные экономические условия заставляют компании внимательнее относиться к вопросам защиты информации, при этом инциденты в сфере информационной безопасности имеют прямое влияние на прибыль компаний. Перед руководителями подразделений по ИБ стоят задачи оптимального построения службы информационной безопасности, ее взаимосвязи с другими подразделениями и распределения полномочий, для обеспечения соответствия современным требованиям бизнеса.

В этих условиях необходимо по новому взглянуть на эффективность систем информационной безопасности, связанные с нею риски, определить обязательные действия по защите информации, и необходимые приоритеты дальнейшего развития.

Сегодня современные методы и решения дают возможность обеспечить очень высокий уровень информационной безопасности, однако и затраты на эти мероприятия могут оказаться весьма значительными – в крупных организациях затраты на защиту информационных систем иногда достигают 20 – 30 % ИТ-бюджета, поэтому одним из важных этапов создания эффективной системы защиты информации является её первичный технико-экономический анализ. Необходимо в первую очередь определить возможный материальный ущерб от нарушения, потери или кражи информации и необходимых затрат на её реализацию.

Анализ затрат на реализацию проектов в сфере ИБ целесообразно начать с анализа возможных потерь от нарушения режима информационной безопасности, определения возможных угроз и издержек и оценки

экономических последствий внедрения и использования таких систем безопасности. Как правило, эти затраты будут иметь следующий характер:

– проектирование информационной системы;

– приобретение аппаратных и программных средств;

– разработка программного обеспечения и его документирование, а также затраты на исправление ошибок и доработку в течение периода эксплуатации;

– текущее администрирование информационных систем;

– техническая поддержка и сервисное обслуживание;

– расходные материалы;

– телекоммуникационные услуги;

– затраты на обучение.

Также в расчет затрат на повышение уровня ИБ необходимо включить расходы на реорганизацию бизнес-процессов и информационную работу с персоналом. Кроме того, при анализе расходов необходимо также учесть, что в большинстве случаев внедрение средств защиты информации предполагает появление дополнительных обязанностей у персонала предприятия и необходимость осуществления дополнительных операций при работе с информационными системами.

Все перечисленное указывает на важность именно комплексного подхода к организации защиты информации и информационных автоматизированных систем, учитывающего законодательные, организационные, кадровые, технические и программные меры обеспечения информационной безопасности.

1. ПОНЯТИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Прежде, чем переходить к исследованию проблем информационной безопасности, необходимо подробно разобраться с самим понятием "*безопасность*" и "*информационная безопасность*" (ИБ). Закон «О безопасности» от 5 марта 1992 г. дает следующее понятие безопасности.

Статья 1. Понятие безопасности и ее объекты

Безопасность – состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.

Жизненно важные интересы – совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства.

К основным объектам безопасности относятся: личность – ее права и свободы; общество – его материальные и духовные ценности; государство – его конституционный строй, суверенитет и территориальная целостность.

Статья 2. Субъекты обеспечения безопасности

Основным субъектом обеспечения безопасности является государство, осуществляющее функции в этой области через органы законодательной, исполнительной и судебной властей.

Государство в соответствии с действующим законодательством обеспечивает безопасность каждого гражданина на территории Российской Федерации. Гражданам Российской Федерации, находящимся за ее пределами, государством гарантируется защита и покровительство.

Граждане, общественные и иные организации и объединения являются субъектами безопасности, обладают правами и обязанностями по участию в обеспечении безопасности в соответствии с законодательством Российской Федерации, законодательством республик в составе Российской Федерации, нормативными актами органов государственной власти и управления краев, областей, автономной области и автономных округов, принятыми в пределах их компетенции в данной сфере. Государство обеспечивает правовую и социальную защиту гражданам, общественным и иным организациям и объединениям, оказывающим содействие в обеспечении безопасности в соответствии с законом.

Статья 4. Обеспечение безопасности

Безопасность достигается проведением единой государственной политики в области обеспечения безопасности, системой мер экономического, политического, организационного и иного характера, адекватных угрозам жизненно важным интересам личности, общества и государства.

Для создания и поддержания необходимого уровня защищенности объектов безопасности в Российской Федерации разрабатывается система правовых норм, регулирующих отношения в сфере безопасности, определяются основные направления деятельности органов государственной власти и управления в данной области, формируются или преобразуются органы обеспечения безопасности и механизм контроля и надзора за их деятельностью.

Для непосредственного выполнения функций по обеспечению безопасности личности, общества и государства в системе исполнительной власти в соответствии с законом образуются государственные органы обеспечения безопасности.

Понятие "*информационная безопасность*" поясняется в нескольких законах и в Доктрине информационной безопасности Российской Федерации.

В Законе "Об информации, информационных технологиях и о защите информации" *информационная безопасность* определяется как состояние защищенности информационной среды.

В Доктрине информационной безопасности Российской Федерации термин "*информационная безопасность*" определяется как состояние защищенности национальных интересов в информационной сфере, опреде-

ляемых совокупностью сбалансированных интересов личности, общества и государства.

Более конкретно информационная безопасность определяется как защищённость информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений.

Необходимо также отметить, что понятие *информационная безопасность* иногда заменяют термином "компьютерная безопасность" (как эквивалент или заменитель ИБ), что совершенно неправильно. Компьютеры – только одна из составляющих информационных систем. Безопасность же автоматизированных систем обработки информации определяется всей совокупностью мер безопасности, таких, как юридические, организационные, физические и другие.

Считается также, что безопасность информации – это состояние защищённости информации, при котором обеспечены её конфиденциальность, доступность и целостность.

Конфиденциальность – недоступность информационных ресурсов для неуполномоченных лиц.

Целостность – неизменность информации в процессе её передачи или хранения.

Доступность – возможность получения и использования информационных ресурсов только по требованию уполномоченных лиц.

В целом условно информационную безопасность можно разделить на три большие составляющие:

1) информационная безопасность государства;

2) информационная безопасность организации;

3) информационная безопасность личности.

Коротко эти составляющие можно определить следующим образом.

Информационная безопасность государства – это состояние государства, в котором ему не может быть нанесен существенный ущерб путем оказания воздействия на его информационную сферу. Проблемы государственной безопасности в своей совокупности образуют весьма сложную, многоплановую и комплексную систему.

Здесь следует заметить, что информационная безопасность государства часто заменяется термином национальная безопасность, что в корне неправильно. Российская Федерация – это многонациональное государство, и говорить о национальных интересах здесь практически невозможно. Национальные интересы – это интересы отдельной национальности, например интересы этнического характера, сохранения самобытности, культуры, традиций.

Государство должно защищать общие интересы всех наций, входящих в его состав. Его задачи в информационной сфере заключаются в создании условий для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, а также в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, развитии равноправного и взаимовыгодного международного сотрудничества.

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

Первая составляющая государственных интересов в информационной сфере включает в себя обеспечение конституционных прав и свобод гражданина в области получения информации и пользования ею, духовного обновления России; сохранение и укрепление нравственных ценностей общества, традиций патриотизма, культурного и научного потенциала страны; защиту их от угрозы путем информационного разрушения.

Вторая составляющая включает в себя информационное обеспечение достоверной информацией о государственной политике Российской Федерации, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам.

Третья составляющая включает в себя развитие современных информационных технологий, отечественной индустрии информации, средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок.

Четвертая включает в себя защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем на территории России, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов, сохранение государственной тайны и конфиденциальности документированной информации.

Информационная безопасность организации – это состояние информационной структуры организации, при котором ей не может быть нанесен существенный ущерб путем воздействия на её информационную сферу. Реализуется через административную и программно-техническую регламентацию производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающей или существенно затрудняющей неправомерное овладение конфиденциальной информацией.

Без надежных мер информационной безопасности любое современное предприятие становится беззащитным перед неправомерными действиями не только внешних злоумышленников, но и собственных сотрудников.

Информационная безопасность личности – это состояние человека, в котором его личности не может быть нанесен ущерб путем оказания воздействия на окружающее информационное пространство. Это защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах.

Кроме того, все меры и способы по реализации информационной безопасности можно разделить на несколько уровней:

1) законодательные меры информационной безопасности;
2) организационные меры информационной безопасности;
3) технические способы информационной безопасности;
4) программные способы информационной безопасности.

Рассмотрим подробно каждый из них.

2. ЗАКОНОДАТЕЛЬНЫЕ МЕРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Законодательный уровень информационной безопасности основывается на положениях национальных и международных законов, правовых актах, уголовном и других кодексах, которые защищают авторское право и конфиденциальность информации. В информационной сфере основу информационной безопасности составляют нормы Конституции РФ о праве каждого на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени (ч. 1 ст. 23), а также на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (ч. 2 ст. 23).

Конституция РФ провозглашает недопустимость разглашения информации, которой обмениваются между собой люди. Вся эта информация не должна подвергаться цензуре. Работники организаций, обслуживающие каналы коммуникаций, должностные и иные официальные лица (следователи, понятые, присутствующие при выемке корреспонденции, и т.п.) несут ответственность за разглашение содержания корреспонденций.

2.1. Нормативно-законодательная база информационной безопасности как часть комплекса информационной безопасности

Нормативно-законодательная база информационной безопасности является частью всего комплекса информационной безопасности. В состав этой базы входит весь комплекс нормативно-технических и нормативно-методических документов по защите информации. Различают:

- законодательные акты или законы РФ;
- постановления Правительства РФ;

– доктрины Российской Федерации в области защиты информации;
– нормативно-методические документы по защите информации;
– документы уполномоченных федеральных органов;
– национальные стандарты в области защиты информации;
– международные стандарты в области защиты информации;
– международные соглашения в области защиты информации.

Рассмотрим наиболее важнейшие из них. Как было указано ранее, первая составляющая государственных интересов в информационной сфере включает в себя обеспечение конституционных прав и свобод гражданина в области получения информации и пользования ею.

2.2. Право граждан на информацию

Право граждан на информацию является одним из важнейших экономических, политических и личных прав человека и гражданина. Реализация права граждан на информацию, обеспечение свободного доступа к имеющей общественное значение информации, информационная открытость органов власти являются важнейшими условиями и критериями функционирования правового государства.

В России право граждан на информацию обеспечивается прежде всего Конституцией Российской Федерации, принятой в 1993 г. Приведем статьи и отдельные их положения по этому вопросу.

Статья 24

2. Органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

Статья 29

1. Каждому гарантируется свобода мысли и слова.

4. Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Перечень сведений, составляющих государственную тайну, определяется федеральным законом.

5. Гарантируется свобода массовой информации. Цензура запрещается.

Статья 41

3. Сокрытие должностными лицами фактов и обстоятельств, создающих угрозу для жизни и здоровья людей, влечет за собой ответственность в соответствии с федеральным законом.

Статья 42

Каждый имеет право на благоприятную окружающую среду, достоверную информацию о ее состоянии и на возмещение ущерба, причиненного его здоровью или имуществу экологическим правонарушением.

Одним из инструментов реализации права граждан на получение информации являются средства массовой информации. Закон РФ «О средствах массовой информации» устанавливает право граждан на оперативное получение через средства массовой информации достоверных сведений о деятельности государственных органов и организаций, общественных объединений, их должностных лиц. Приведем отдельные наиболее важные статьи этого закона.

Статья 1. Свобода массовой информации

В Российской Федерации поиск, получение, производство и распространение массовой информации, учреждение средств массовой информации, владение, пользование и распоряжение ими, изготовление, приобретение, хранение и эксплуатация технических устройств и оборудования, сырья и материалов, предназначенных для производства и распространения продукции средств массовой информации, не подлежат ограничениям, за исключением предусмотренных законодательством Российской Федерации о средствах массовой информации.

Статья 38. Право на получение информации

Граждане имеют право на оперативное получение через средства массовой информации достоверных сведений о деятельности государственных органов и организаций, общественных объединений, их должностных лиц.

Государственные органы и организации, общественные объединения, их должностные лица предоставляют сведения о своей деятельности средствам массовой информации по запросам редакций, а также путем проведения пресс-конференций, рассылки справочных и статистических материалов и в иных формах.

Статья 39. Запрос информации

Редакция имеет право запрашивать информацию о деятельности государственных органов и организаций, общественных объединений, их должностных лиц. Запрос информации возможен как в устной, так и в письменной форме. Запрашиваемую информацию обязаны предоставлять руководители указанных органов, организаций и объединений, их заместители, работники пресс-служб либо другие уполномоченные лица в пределах их компетенции.

Статья 40. Отказ и отсрочка в предоставлении информации

Отказ в предоставлении запрашиваемой информации возможен, только если она содержит сведения, составляющие государственную, коммерческую или иную специально охраняемую законом тайну. Уведомление об отказе вручается представителю редакции в трехдневный срок со дня получения письменного запроса информации. В уведомлении должны быть указаны:

1) причины, по которым запрашиваемая информация не может быть отделена от сведений, составляющих специально охраняемую законом тайну;

2) должностное лицо, отказывающее в предоставлении информации;

3) дата принятия решения об отказе.

Наиболее существенно здесь то, что этим законом редакциям СМИ предоставляется право запрашивать информацию о деятельности государственных органов и организаций, общественных объединений, должностных лиц, и отказ в предоставлении информации возможен только в том случае, если она содержит государственную, коммерческую или иную специально охраняемую законом тайну. Иное будет наказуемо в судебном порядке.

В 1993 г. был издан Указ Президента РФ «О дополнительных гарантиях права граждан на информацию» (от 31.12.1993 № 2334), провозгласивший принцип информационной открытости деятельности государственных органов, организаций и предприятий, общественных объединений, должностных лиц. Этот очень важный указ позволяет гражданам получать беспрепятственно любую информацию о деятельности любых государственных органов без объяснения мотивов такого запроса. Ввиду его важности приведем также отдельные наиболее важные положения этого указа.

«Исходя из того, что право на информацию является одним из фундаментальных прав человека; в целях обеспечения свободы получения гражданами информации о деятельности органов законодательной, исполнительной и судебной власти; основываясь на пункте 4 статьи 29 и пункте 2 статьи 80 Конституции Российской Федерации, постановляю:

3. Деятельность государственных органов, организаций и предприятий, общественных объединений, должностных лиц осуществляется на принципах информационной открытости, что выражается:

- в доступности для граждан информации, представляющей общественный интерес или затрагивающей личные интересы граждан;

- в систематическом информировании граждан о предполагаемых или принятых решениях;

- в осуществлении гражданами контроля за деятельностью государственных органов, организаций и предприятий, общественных объединений, должностных лиц и принимаемыми ими решениями, связанными с соблюдением, охраной и защитой прав и законных интересов граждан.

4. Установить, что в информационных программах государственных телерадиовещательных компаний до сведения граждан в обязательном порядке доводятся основные положения правовых актов и решений государственных органов по основным вопросам внутренней и внешней политики в день их выпуска.

5. Государственным телерадиовещательным компаниям создать циклы передач (программы), разъясняющие деятельность федеральных органов законодательной, исполнительной и судебной власти, существо принимае-

мых решений с привлечением к работе над этими программами ведущих специалистов, экспертов, разработчиков соответствующих документов.

Установить, что объем и периодичность выпуска указанных программ определяется руководителями государственных телерадиовещательных компаний самостоятельно.

6. Деятельность федеральных органов законодательной, исполнительной и судебной власти освещается в программах государственной телерадиовещательных компаний в равном объеме.

Контроль за объективностью освещения такой деятельности осуществляется Судебной палатой по информационным спорам при Президенте Российской Федерации.

7. Руководствуясь пунктом 4 статьи 15 Конституции Российской Федерации, при освещении деятельности Федерального собрания средствами массовой информации исходить из Резолюции Парламентской ассамблеи Совета Европы № 820 (1984) об отношениях парламентов государств со средствами массовой информации (Собрание актов Президента и Правительства Российской Федерации, 1993, № 15, ст. 1340), в том числе имея в виду ограниченность каналов телевидения:

- доводить содержание выступлений депутатов в прениях по законопроектам до сведения их избирателей, как правило, через печатные средства массовой информации;

- публиковать большее число статей просветительного характера о парламентской деятельности.

Распространить положения Резолюции № 820 (1984) на отношения других федеральных органов государственной власти со средствами массовой информации, в том числе установить одинаковые для всех федеральных органов следующие принципы проведения прямых теле- и радиотрансляций или вещания в записи:

- необходимость получения телерадиовещательной компанией согласия на проведение трансляций с заседания соответствующего федерального органа государственной власти;

- заблаговременное извещение телерадиовещательных компаний о предполагаемом рассмотрении наиболее важных вопросов, представляющих общественный интерес;

- выбор времени (объема) вещания и его формы (прямое или в записи) телерадиовещательной компанией.

8. Федеральной службе России по телевидению и радиовещанию усилить контроль за строгим соблюдением телерадиовещательными организациями Закона Российской Федерации «О средствах массовой информации».

9. Указ вступает в силу с момента подписания.»

Существенные права пользователям государственных информационных ресурсов дает принятый 20 февраля 1995 г. Федеральный закон «Об

информации, информатизации и защите информации», (принят Государственной Думой 25 января 1995 г.), который закрепил право доступа физических и юридических лиц к государственным информационным ресурсам. В данном законе особо оговаривается, что за исключением специально предусмотренных законом случаев владельцы информационных ресурсов не вправе требовать обоснования необходимости получения запрашиваемой информации. При этом все пользователи информации (граждане, общественные объединения, органы государственной власти и органы местного самоуправления) наделяются равными правами доступа к государственным информационным ресурсам. Ниже приведены отдельные статьи этого закона.

Статья 1. Сфера действия настоящего Федерального закона

1. Настоящий Федеральный закон регулирует отношения, возникающие:

- при формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителю документированной информации;
- создании и использовании информационных технологий и средств их обеспечения;
- защите информации, прав субъектов, участвующих в информационных процессах и информатизации.

Статья 3. Обязанности государства в сфере формирования информационных ресурсов и информатизации

1. Государственная политика в сфере формирования информационных ресурсов и информатизации направлена на создание условий для эффективного и качественного информационного обеспечения решения стратегических и оперативных задач социального и экономического развития Российской Федерации.

2. Основными направлениями государственной политики в сфере информатизации являются:

- обеспечение условий для развития и защиты всех форм собственности на информационные ресурсы;
- создание условий для качественного и эффективного информационного обеспечения граждан, органов государственной власти, органов местного самоуправления, организаций и общественных объединений на основе государственных информационных ресурсов;
- обеспечение национальной безопасности в сфере информатизации, а также обеспечение реализации прав граждан, организаций в условиях информатизации.

Статья 12. Реализация права на доступ к информации из информационных ресурсов

1. Пользователи – граждане, органы государственной власти, органы местного самоуправления, организации и общественные объединения –

обладают равными правами на доступ к государственным информационным ресурсам и не обязаны обосновывать перед владельцем этих ресурсов необходимость получения запрашиваемой ими информации. Исключение составляет информация с ограниченным доступом.

Доступ физических и юридических лиц к государственным информационным ресурсам является основой осуществления общественного контроля за деятельностью органов государственной власти, органов местного самоуправления, общественных, политических и иных организаций, а также за состоянием экономики, экологии и других сфер общественной жизни.

2. Владельцы информационных ресурсов обеспечивают пользователей (потребителей) информацией из информационных ресурсов на основе законодательства, уставов указанных органов и организаций, положений о них, а также договоров на услуги по информационному обеспечению.

3. Порядок получения пользователем информации (указание места, времени, ответственных должностных лиц, необходимых процедур) определяет собственник или владелец информационных ресурсов с соблюдением требований, установленных настоящим Федеральным законом.

Перечни информации и услуг по информационному обеспечению, сведения о порядке и условиях доступа к информационным ресурсам владельцы информационных ресурсов и информационных систем предоставляют пользователям бесплатно.

4. Органы государственной власти и организации, ответственные за формирование и использование информационных ресурсов, обеспечивают условия для оперативного и полного предоставления пользователю документированной информации в соответствии с обязанностями, установленными уставами (положениями) этих органов и организаций.

Статья 13. Гарантии предоставления информации

1. Органы государственной власти и органы местного самоуправления создают доступные для каждого информационные ресурсы по вопросам деятельности этих органов и подведомственных им организаций, а также в пределах своей компетенции осуществляют массовое информационное обеспечение пользователей по вопросам прав, свобод и обязанностей граждан, их безопасности и другим вопросам, представляющим общественный интерес.

2. Отказ в доступе к информационным ресурсам, предусмотренным в пункте 1 настоящей статьи, может быть обжалован в суде.

3. Комитет при Президенте Российской Федерации по политике информатизации организует регистрацию всех информационных ресурсов, информационных систем и публикацию сведений о них для обеспечения права граждан на доступ к информации.

Статья 14. Доступ граждан и организаций к информации о них

1. Граждане и организации имеют право на доступ к документированной информации о них, на уточнение этой информации в целях обеспечения ее полноты и достоверности, имеют право знать, кто и в каких целях использует или использовал эту информацию. Ограничение доступа граждан и организаций к информации о них допустимо лишь на основаниях, предусмотренных федеральными законами.

2. Владелец документированной информации о гражданах обязан предоставить информацию бесплатно по требованию тех лиц, которых она касается. Ограничения возможны лишь в случаях, предусмотренных законодательством Российской Федерации.

3. Субъекты, представляющие информацию о себе для комплектования информационных ресурсов на основании статей 7 и 8 настоящего Федерального закона, имеют право бесплатно пользоваться этой информацией.

4. Отказ владельца информационных ресурсов субъекту в доступе к информации о нем может быть обжалован в судебном порядке.

Статья 24. Защита права на доступ к информации

1. Отказ в доступе к открытой информации или предоставление пользователям заведомо недостоверной информации могут быть обжалованы в судебном порядке.

Неисполнение или ненадлежащее исполнение обязательств по договору поставки, купли-продажи, по другим формам обмена информационными ресурсами между организациями рассматриваются арбитражным судом.

Во всех случаях лица, которым отказано в доступе к информации, и лица, получившие недостоверную информацию, имеют право на возмещение понесенного ими ущерба.

2. Суд рассматривает споры о необоснованном отнесении информации к категории информации с ограниченным доступом, иски о возмещении ущерба в случаях необоснованного отказа в предоставлении информации пользователям или в результате других нарушений прав пользователей.

3. Руководители, другие служащие органов государственной власти, организаций, виновные в незаконном ограничении доступа к информации и нарушении режима защиты информации, несут ответственность в соответствии с уголовным, гражданским законодательством и законодательством об административных правонарушениях.

Право граждан на доступ к информации защищено также статьей 5.39 Кодекса об административных правонарушениях от 30.12.2003 (ред. от 23.12.2003). Статья устанавливает ответственность за неправомерный отказ в предоставлении гражданину собранных в установленном порядке документов, материалов, непосредственно затрагивающих права и свободы гражданина, либо несвоевременное предоставление таких документов и материалов, непредоставление иной информации в случаях, предусмот-

ренных законом, либо предоставление гражданину неполной или заведомо недостоверной информации. На должностных лиц, признанных виновными в совершении указанных противоправных деяний, возлагается ответственность в виде административного штрафа в размере от пяти до десяти минимальных размеров оплаты труда.

Наиболее часто запрашивается экологическая информация. Кодекс предусматривает ответственность за сокрытие или искажение экологической информации:

Статья 8.5. Сокрытие или искажение экологической информации

Сокрытие, умышленное искажение или несвоевременное сообщение полной и достоверной информации о состоянии окружающей природной среды и природных ресурсов, об источниках загрязнения окружающей природной среды и природных ресурсов или иного вредного воздействия на окружающую природную среду и природные ресурсы, о радиационной обстановке, а равно искажение сведений о состоянии земель, водных объектов и других объектов окружающей природной среды лицами, обязанными сообщать такую информацию, влечет наложение административного штрафа на граждан в размере от пяти до десяти минимальных размеров оплаты труда; на должностных лиц – от десяти до двадцати минимальных размеров оплаты труда; на юридических лиц – от ста до двухсот минимальных размеров оплаты труда.

Также федеральные законы «Об охране окружающей среды» от 10.01.2002 № 7-ФЗ и «О санитарно-эпидемиологическом благополучии населения» от 30.03.1999 № 52-ФЗ предусматривают право граждан на достоверную информацию о состоянии окружающей среды, санитарно-эпидемиологической обстановке, качестве и безопасности продукции производственно-технического назначения, пищевых продуктов, товаров для личных и бытовых нужд, потенциальной опасности для здоровья человека выполняемых работ и оказываемых услуг.

Так, в Федеральном законе «О гидрометеорологической службе» принятом Государственной Думой 3 июля 1998 г. и одобренном Советом Федерации 9 июля 1998 г. есть главы и статьи, прямо указывающие на обязанность должностных лиц информировать население о состоянии экологии.

Статья 14. Категории доступа к информации о состоянии окружающей природной среды, ее загрязнении и информационной продукции

1. Информация о состоянии окружающей природной среды, ее загрязнении и информационная продукция являются открытыми и общедоступными, за исключением информации, отнесенной законодательством Российской Федерации к категории ограниченного доступа.

Статья 16. Порядок предоставления информации о состоянии окружающей природной среды, ее загрязнении юридическими и физическими лицами

1. Юридические лица независимо от организационно-правовых форм и физические лица, осуществляющие сбор информации о состоянии окружающей природной среды, ее загрязнении, обязаны предоставлять данную информацию в специально уполномоченный федеральный орган исполнительной власти в области гидрометеорологии и смежных с ней областях в порядке, установленном Правительством Российской Федерации.

Статья 17. Условия предоставления пользователям (потребителям) информации о состоянии окружающей природной среды, ее загрязнении и информационной продукции

1. Информация о состоянии окружающей природной среды, ее загрязнении и информационная продукция предоставляются пользователям (потребителям) бесплатно, а также на основе договоров в соответствии с настоящим Федеральным законом и законодательством Российской Федерации об охране окружающей природной среды.

2. Информация общего назначения доводится до пользователей (потребителей) в виде текстов в письменной форме, таблиц и графиков по сетям электрической и почтовой связи, через средства массовой информации в режиме регулярных сообщений или по запросам пользователей (потребителей).

4. Специально уполномоченный федеральный орган исполнительной власти в области гидрометеорологии и смежных с ней областях обязан информировать пользователей (потребителей) о составе предоставляемой информации о состоянии окружающей природной среды, ее загрязнении, о формах доведения данной информации и об организациях, осуществляющих информационное обслуживание пользователей (потребителей).

Граждане имеют право на доступ к информации в самых разнообразных других областях. Например, граждане вправе иметь достоверную и полную информацию о товарах, находящихся в продаже, о состоянии экологической среды, по избирательной кампании. Право на это закреплено также в самых различных законах и законодательных актах. Так, право на информацию о товарах закреплено в гражданском кодексе Российской Федерации, статья 495, где регламентируются обязанности продавца по информации о товаре.

Статья 495. Предоставление покупателю информации о товаре

1. Продавец обязан предоставить покупателю необходимую и достоверную информацию о товаре, предлагаемом к продаже, соответствующую установленным законом, иными правовыми актами и обычно предъявляемым в розничной торговле требованиям к содержанию и способам предоставления такой информации.

2. Покупатель вправе до заключения договора розничной купли-продажи осмотреть товар, потребовать проведения в его присутствии проверки свойств или демонстрации использования товара, если это не исключено ввиду характера товара и не противоречит правилам, принятым в розничной торговле.

3. Если покупателю не предоставлена возможность незамедлительно получить в месте продажи информацию о товаре, указанную в пунктах 1 и 2 настоящей статьи, то он вправе потребовать от продавца возмещения убытков, вызванных необоснованным уклонением от заключения договора розничной купли-продажи (п. 4 ст. 445), а если договор заключен, в разумный срок отказаться от исполнения договора, потребовать возврата уплаченной за товар суммы и возмещения других убытков.

4. Продавец, не предоставивший покупателю возможность получить соответствующую информацию о товаре, несет ответственность и за недостатки товара, возникшие после его передачи покупателю, в отношении которых покупатель докажет, что они возникли в связи с отсутствием у него такой информации.

Кроме того, правительство России 12 февраля 2003 г. приняло Постановление № 98 «Об обеспечении доступа к информации о деятельности Правительства Российской Федерации и федеральных органов исполнительной власти». Согласно Постановлению федеральные органы исполнительной власти обязаны обеспечить доступ граждан и организаций к информации о своей деятельности, за исключением сведений, отнесенных к информации ограниченного доступа, путем создания информационных ресурсов в соответствии с перечнем, утвержденным настоящим Постановлением, и размещения их в информационных системах общего пользования.

Следует иметь в виду, что нормативные правовые акты, закрепляющие права граждан по производству, распространению, поиску, получению и передаче информации, принимаются и на уровне субъектов Российской Федерации.

Так, в Волгоградской области принят Закон от 28 января 2003 г. № 782-ОД «О порядке предоставления информации органами государственной власти Волгоградской области». Он во многом повторяет положения принятого в 2002 г. Закона Калининградской области «О порядке предоставления информации органами государственной власти Калининградской области». При этом калининградский закон содержит отдельную главу, в которой устанавливается порядок предоставления документов и материалов на основании запроса.

Владимирская область пошла по пути законодательного закрепления порядка доступа к информации, касающейся отдельных направлений деятельности органов власти. Так, в 2003 г. был принят Закон «О порядке информирования граждан, их объединений и юридических лиц о градостроительной деятельности на территории Владимирской области».

Закон города Москвы от 24 октября 2001 г. «Об информационных ресурсах и информатизации города Москвы» определяет перечень информационных ресурсов, находящихся в собственности г. Москвы, их правовой режим, а также порядок их формирования.

Постановление Правительства Москвы от 7 октября 2003 г. «Об обеспечении доступности информации о деятельности Правительства Москвы, городских органов исполнительной власти и городских организаций» утверждает перечень предприятий города, для которых создание и ведение информационных ресурсов является обязательным, также утверждается перечень сведений о деятельности Правительства Москвы и комплексов городского управления, подлежащих обязательному размещению в общедоступных информационных ресурсах в сети Интернет.

2.3. Ответственность за нарушение прав на информацию

За нарушение прав на информацию законодательство Российской Федерации предусматривает достаточно жесткие меры наказания. Так отдельные статьи Уголовного кодекса РФ, вступившие в силу в мае 1996 г., предусматривают солидные штрафы, обязательные работы и вплоть до тюремного заключения.

Статья 137. Нарушение неприкосновенности частной жизни

1. 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 наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо обязательными работами на срок от ста двадцати до ста восьмидесяти часов, либо исправительными работами на срок до одного года, либо арестом на срок до четырех месяцев, либо лишением свободы на срок до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

2. Те же деяния, совершенные лицом с использованием своего служебного положения, наказываются штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет, либо арестом на срок до шести месяцев, либо лишением свободы на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет.

Статья 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений

1. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан наказывается штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев, либо обязательными работами на срок от ста двадцати до ста восьмидесяти часов, либо исправительными работами на срок до одного года.

2. То же деяние, совершенное лицом с использованием своего служебного положения или специальных технических средств, предназначенных для негласного получения информации, наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо арестом на срок до четырех месяцев, либо лишением свободы на срок до четырех лет.

3. Незаконные производство, сбыт или приобретение специальных технических средств, предназначенных для негласного получения информации, наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо ограничением свободы на срок до трех лет, либо лишением свободы на срок до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

Аналогичную роль для банковской и коммерческой тайны играет статья 183 УК РФ.

Статья 183. Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну

1. Собирание сведений, составляющих коммерческую, налоговую или банковскую тайну, путем похищения документов, подкупа или угроз, а равно иным незаконным способом наказывается штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного до шести месяцев, либо исправительными работами на срок до одного года, либо лишением свободы на срок до двух лет.

2. Незаконные разглашение или использование сведений, составляющих коммерческую, налоговую или банковскую тайну, без согласия их владельца лицом, которому она была доверена или стала известна по службе или работе, наказываются штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного

за период до одного года с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо исправительными работами на срок до двух лет, либо лишением свободы на срок до трех лет.

3. Те же деяния, причинившие крупный ущерб или совершенные из корыстной заинтересованности, наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет либо лишением свободы на срок до пяти лет.

4. Деяния, предусмотренные частями второй или третьей настоящей статьи, повлекшие тяжкие последствия, наказываются лишением свободы на срок до десяти лет.

В разделе IX "Преступления против общественной безопасности" имеется глава 28. "Преступления в сфере компьютерной информации", которая содержит три статьи: 272, 273, 274.

Статья 272. Неправомерный доступ к компьютерной информации

1 Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, наказывается штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

2 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, наказывается штрафом в размере от пятисот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от пяти до восьми месяцев, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ

1. 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 – наказываются лишением свободы на срок до трех лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев.

2. Те же деяния, повлекшие по неосторожности тяжкие последствия, наказываются лишением свободы на срок от трех до семи лет.

Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

1. 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, наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет.

2. То же деяние, повлекшее по неосторожности тяжкие последствия, наказывается лишением свободы на срок до четырех лет.

Основополагающим среди российских законов, посвященных вопросам информационной безопасности, следует считать закон "Об информации, информатизации и защите информации" от 20 февраля 1995 г. № 24-ФЗ (принят Государственной Думой 25 января 1995 г.). В нем даются основные определения и намечаются направления развития законодательства в данной области.

Вот некоторые из этих определений:

- информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;
- документированная информация (документ) – зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать;
- информационные процессы – процессы сбора, обработки, накопления, хранения, поиска и распространения информации;
- информационная система – организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы;
- информационные ресурсы – отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах);
- информация о гражданах (персональные данные) – сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность;

• конфиденциальная информация – документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации;

• пользователь (потребитель) информации – субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею.

Обратим внимание на гибкость определения конфиденциальной информации, которая не сводится к сведениям, составляющим государственную тайну, а также на понятие персональных данных, закладывающее основу защиты последних.

Статья 21. Защита информации

1. Защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу.

Режим защиты информации устанавливается:

– в отношении сведений, отнесенных к государственной тайне, – уполномоченными органами на основании Закона Российской Федерации "О государственной тайне";

– в отношении конфиденциальной документированной информации – собственником информационных ресурсов или уполномоченным лицом на основании настоящего Федерального закона;

– в отношении персональных данных – федеральным законом.

4. Организации, обрабатывающие информацию с ограниченным доступом, которая является собственностью государства, создают специальные службы, обеспечивающие защиту информации.

Статья 22. Права и обязанности субъектов в области защиты информации

1. Собственник документов, массива документов, информационных систем или уполномоченные им лица в соответствии с настоящим Федеральным законом устанавливают порядок предоставления пользователю информации с указанием места, времени, ответственных должностных лиц, а также необходимых процедур и обеспечивают условия доступа пользователей к информации.

2. Владелец документов, массива документов, информационных систем обеспечивает уровень защиты информации в соответствии с законодательством Российской Федерации.

3. Риск, связанный с использованием несертифицированных информационных систем и средств их обеспечения, лежит на собственнике (владельце) этих систем и средств.

Риск, связанный с использованием информации, полученной из несертифицированной системы, лежит на потребителе информации.

4. Собственник документов, массива документов, информационных систем может обращаться в организации, осуществляющие сертификацию средств защиты информационных систем и информационных ресурсов, для проведения анализа достаточности мер защиты его ресурсов и систем и получения консультаций.

5. Владелец документов, массива документов, информационных систем обязан оповещать собственника информационных ресурсов и (или) информационных систем о всех фактах нарушения режима защиты информации.

Статья 23. Защита прав субъектов в сфере информационных процессов и информатизации

1. Защита прав субъектов в сфере формирования информационных ресурсов, пользования информационными ресурсами, разработки, производства и применения информационных систем, технологий и средств их обеспечения осуществляется в целях предупреждения правонарушений, пресечения неправомерных действий, восстановления нарушенных прав и возмещения причиненного ущерба.

2. Защита прав субъектов в указанной сфере осуществляется судом, арбитражным судом, третейским судом с учетом специфики правонарушений и нанесенного ущерба.

3. За правонарушения при работе с документированной информацией органы государственной власти, организации и их должностные лица несут ответственность в соответствии с законодательством Российской Федерации и субъектов Российской Федерации.

4. Ответственность за нарушения международных норм и правил в области формирования и использования информационных ресурсов, создания и использования информационных систем, технологий и средств их обеспечения возлагается на органы государственной власти, организации и граждан в соответствии с договорами, заключенными ими с зарубежными фирмами и другими партнерами с учетом международных договоров, ратифицированных Российской Федерацией.

Кроме приведенных законов, также существенную роль сейчас играет Федеральный закон "О персональных данных", вступивший в силу 26 января 2007 г. В этом законе сформулированы требования по защите персональных данных. Важно отметить, что требования данного закона являются обязательными и для коммерческих, и для государственных организаций. При этом, согласно статье 25, информационные системы должны быть приведены в соответствие с требованиями настоящего Федерального закона не позднее 1 января 2010 г.

Наиболее важные статьи его указывают на следующее.

Статья 5. Принципы обработки персональных данных

1. Обработка персональных данных должна осуществляться на основе принципов:

1) законности целей и способов обработки персональных данных и добросовестности;

2) соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям оператора;

3) соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;

4) достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;

5) недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.

2. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъект персональных данных, не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

Статья 6. Условия обработки персональных данных

1. Обработка персональных данных может осуществляться оператором с согласия субъектов персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи.

2. Согласие субъекта персональных данных, предусмотренное частью 1 настоящей статьи, не требуется в следующих случаях:

1) обработка персональных данных осуществляется на основании федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора;

2) обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных;

3) обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;

4) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

5) обработка персональных данных необходима для доставки почтовых отправлений организациями почтовой связи, для осуществления опе-

раторами электросвязи расчетов с пользователями услуг связи за оказанные услуги связи, а также для рассмотрения претензий пользователей услугами связи;

6) обработка персональных данных осуществляется в целях профессиональной деятельности журналиста либо в целях научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

7) осуществляется обработка персональных данных, подлежащих опубликованию в соответствии с федеральными законами, в том числе персональных данных лиц, замещающих государственные должности, должности государственной гражданской службы, персональных данных кандидатов на выборные государственные или муниципальные должности.

Статья 7. Конфиденциальность персональных данных

1. Операторами и третьими лицами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных, за исключением случаев, предусмотренных частью 2 настоящей статьи.

2. Обеспечение конфиденциальности персональных данных не требуется:

1) в случае обезличивания персональных данных;

2) в отношении общедоступных персональных данных.

Статья 9. Согласие субъекта персональных данных на обработку своих персональных данных

1. Субъект персональных данных принимает решение о предоставлении своих персональных данных и дает согласие на их обработку своей волей и в своем интересе, за исключением случаев, предусмотренных частью 2 настоящей статьи. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных.

2. Настоящим Федеральным законом и другими федеральными законами предусматриваются случаи обязательного предоставления субъектом персональных данных своих персональных данных в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

3. Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных, а в случае обработки общедоступных персональных данных обязанность доказывания того, что обрабатываемые персональные данные являются общедоступными, возлагается на оператора.

4. В случаях, предусмотренных настоящим Федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. Письменное согласие субъекта персональных данных на обработку своих персональных данных должно включать в себя:

1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

2) наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных;

3) цель обработки персональных данных;

4) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

5) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

6) срок, в течение которого действует согласие, а также порядок его отзыва.

5. Для обработки персональных данных, содержащихся в согласии в письменной форме субъекта на обработку его персональных данных, дополнительное согласие не требуется.

6. В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает в письменной форме законный представитель субъекта персональных данных.

7. В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают в письменной форме наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни.

Статья 10. Специальные категории персональных данных

1. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением случаев, предусмотренных частью 2 настоящей статьи.

2. Обработка указанных в части 1 настоящей статьи специальных категорий персональных данных допускается в случаях, если:

1) субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;

2) персональные данные являются общедоступными;

3) персональные данные относятся к состоянию здоровья субъекта персональных данных и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц, и получение согласия субъекта персональных данных невозможно.

Статья 11. Биометрические персональные данные

1. Сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность (биометри-

ческие персональные данные), могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи.

Кроме того, стоит отметить, что Федеральный закон "О персональных данных" не является единственным нормативно-правовым актом, регламентирующим положение о персональных данных. Существует ряд документов, к которым относятся: Постановление правительства РФ от 17 ноября 2007 г. № 781 "Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных" и нормативные и методические документы ФСТЭК и ФСБ России. Согласно этим документам, обеспечение безопасности персональных данных является неотъемлемой и обязательной частью работ по созданию и поддержке информационных систем.

Работа субъектов с информацией может также иметь ограничения, связанные со специальными задачами информационной безопасности. Такие ограничения могут иметь место в соответствии с законом "О лицензировании отдельных видов деятельности" от 8 августа 2001 г. № 128-ФЗ (Принят Государственной Думой 13 июля 2001 г.).

Приведем основные определения этого закона.

Лицензия – специальное разрешение на осуществление конкретного вида деятельности при обязательном соблюдении лицензионных требований и условий, выданное лицензирующим органом юридическому лицу или индивидуальному предпринимателю.

Лицензируемый вид деятельности – вид деятельности, на осуществление которого на территории Российской Федерации требуется получение лицензии в соответствии с настоящим Федеральным законом.

Лицензирование – мероприятия, связанные с предоставлением лицензий, переоформлением документов, подтверждающих наличие лицензий, приостановлением и возобновлением действия лицензий, аннулированием лицензий и контролем лицензирующих органов за соблюдением лицензиатами при осуществлении лицензируемых видов деятельности соответствующих лицензионных требований и условий.

Лицензирующие органы – федеральные органы исполнительной власти, органы исполнительной власти субъектов Российской Федерации, осуществляющие лицензирование в соответствии с настоящим Федеральным законом.

Лицензиат – юридическое лицо или индивидуальный предприниматель, имеющие лицензию на осуществление конкретного вида деятельности.

Статья 12 Закона устанавливает перечень видов деятельности, на осуществление которых требуются лицензии. Наиболее важные в сфере защиты информации:

– распространение шифровальных (криптографических) средств;

– техническое обслуживание шифровальных (криптографических) средств;

– техническое обслуживание шифровальных (криптографических) средств;

– предоставление услуг в области шифрования информации;

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

– выдача сертификатов ключей электронных цифровых подписей, регистрация владельцев электронных цифровых подписей, оказание услуг, связанных с использованием электронных цифровых подписей и подтверждением подлинности электронных цифровых подписей;

– выявление 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);

– разработка и (или) производство средств защиты конфиденциальной информации;

– техническая защита конфиденциальной информации;

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

Необходимо учитывать, что, согласно статье 1, действие данного Закона не распространяется на следующие виды деятельности:

– деятельность, связанная с защитой государственной тайны;

– деятельность в области связи;

– образовательная деятельность.

Основными лицензирующими органами в области защиты информации являются Федеральное агентство правительственной связи и информации (ФАПСИ) и Гостехкомиссия России. ФАПСИ ведает всем, что связано с криптографией, Гостехкомиссия лицензирует деятельность по защите конфиденциальной информации. Эти же организации возглавляют работы по сертификации средств соответствующей направленности. Кроме того, ввоз и вывоз средств криптографической защиты информации (шифровальной техники) и нормативно-технической документации к ней может осуществляться исключительно на основании лицензии Министерства внешних экономических связей Российской Федерации, выдаваемой на основании решения ФАПСИ. Все эти вопросы регламентированы соответ-

ствующими указами Президента и постановлениями Правительства РФ, которые здесь перечисляться не будут.

Законодательно также защищаются в любой форме объекты авторского права. Так, произведение, размещённое в Интернете, отвечает всем признакам объекта авторского права: оно, во-первых, является результатом творческой деятельности, независимо от назначения и достоинства произведения, а также от способа его выражения; во-вторых, закреплено в объективной форме – в письменной форме (текстовые файлы и web-страницы) и в форме изображений.

Российское законодательство отвечает всем принципам международных соглашений об авторском праве. Оно включает разнообразные формы его защиты. В самом общем виде интересы собственников информации защищает Конституция Российской Федерации, ст. 44-1, в которой указывается, что "Каждому гарантируется свобода литературного, художественного, научного, технического и других видов творчества, преподавания. Интеллектуальная собственность охраняется законом".

Детально авторское право регулируется Законом РФ от 9 июля 1993 г. «Об авторском праве и смежных правах».

Авторское право – это часть гражданского права, которое регулирует порядок использования произведений литературы, науки и искусства. Объектами авторского права признаются также программы для компьютеров и электронные базы данных.

Охраняемое произведение должно быть результатом творческого труда, продуктом интеллектуальной деятельности человека, оригинальным, отмеченным индивидуальностью автора. Результаты интеллектуальной деятельности называют интеллектуальной собственностью.

Субъектами авторского права, т. е. лицами, обладающими исключительным правом на произведение, считаются прежде всего авторы произведений. Правообладателями также могут быть различные компании, приобретающие право на коммерческое использование произведения, или наследники автора.

Авторские права делятся на личные неимущественные и имущественные права. Из неимущественных прав автору принадлежат:

– право авторства – право признаваться автором произведения;

– право на имя – право использовать или разрешать использовать произведение под именем автора или его псевдонимом;

– право на обнародование – право обнародовать или разрешать обнародовать произведение в любой форме;

– право на защиту репутации автора, право на защиту произведения, включая его название, от всякого искажения или иного посягательства, способного нанести ущерб чести и достоинству автора.

Личные неимущественные права принадлежат автору независимо от его имущественных прав и сохраняются за ним, например, даже в случае передачи исключительных прав на публикацию произведения.

К имущественным правам автора относятся:

- право на воспроизведение;
- право на распространение;
- право на импорт;
- право на перевод;
- право па публичный показ;
- право на публичное исполнение;
- право на передачу в эфир;
- право на сообщение для всеобщего сведения по кабелю (т. е. передавать произведение, включая показ, исполнение или передачу в эфир, для всеобщего сведения по кабелю, проводам или с помощью других аналогичных средств).

Авторское право действует в течение всей жизни автора и 50 лет после его смерти. По истечении срока охраны произведение переходит в общественное достояние, его можно использовать, не спрашивая разрешения. Право авторства, право на имя и право на защиту репутации автора охраняются бессрочно.

За нарушение авторских прав наступает гражданская, уголовная и административная ответственность, предусмотренная в Уголовном кодексе, ст. 146.

Статья 146. Нарушение авторских и смежных прав

1. Присвоение авторства (плагиат), если это деяние причинило крупный ущерб автору или иному правообладателю, наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо арестом на срок от трех до шести месяцев.

2. 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, наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо лишением свободы на срок до двух лет.

3. Деяния, предусмотренные частью второй настоящей статьи, если они совершены:

б) группой лиц по предварительному сговору или организованной группой;

в) в особо крупном размере;

г) лицом с использованием своего служебного положения,

наказываются лишением свободы на срок до пяти лет со штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет либо без такового.

Объектами авторского права признаются также программы для компьютеров и электронные базы данных. Сегодня компьютерные программы (редакторы, компиляторы, базы данных) приобрели значение товарной продукции. Например, база данных – это объективная форма представления и организации совокупности данных (статьи, расчёты и пр.), систематизированных таким образом, чтобы они могли быть найдены и обработаны с помощью ЭВМ.

Авторское право на компьютерные программы охраняет Закон РФ «О правовой охране программ для электронных вычислительных машин и баз данных» от 23 сентября 1992 г. Закон признает авторское право на любые программы для ЭВМ и базы данных.

Статья 3. Объект правовой охраны

1. Авторское право распространяется на любые программы для ЭВМ и базы данных, как выпущенные, так и не выпущенные в свет, представленные в объективной форме, независимо от их материального носителя, назначения и достоинства.

2. Авторское право распространяется на программы для ЭВМ и базы данных, являющиеся результатом творческой деятельности автора (соавторов). Творческий характер деятельности автора (соавторов) предполагается до тех пор, пока не доказано обратное.

3. Предоставляемая настоящим Законом правовая охрана распространяется на все виды программ для ЭВМ (в том числе на операционные системы и программные комплексы), которые могут быть выражены на любом языке и в любой форме, включая исходный текст и объектный код.

4. Предоставляемая настоящим Законом правовая охрана распространяется на базы данных, представляющие собой результат творческого труда по подбору и организации данных. Базы данных охраняются независимо от того, являются ли данные, на которых они основаны или которые они включают, объектами авторского права.

Независимо от формы своего выражения программы и базы данных защищаются так же, как и произведения литературы.

В отличие от материальной собственности, объекты интеллектуальной собственности, в том числе и компьютерные программы, покупатели могут использовать лишь на особых условиях, устанавливаемых автором. При этом в собственность покупателя переходит только носитель информации, например компакт-диск, на котором программа записана. Однако покупатель вправе без согласия правообладателя и без выплаты ему до-

полнительного вознаграждения изготавливать копии программы при условии, что они предназначены исключительно для архивных целей.

Экземпляры произведения или программы, изготовление или распространение которых влечёт за собой нарушение авторских прав, называются по закону контрафактными (от фр. *contrefacon* – «подделка»). В обиходе же часто употребляется термин «пиратская копия» (от англ. *Piracy* – «нарушение авторского права»). Обладатели авторских прав могут обратиться за защитой в суд и вправе требовать от нарушителя признания прав автора; восстановления положения, существовавшего до нарушения права, и прекращения действий, нарушающих право или создающих угрозу его нарушения; возмещения убытков, включая упущенную выгоду; взыскания дохода, полученного нарушителем вследствие нарушения авторских и смежных прав; выплаты компенсации в сумме от 10 до 50 тысяч минимальных размеров оплаты труда (МРОТ). Контрафактные экземпляры произведений подлежат конфискации и уничтожению.

В соответствии со статьями Кодекса Российской Федерации об административных правонарушениях незаконное использование контрафактных экземпляров влечёт наложение на граждан административного штрафа в размере от 15 до 20 МРОТ.

Этот же кодекс предусматривает наказание за незаконную работу с защитой информации.

Статья 13.11. Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)

Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) влечет предупреждение или наложение административного штрафа на граждан в размере от трех до пяти минимальных размеров оплаты труда; на должностных лиц – от пяти до десяти минимальных размеров оплаты труда; на юридических лиц – от пятидесяти до ста минимальных размеров оплаты труда.

Статья 13.12. Нарушение правил защиты информации

1. Нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну), влечет наложение административного штрафа на граждан в размере от трех до пяти минимальных размеров оплаты труда; на должностных лиц - от пяти до десяти минимальных размеров оплаты труда; на юридических лиц - от пятидесяти до ста минимальных размеров оплаты труда.

2. Использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключени-

ем средств защиты информации, составляющей государственную тайну), влечет наложение административного штрафа на граждан в размере от пяти до десяти минимальных размеров оплаты труда с конфискацией несертифицированных средств защиты информации или без таковой; на должностных лиц – от десяти до двадцати минимальных размеров оплаты труда; на юридических лиц – от ста до двухсот минимальных размеров оплаты труда с конфискацией несертифицированных средств защиты информации или без таковой.

3. Нарушение условий, предусмотренных лицензией на проведение работ, связанных с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну, влечет наложение административного штрафа на должностных лиц в размере от двадцати до тридцати минимальных размеров оплаты труда; на юридических лиц – от ста пятидесяти до двухсот минимальных размеров оплаты труда.

4. Использование несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну, влечет наложение административного штрафа на должностных лиц в размере от тридцати до сорока минимальных размеров оплаты труда; на юридических лиц – от двухсот до трехсот минимальных размеров оплаты труда с конфискацией несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну, или без таковой.

Статья 13.13. Незаконная деятельность в области защиты информации

1. Занятие видами деятельности в области защиты информации (за исключением информации, составляющей государственную тайну) без получения в установленном порядке специального разрешения (лицензии), если такое разрешение (такая лицензия) в соответствии с федеральным законом обязательно (обязательна), влечет наложение административного штрафа на граждан в размере от пяти до десяти минимальных размеров оплаты труда с конфискацией средств защиты информации или без таковой; на должностных лиц – от двадцати до тридцати минимальных размеров оплаты труда с конфискацией средств защиты информации или без таковой; на юридических лиц – от ста до двухсот минимальных размеров оплаты труда с конфискацией средств защиты информации или без таковой.

2. Занятие видами деятельности, связанной с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну, без лицензии влечет наложение административного штрафа на должностных лиц в

размере от сорока до пятидесяти минимальных размеров оплаты труда; на юридических лиц – от трехсот до четырехсот минимальных размеров оплаты труда с конфискацией созданных без лицензии средств защиты информации, составляющей государственную тайну, или без таковой.

Статья 13.14. Разглашение информации с ограниченным доступом

Разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, влечет наложение административного штрафа на граждан в размере от пяти до десяти минимальных размеров оплаты труда; на должностных лиц – от сорока до пятидесяти минимальных размеров оплаты труда.

Статья 13.16. Воспрепятствование распространению продукции средства массовой информации

Воспрепятствование осуществляемому на законном основании распространению продукции средства массовой информации либо установление незаконных ограничений на розничную продажу тиража периодического печатного издания влечет наложение административного штрафа на граждан в размере от трех до пяти минимальных размеров оплаты труда; на должностных лиц – от пяти до десяти минимальных размеров оплаты труда; на юридических лиц – от пятидесяти до ста минимальных размеров оплаты труда.

Защита государственной тайны также обеспечивается законодательно. Законодательство Российской Федерации о государственной тайне основывается на Конституции Российской Федерации, Законе Российской Федерации "О безопасности", включает Закон "О защите государственной тайны", а также положения других актов законодательства, регулирующих отношения, связанные с защитой государственной тайны.

В Законе "О защите государственной тайны" дается перечень сведений, составляющих государственную тайну.

Государственную тайну составляют:

1) сведения в военной области:

– о содержании стратегических и оперативных планов, документов боевого управления по подготовке и проведению операций, стратегическому, оперативному и мобилизационному развертыванию Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов, предусмотренных Федеральным законом "Об обороне", об их боевой и мобилизационной готовности, о создании и об использовании мобилизационных ресурсов;

– о планах строительства Вооруженных Сил Российской Федерации, других войск Российской Федерации, о направлениях развития вооружения и военной техники, о содержании и результатах выполнения целевых

программ, научно-исследовательских и опытно-конструкторских работ по созданию и модернизации образцов вооружения и военной техники;

– о разработке, технологии, производстве, об объемах производства, о хранении, об утилизации ядерных боеприпасов, их составных частей, делящихся ядерных материалов, используемых в ядерных боеприпасах, о технических средствах и (или) методах защиты ядерных боеприпасов от несанкционированного применения, а также о ядерных энергетических и специальных физических установках оборонного значения;

– о тактико-технических характеристиках и возможностях боевого применения образцов вооружения и военной техники, о свойствах, рецептурах или технологиях производства новых видов ракетного топлива или взрывчатых веществ военного назначения;

– о дислокации, назначении, степени готовности, защищенности режимных и особо важных объектов, об их проектировании, строительстве и эксплуатации, а также об отводе земель, недр и акваторий для этих объектов;

– о дислокации, действительных наименованиях, об организационной структуре, о вооружении, численности войск и состояния их боевого обеспечения, а также о военно-политической и (или) оперативной обстановке;

2) сведения в области экономики, науки и техники:

– о содержании планов подготовки Российской Федерации и ее отдельных регионов к возможным военным действиям, о мобилизационных мощностях промышленности по изготовлению и ремонту вооружения и военной техники, об объемах производства, поставок, о запасах стратегических видов сырья и материалов, а также о размещении, фактических размерах и об использовании государственных материальных резервов;

– об использовании инфраструктуры Российской Федерации в целях обеспечения обороноспособности и безопасности государства;

– о силах и средствах гражданской обороны, о дислокации, предназначении и степени защищенности объектов административного управления, о степени обеспечения безопасности населения, о функционировании транспорта и связи в Российской Федерации в целях обеспечения безопасности государства;

– об объемах, о планах (заданиях) государственного оборонного заказа, о выпуске и поставках (в денежном или натуральном выражении) вооружения, военной техники и другой оборонной продукции, о наличии и наращивании мощностей по их выпуску, о связях предприятий по кооперации, о разработчиках или об изготовителях указанных вооружения, военной техники и другой оборонной продукции;

– о достижениях науки и техники, о научно-исследовательских, об опытно-конструкторских, о проектных работах и технологиях, имеющих важное оборонное или экономическое значение, влияющих на безопасность государства;

– об объемах запасов, добычи, передачи и потребления платины, металлов платиновой группы, природных алмазов, а также об объемах других стратегических видов полезных ископаемых Российской Федерации (по списку, определяемому Правительством Российской Федерации);

3) сведения в области внешней политики и экономики:

– о внешнеполитической, внешнеэкономической деятельности Российской Федерации, преждевременное распространение которых может нанести ущерб безопасности государства;

– о финансовой политике в отношении иностранных государств (за исключением обобщенных показателей по внешней задолженности), а также о финансовой или денежно-кредитной деятельности, преждевременное распространение которых может нанести ущерб безопасности государства;

4) сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности:

– о силах, средствах, об источниках, о методах, планах и результатах разведывательной, контрразведывательной и оперативно-розыскной деятельности, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения;

– о лицах, сотрудничающих или сотрудничавших на конфиденциальной основе с органами, осуществляющими разведывательную, контрразведывательную и оперативно-розыскную деятельность;

– об организации, о силах, средствах и методах обеспечения безопасности объектов государственной охраны, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения;

– о системе президентской, правительственной, шифрованной, в том числе кодированной и засекреченной связи, о шифрах, о разработке, об изготовлении шифров и обеспечении ими, о методах и средствах анализа шифровальных средств и средств специальной защиты, об информационно-аналитических системах специального назначения;

– о методах и средствах защиты секретной информации;

– об организации и о фактическом состоянии защиты государственной тайны;

– о защите Государственной границы Российской Федерации, исключительной экономической зоны и континентального шельфа Российской Федерации;

– о расходах федерального бюджета, связанных с обеспечением обороны, безопасности государства и правоохранительной деятельности в Российской Федерации.

В части международных соглашений в области защиты информации следует указать на Постановление Межпарламентской Ассамблеи государств-участников Содружества Независимых Государств № 19-7 «О мо-

дельном законе "О международном информационном обмене"», в котором в частности указывается:

Статья 1. Цели и сфера действия настоящего Закона

1. Цели настоящего Закона – создание условий для эффективного участия стран СНГ в международном информационном обмене в рамках единого мирового информационного пространства, защита их интересов при международном информационном обмене, защита интересов, прав и свобод физических и юридических лиц при международном информационном обмене.

2. Международный обмен конфиденциальной информацией, массовой информацией осуществляется в порядке, устанавливаемом национальным законодательством.

Статья 3. Объекты и субъекты международного информационного обмена

1. Объекты международного информационного обмена – это документированная информация, информационные ресурсы, информационные продукты, информационные услуги, средства международного информационного обмена.

2. Субъектами международного информационного обмена могут являться: государство, органы государственной власти и органы местного самоуправления, физические и юридические лица, физические и юридические лица иностранных государств, лица без гражданства.

Статья 4. Обязанности государства в сфере международного информационного обмена

Органы государственной власти:

– создают условия для обеспечения государства, муниципальных образований, физических и юридических лиц иностранными информационными продуктами и информационными услугами, в том числе с использованием глобальных информационных сетей;

– обеспечивают своевременное и достаточное пополнение государственных информационных ресурсов иностранными информационными продуктами;

– содействуют внедрению современных информационных технологий, обеспечивающих эффективное участие государства, муниципальных образований, физических и юридических лиц в международном информационном обмене;

– обеспечивают защиту государственных информационных ресурсов государства, муниципальных и частных информационных ресурсов, средств международного информационного обмена и соблюдение правового режима информации;

– стимулируют расширение взаимовыгодного международного информационного обмена документированной информацией и охраняют за-

конные интересы государства, муниципальных образований, физических и юридических лиц;

– создают условия для защиты отечественных собственников и владельцев документированной информации, информационных ресурсов, информационных продуктов, средств международного информационного обмена, пользователей от некачественной и недостоверной иностранной информации, недобросовестной конкуренции со стороны физических и юридических лиц иностранных государств в информационной сфере;

– способствуют развитию товарных отношений при международном информационном обмене.

Статья 5. Участие муниципальных образований в международном информационном обмене

1. Муниципальные образования участвуют в международном информационном обмене в качестве субъектов права, представляющих интересы населения муниципальных образований по вопросам, отнесенным к предметам ведения местного самоуправления.

Правом выступать от имени муниципальных образований по вопросам международного информационного обмена обладают органы местного самоуправления в рамках их полномочий, установленных нормативными правовыми актами, определяющими статус этих органов.

2. Муниципальные информационные службы и средства массовой информации муниципальных образований вправе самостоятельно участвовать в международном информационном обмене.

Данный закон в Российской Федерации принят Государственной Думой 5 июня 1996 г.

Следует также указать на другой международный документ по обмену информацией, это Окинавская хартия глобального информационного общества. Принята 22 июля 2000 г. лидерами стран «Большой Восьмерки». В ней в частности указывается:

1) Информационно-коммуникационные технологии (ИКТ) являются одним из наиболее важных факторов, влияющих на формирование общества двадцать первого века. Их революционное воздействие касается образа жизни людей, их образования и работы, а также взаимодействия правительства и гражданского общества. ИКТ быстро становятся жизненно важным стимулом развития мировой экономики. Они также дают возможность всем частным лицам, фирмам и сообществам, занимающимся предпринимательской деятельностью, более эффективно и творчески решать экономические и социальные проблемы. Перед всеми нами открываются огромные возможности.

2) Суть стимулируемой ИКТ экономической и социальной трансформации заключается в ее способности содействовать людям и обществу в использовании знаний и идей. Информационное общество, как мы его

представляем, позволяет людям шире использовать свой потенциал и реализовывать свои устремления. Для этого мы должны сделать так, чтобы ИКТ служили достижению взаимодополняющих целей обеспечения устойчивого экономического роста, повышения общественного благосостояния, стимулирования социального согласия и полной реализации их потенциала в области укрепления демократии, транспарентного и ответственного управления международного мира и стабильности.

3) Стремясь к достижению этих целей, мы вновь подтверждаем нашу приверженность принципу участия в этом процессе: все люди повсеместно, без исключения должны иметь возможность пользоваться преимуществами глобального информационного общества. Устойчивость глобального информационного общества основывается на стимулирующих развитие человека демократических ценностях, таких как, свободный обмен информацией и знаниями, взаимная терпимость и уважение к особенностям других людей.

4) Мы будем осуществлять руководство в продвижении усилий правительств по укреплению соответствующей политики и нормативной базы, стимулирующих конкуренцию и новаторство, по обеспечению экономической и финансовой стабильности, содействующих сотрудничеству по оптимизации глобальных сетей, борьбе со злоупотреблениями, которые подрывают целостность сети, по сокращению разрыва в цифровых технологиях, инвестированию в людей и обеспечению глобального доступа и участия в этом процессе.

5) Настоящая Хартия является прежде всего призывом ко всем как в государственном, так и в частном секторах, ликвидировать международный разрыв в области информации. Солидная основа политики и действий в сфере ИКТ может изменить методы нашего взаимодействия по продвижению социального и экономического прогресса во всем мире. Эффективное партнерство среди участников, включая совместное политическое сотрудничество, также является ключевым элементом рационального развития информационного общества.

Существует также Конвенция Совета Европы о защите личности в связи с автоматической обработкой персональных данных, в которой указано, что целью настоящей Конвенции является усиление защиты данных, точнее говоря, правовая защита личности при автоматической обработке персональной информации.

Необходимость таких правовых норм объясняется ростом использования компьютерной техники для целей управления. По сравнению с обработкой документации вручную автоматизированные базы данных имеют несоизмеримо большую накопительную способность и создают возможности для значительно более широкого набора операций, которые осуществляются с большой скоростью.

В ближайшие годы предполагается дальнейший рост автоматической обработки данных в сфере управления как следствие снижения издержек по обработке информации, доступности обрабатывающих устройств и создания нового телекоммуникационного оборудования для передачи информации.

"Информационная власть" обязывает пользователей данных как в частном, так и в публичном секторах к соответствующей социальной ответственности. В современном обществе многие решения, затрагивающие личность, принимаются на основе информации, накапливаемой в компьютеризированных базах данных: платежных ведомостях, документах по социальному обеспечению, историях болезни и т.п. Важно, чтобы те, кто отвечает за такие базы данных, смогли бы обеспечить положение, при котором неоспоримые достижения, которых можно добиться с помощью автоматической обработки данных, не привели бы в то же время к ослаблению позиции тех лиц, сведения о которых накапливаются. Это обязывает их придерживаться требований, касающихся качественных характеристик вверенной им информации, воздерживаться от накопления информации, которая не является необходимой для поставленной цели, принимать меры против несанкционированного раскрытия или злоупотребления информацией и охранять данные, оборудование и программное обеспечение от физического повреждения.

Существующие правовые системы государств – членов Совета Европы не в полной мере отвечают правилам, которые могли бы помочь достижению этих целей. Хотя у них есть законы о неприкосновенности личной сферы, обязательствах, вытекающих из причинения вреда, секретности или конфиденциальности определенной информации, тем не менее ощущается отсутствие общих правил, регламентирующих накопление и использование персональной информации, и в особенности по вопросу о том, каким образом лицо может осуществлять контроль над информацией о нем, которая собирается и используется другими лицами.

Немало есть и национальных законов в разных странах по защите информации.

3. ОРГАНИЗАЦИОННЫЕ МЕРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Организационные меры являются той основой, которая объединяет различные меры защиты в единую систему. Достижение высокого уровня безопасности невозможно без принятия должных организационных мер. С одной стороны, эти меры должны быть направлены на обеспечение правильности функционирования механизмов защиты и выполняться администратором безопасности системы. С другой стороны, руководство организации, эксплуатирующей средства автоматизации, должно регламентиро-

вать правила автоматизированной обработки информации, включая и правила ее защиты, а также установить меру ответственности за нарушение этих правил.

Организационное обеспечение заключается в регламентации взаимоотношений исполнителей на нормативно-правовой основе таким образом, что разглашение, утечка и несанкционированный доступ к информации становится невозможным или будет существенно затруднен за счет проведения организационных мероприятий. К основным организационным и режимным мероприятиям относятся:

– привлечение к проведению работ по защите информации организаций, имеющих лицензию на деятельность в области защиты информации, выданную соответствующими органами;

– категорирование и аттестация объектов технических средств передачи информации (ТСПИ) и выделенных для проведения закрытых мероприятий помещений (далее выделенных помещений) по выполнению требований обеспечения защиты информации при проведении работ со сведениями соответствующей степени секретности;

– использование на объекте сертифицированных ТСПИ и вспомогательных технических средств и систем (ВТСС);

– установление контролируемой зоны вокруг объекта;

– привлечение к работам по строительству, реконструкции объектов ТСПИ, монтажу аппаратуры организаций, имеющих лицензию на деятельность в области защиты информации по соответствующим пунктам;

– организация контроля и ограничение доступа на объекты ТСПИ и в выделенные помещения;

– введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите;

– отключение на период закрытых мероприятий технических средств, имеющих элементы, выполняющие роль электроакустических преобразователей, от линий связи и т.д.

Организационная защита обеспечивает:

– организацию охраны, режима, работу с кадрами, с документами;

– использование технических средств безопасности и информационно-аналитическую деятельность по выявлению внутренних и внешних угроз предпринимательской деятельности.

К основным организационным мероприятиям можно также отнести:

– организацию режима и охраны. Их цель – исключение возможности тайного проникновения на территорию и в помещения посторонних лиц;

– организацию работы с сотрудниками, которая предусматривает подбор и расстановку персонала, включая ознакомление с сотрудниками,

их изучение, обучение правилам работы с конфиденциальной информацией, ознакомление с мерами ответственности за нарушение правил защиты информации и др.;

– организацию работы с документами и документированной информацией, включая организацию разработки и использования документов и носителей конфиденциальной информации, их учёт, исполнение, возврат, хранение и уничтожение;

– организацию использования технических средств сбора, обработки, накопления и хранения конфиденциальной информации;

– организацию работы по проведению систематического контроля за работой персонала с конфиденциальной информацией, порядком учёта, хранения и уничтожения документов и технических носителей.

Основные организационные мероприятия по созданию и поддержанию функционирования комплексной системы защиты включают:

– разовые (однократно проводимые и повторяемые только при полном пересмотре принятых решений) мероприятия;

– мероприятия, проводимые при осуществлении или возникновении определенных изменений в самой защищаемой АС или внешней среде (по необходимости);

– периодически проводимые мероприятия;

– постоянно проводимые мероприятия.

Разовые мероприятия. К разовым мероприятиям относят:

– мероприятия, осуществляемые при проектировании, строительстве и оборудовании вычислительных центров и других объектов АС (исключение возможности тайного проникновения в помещения, исключение возможности установки прослушивающей аппаратуры и т.п.);

– разработка и утверждение функциональных обязанностей должностных лиц службы компьютерной безопасности;

– внесение необходимых изменений и дополнений во все организационно-распорядительные документы;

– оформление юридических документов (в форме договоров, приказов и распоряжений руководства организации) по вопросам регламентации отношений с пользователями (клиентами), работающими в автоматизированной системе;

– определение порядка назначения, изменения, утверждения и предоставления конкретным должностным лицам необходимых полномочий по доступу к ресурсам системы;

– мероприятия по разработке правил управления доступом к ресурсам системы;

– организацию надежного пропускного режима;

– определение порядка учета, выдачи, использования и хранения съемных магнитных носителей информации, содержащих эталонные и резервные копии программ и массивов информации, архивные данные и т.п.;

– создание отделов (служб) компьютерной безопасности или, в случае небольших организаций и подразделений, назначение нештатных ответственных, осуществляющих единое руководство, организацию и контроль за соблюдением всеми категориями должностных лиц требований по обеспечению безопасности.

Периодически проводимые мероприятия. К периодически проводимым мероприятиям относят:

– распределение реквизитов разграничения доступа (паролей, ключей шифрования и т.п.);

– анализ системных журналов, принятие мер по обнаруженным нарушениям правил работы;

– мероприятия по пересмотру правил разграничения доступа пользователей к информации в организации.

Мероприятия, проводимые по необходимости. К мероприятиям, проводимым по необходимости, относят:

– мероприятия, осуществляемые при кадровых изменениях в составе персонала системы;

– мероприятия, осуществляемые при ремонте и модификациях оборудования и программного обеспечения (строгое санкционирование, рассмотрение и утверждение всех изменений, проверка их на удовлетворение требованиям защиты, документальное отражение изменений и т.п.);

– мероприятия по подбору и расстановке кадров (проверка принимаемых на работу, обучение правилам работы с информацией, ознакомление с мерами ответственности за нарушение правил защиты, обучение, создание условий, при которых персоналу было бы невыгодно нарушать свои обязанности и т.д.).

Постоянно проводимые мероприятия. Постоянно проводимые мероприятия включают:

– мероприятия по обеспечению достаточного уровня физической защиты всех компонентов АС (противопожарная охрана, охрана помещений, пропускной режим, обеспечение сохранности и физической целостности средств вычислительной техники (СВТ), носителей информации и т.п.);

– мероприятия по непрерывной поддержке функционирования и управлению используемыми средствами защиты;

– явный и скрытый контроль за работой персонала системы;

– контроль за реализацией выбранных мер защиты в процессе проектирования, разработки, ввода в строй и функционирования АС;

– постоянно (силами отдела (службы) безопасности) и периодически (с привлечением сторонних специалистов) осуществляемый анализ состояния и оценка эффективности мер и применяемых средств защиты.

В каждом конкретном случае организационные мероприятия носят специфическую для данной организации форму и содержание, направленные на обеспечение безопасности информации в конкретных условиях.

3.1. Кадрово-организационные меры безопасности

В последнее время проблема кадрового обеспечения информационной безопасности привлекает к себе повышенное внимание. Эффективное развитие любого региона, да и всей страны в целом, невозможно без создания в государственных или иных структурах пользователей подлежащей защите информации специальных служб защиты, укомплектованных высококвалифицированными кадрами.

Сотрудники – не только основной актив компании, но и главный источник потенциальных угроз для нее, поэтому обеспечение комплекса мер по предотвращению рисков и опасностей, связанных с людьми, их деятельностью, – важнейшая задача службы управления персоналом. Невнимание к этим проблемам может привести к огромным потерям, поставить компанию на грань разорения. Служба управления персоналом обязана защитить информацию компании от угроз, возникающих с приходом в нее нечестных, недобросовестных работников, а возможно, и потенциальных злоумышленников.

Для начала нужно решить, что лучше: взять человека со стороны или закрыть образовавшуюся вакансию кем-либо из сотрудников компании. Первый вариант позволяет выбирать из более широкого круга претендентов. Однако он более опасен (особенно, если мы говорим о руководящей должности). Выдвижение на вакантную должность кандидата из числа сотрудников предприятия и легче, и не столь рискованно, хотя возможностей для выбора меньше. При грамотном, разумном использовании внутренних человеческих ресурсов можно значительно уменьшить количество работников, привлеченных извне.

Когда принято решение привлекать кандидатов извне, возникает вопрос о методе поиска. Один из каналов – рекомендации родственников и друзей сотрудников предприятия, их знакомых и т. д. Даже в западных странах, где рынок рекрутинга развит очень хорошо, до 40 % специалистов привлекаются благодаря использованию внутрифирменных источников информации. При таком методе поиска значительно упрощается проверка кандидата, к тому же у сотрудника-«рекомендателя» появляется чувство ответственности за приглашенного человека. В конфликтной или спорной ситуации это может оказаться очень кстати.

Привлечение людей со стороны – так называемый «открытый» поиск неизбежно ставит вопросы, связанные с проблемами безопасности. Например, выбор рекрутингового агентства. Неосмотрительность в этом вопросе опасна: аналитикам из конкурирующих организаций будут крайне любопытны многие данные из ваших кадровых заявок. К примеру, их заинтересует, в специалистах каких профессий, какой квалификации, в каком количестве и как срочно нуждается ваша компания.

С точки зрения обеспечения кадровой безопасности важными задачами являются:

- получение полных данных о кандидате;
- установление компрометирующих обстоятельств, предшествующей деловой жизни кандидата;
- определение достоверности представленных кандидатом сведений.

На этапе анкетирования вам крайне необходимо выявить все компрометирующие кандидата факты его биографии и определить степень достоверности представленных им сведений и документов. Без ряда вопросов «о жизни» тут не обойтись. Какие вопросы допустимо задавать кандидату? Любые. Однако не следует забывать о профессиональной этике. Итак, вы можете испросить у кандидата:

- данные о судимости и нахождении под следствием, об административных взысканиях, ограничениях правоспособности, о дисквалификации;
- сведения о существующих финансовых зависимостях (кредиты, ссуды, займы, долговые расписки, алименты);
- сведения о собственности (движимое и недвижимое имущество), а также о том, является ли кандидат учредителем (акционером, участником) юридических лиц и/или общественных организаций;
- данные о родственниках (особое внимание надо уделить родственникам, работающим в конкурирующих компаниях);
- сведения о семейном положении;
- уровень владения компьютером (сведения о навыках программирования могут быть интересны с точки зрения информационной безопасности компании в случае возникновения конфликтной ситуации при увольнении сотрудника);
- отношение к религии, в том числе членство в запрещенных (или деструктивных) сектах;
- сведения о состоянии здоровья (состоит ли на учете в диспансерах и др.).

Знать ответы на эти вопросы жизненно необходимо. В частности для того, чтобы проверить искренность будущего работника, достоверность полученных данных и иметь возможность прогнозировать его благонадежность.

При проверке документов следует быть внимательным, проверять на подделки. Среди наиболее распространенных способов подделки: внесение

изменений в подлинный документ путем подчисток, дописок, травлений; замена фотографии или отдельных страниц документа. При внимательной проверке удается обнаружить несоответствия в нумерации (страницы, серия и номер), в степени загрязненности, в размере и цвете листов; наличие лишних и не совпадающих проколов от скрепок.

Не стоит стесняться рассматривать паспорт со всех сторон, даже за обложкой. Вас должны насторожить:

– несоответствие личной подписи в паспорте личным подписям в других документах;

– различия в данных о семейном положении, количестве детей, указанном в паспорте и в анкете;

– несовпадение места регистрации проживания и места фактического проживания;

– отметки милиции (в виде указания мелким почерком где-нибудь в уголочке номера статьи Уголовного кодекса, по которой осужден владелец документа);

– наличие или отсутствие записи об отношении к военной службе.

Внешние характеристики и рекомендации как компетентное и независимое мнение о кандидате всегда полезны, особенно если получены вовремя. Приведем несколько простых советов:

– обязательно проверяйте, действительно ли кандидат работал в указанной организации, правильно ли он указал свою предыдущую должность и срок работы в ней;

– проясняйте только ту информацию о кандидате, которая непосредственно связана с его служебной деятельностью;

– гарантируйте (и обеспечивайте) конфиденциальность рекомендательных писем;

– уточняйте факты, содержащиеся в рекомендательных письмах, и те, которые кандидат привел в ходе интервью (например, размер заработной платы и дополнительных вознаграждений, функциональные обязанности, сферы ответственности, достижения, сильные и слабые стороны кандидата, рабочие привычки, модели поведения);

– точно фиксируйте все ответы, полученные при проверке рекомендаций кандидата;

– старайтесь минимизировать риски (к дополнительным рискам следует отнести информацию о том, что кандидат испытывал трудности, связанные с национальностью, полом, какой-либо формой неполноценности, с политическими или религиозными убеждениями или наличием судимости).

Весь процесс поиска и отбора кандидатов (часто сложный и длительный) служба по управлению персоналом проводит в тесном взаимодействии со службой безопасности компании. Каждая из служб делает

свою часть работы. К решению каких вопросов менеджеры по персоналу могут привлекать сотрудников службы безопасности? Для прояснения любых сомнений (а тем более подозрений) по поводу личности соискателя, его поведения, представленных им документов или сообщенных сведений. Для проведения проверок, например:

- по «милицейским» учетам (судимости, существенные административные взыскания, утеря паспорта, наличие розыскных дел и пр.);
- регистрации по месту жительства (пребывания);
- кредитной истории (через службы безопасности или кредитные отделы банков, предоставляющих потребительские и иные кредиты);
- на наличие связей в криминальной среде, в том числе через родственников;
- наличия недвижимого и движимого имущества (в том числе на соответствие заявленным);
- участия в капитале (учреждение, акционирование) юридических лиц (коммерческих или общественных организаций);
- представляемых документов.

В целом людей, непосредственно связанных с хранящейся в ЭВМ информацией, можно разделить по уровню её использования и опасности доступа на три группы.

1) Системные программисты.

Досконально знают устройство и принципы работы ЭВМ, способны использовать в своих целях все её ресурсы. В основном создают «средства производства» (инструментальные и языковые), т. е. ОС, системные утилиты, трансляторы, СУБД, интегрированные пакеты, оболочки экспертных систем, пакеты графики (в том числе средства защиты ПО и средства её снятия). Эта категория наиболее опасна, так как от них скрыть информацию почти не возможно.

2) Разработчики прикладного ПО.

Пользуясь продукцией системных программистов – «средствами производства», создают «предметы потребления», т. е. системы реального применения – базы данных, электронные таблицы под конкретные заказы, экспертные системы. Они владеют методами программирования и пишут программы, как правило, на языках высокого уровня: Си, Паскале, Прологе, Бейсике, и входных языках СУБД. Эта категория менее опасна, так как они работают в основном уже созданными программами.

3) Пользователи. В системах, разработанных прикладными программистами, используют программы для получения разного рода информации и вычислительных услуг. Пользователи практически не связаны с программированием. Эта категория наименее опасна, так как не владеют программированием. Однако эта категория представляет опасность от неумелых действий.

3.2. Режимно-административные меры безопасности

Режимно-административные меры безопасности определяют порядок доступа к информации путём установления перечня лиц, допущенных к ней, и условия этого допуска специальным приказом руководителя. Включают в себя:

1) заключение договора с сотрудниками о нераспространении конфиденциальной информации;
2) установление уровня секретности информации;
3) назначение ответственного за информационную безопасность;
4) установление системы изменения паролей;
5) заведение специальных журналов регистрации пользователей;
6) разработку специальных процедур пользования конфиденциальной информацией, её хранение и выдача специальных пропусков.

В целом ответственность за соблюдение информационной безопасности несет каждый сотрудник компании. Это значит, что информация должна быть защищена не менее надежно, чем любой другой основной актив. Главные цели безопасности информации не могут быть достигнуты без перечисленных мер безопасности.

Одной из важнейших составляющих информационной безопасности является политика информационной безопасности, о которой должен быть хорошо информирован каждый сотрудник организации или предприятия.

Политика информационной безопасности определяется как совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов. При разработке и проведении ее в жизнь целесообразно руководствоваться следующими принципами:

- невозможность миновать защитные средства;
- усиление самого слабого звена;
- невозможность перехода в небезопасное состояние;
- минимизация привилегий;
- разделение обязанностей;
- эшелонированность обороны;
- разнообразие защитных средств;
- простота и управляемость информационной системы;
- обеспечение всеобщей поддержки мер безопасности.

Поясним смысл перечисленных принципов. Если у злоумышленника или недовольного пользователя появится возможность миновать защитные средства, то он, разумеется, так и сделает. Применительно к межсетевым экранам данный принцип означает, что все информационные потоки в защищаемую сеть и из нее должны проходить через экран. Не должно быть “тайных” модемных входов или линий, идущих в обход экрана.

Принцип невозможности перехода в небезопасное состояние означает, что при любых обстоятельствах, в том числе нештатных, защитное средство либо полностью выполняет свои функции, либо полностью блокирует доступ. Образно говоря, если в крепости механизм подъемного моста ломается, мост должен оставаться в поднятом состоянии, препятствуя проходу неприятеля.

Принцип минимизации привилегий предписывает выделять пользователям и администраторам только те права доступа, которые необходимы им для выполнения служебных обязанностей.

Принцип разделения обязанностей предполагает такое распределение ролей и ответственности, при котором один человек не может нарушить критически важный для организации процесс. Это особенно важно, чтобы предотвратить злонамеренные или неквалифицированные действия системного администратора.

Принцип эшелонированности обороны предписывает не полагаться на один защитный рубеж, каким бы надежным он ни казался. За средствами физической защиты должны следовать программно-технические средства и т.д.

Принцип разнообразия защитных средств рекомендует организовывать различные по своему характеру оборонительные рубежи, чтобы от потенциального злоумышленника требовалось овладение разнообразными и, по возможности, несовместимыми между собой навыками (например, умением преодолевать высокую ограду и знанием слабостей нескольких операционных систем).

Очень важен **принцип простоты и управляемости** информационной системы в целом и защитных средств в особенности. Только для простого защитного средства можно формально или неформально доказать его корректность. Только в простой и управляемой системе можно проверить согласованность конфигурации разных компонентов и осуществить централизованное администрирование.

Последний **принцип – всеобщая поддержка мер безопасности** – носит нетехнический характер. Если пользователи и/или системные администраторы считают информационную безопасность чем-то излишним или даже враждебным, то режим безопасности сформировать заведомо не удастся. Следует с самого начала предусмотреть комплекс мер, направленный на обеспечение лояльности персонала, на постоянное обучение, теоретическое и, главное, практическое.

Как правило, следует придерживаться принципа "все, что не разрешено, запрещено", поскольку "лишний" сетевой сервис может предоставить канал проникновения в корпоративную систему. В принципе, ту же мысль выражает положение "все непонятное опасно".

Руководители подразделений должны обеспечить регулярный контроль за соблюдением положений настоящей политики. Кроме того, должна быть организована периодическая проверка соблюдения информационной безопасности с последующим представлением отчета по результатам указанной проверки руководству.

Требования настоящей политики информационной безопасности распространяются на всю информацию и ресурсы обработки информации предприятия. Соблюдение настоящей политики обязательно для всех сотрудников (как постоянных, так и временных). В договорах с третьими лицами, получающими доступ к информации, должна быть оговорена обязанность третьего лица по соблюдению требований настоящей политики информационной безопасности.

Кроме политики безопасности, необходимыми мерами для организации комплексной системы защиты информации является разработка следующих групп организационно-распорядительных документов:

– документы, определяющие порядок и правила обеспечения безопасности информации при ее обработке в АС (план защиты информации в АС, план обеспечения непрерывной работы и восстановления информации);

– документы, определяющие ответственность взаимодействующих организаций (субъектов) при обмене электронными документами (договор об организации обмена электронными документами).

План защиты информации в АС должен содержать следующие сведения:

– описание защищаемой системы (основные характеристики защищаемого объекта): назначение АС, перечень решаемых АС задач, конфигурация, характеристики и размещение технических средств и программного обеспечения, перечень категорий информации (пакетов, файлов, наборов и баз данных, в которых они содержатся), подлежащих защите в АС и требований по обеспечению доступности, конфиденциальности, целостности этих категорий информации, список пользователей и их полномочий по доступу к ресурсам системы и т.п.;

– цель защиты системы и пути обеспечения безопасности АС и циркулирующей в ней информации;

– перечень значимых угроз безопасности АС, от которых требуется защита, и наиболее вероятных путей нанесения ущерба;

– основные требования к организации процесса функционирования АС и мерам обеспечения безопасности обрабатываемой информации;

– требования к условиям применения и определение зон ответственности установленных в системе технических средств защиты от НСД;

– основные правила, регламентирующие деятельность персонала по вопросам обеспечения безопасности АС (особые обязанности должностных лиц АС).

План обеспечения непрерывной работы и восстановления информации должен отражать следующие вопросы:

– цель обеспечения непрерывности процесса функционирования АС, своевременность восстановления ее работоспособности и чем она достигается;

– перечень и классификация возможных кризисных ситуаций;

– требования, меры и средства обеспечения непрерывной работы и восстановления процесса обработки информации (порядок создания, хранения и использования резервных копий информации и дублирующих ресурсов и т.п.);

– обязанности и порядок действий различных категорий персонала системы в кризисных ситуациях по ликвидации их последствий, минимизации наносимого ущерба и восстановлению нормального процесса функционирования системы.

Договор о порядке организации обмена электронными документами должен включать документы, в которых отражаются следующие вопросы:

– разграничение ответственности субъектов, участвующих в процессах обмена электронными документами;

– определение порядка подготовки, оформления, передачи, приема, проверки подлинности и целостности электронных документов;

– определение порядка генерации, сертификации и распространения ключевой информации (ключей, паролей и т.п.);

– определение порядка разрешения споров в случае возникновения конфликтов.

3.3. Контроль доступа к информационным системам

В целях сохранности информации, имеющейся в информационных системах, должен быть налажен и определен доступ к ней. Эта задача разделяется на два взаимно исключающих варианта: недопущения доступа посторонних лиц и ограничение допуска сотрудников, контроль их работы. Первая задача решается физической частью службы безопасности, вторая – организационно – компьютерной или программной.

В общем случае должны выполняться следующие требования. Все работы в пределах офисов выполняются в соответствии с должностными обязанностями и только на компьютерах, разрешенных к использованию. Внос в здания и помещения личных портативных компьютеров и внешних носителей информации (диски, дискеты, флэш-карты и т.п.), а также вынос их за пределы производится только при согласовании с руководителем предприятия.

Все данные (конфиденциальные или строго конфиденциальные), составляющие коммерческую тайну и хранящиеся на жестких дисках порта-

тивных компьютеров, должны быть зашифрованы. Все портативные компьютеры должны быть оснащены программным обеспечением по шифрованию жесткого диска.

Руководители подразделений должны периодически пересматривать права доступа своих сотрудников и других пользователей к соответствующим информационным ресурсам.

В целях обеспечения санкционированного доступа к информационному ресурсу любой вход в систему должен осуществляться с использованием уникального имени пользователя и пароля.

Пользователи должны руководствоваться рекомендациями по защите своего пароля на этапе его выбора и последующего использования. Запрещается сообщать свой пароль другим лицам или предоставлять свою учетную запись другим, в том числе членам своей семьи и близким, если работа выполняется дома.

Доступ третьих лиц к системам

Каждый сотрудник обязан немедленно уведомить руководителя организации информационных технологий и руководителя организации защиты информации обо всех случаях предоставления доступа третьим лицам к ресурсам корпоративной сети.

Доступ третьих лиц к информационным системам должен быть обусловлен производственной необходимостью. В связи с этим порядок доступа к информационным ресурсам должен быть четко определен, контролируем и защищен.

Удаленный доступ

Пользователи получают право удаленного доступа к информационным ресурсам с разрешения руководства.

Сотрудникам, использующим в работе портативные компьютеры, может быть предоставлен удаленный доступ к сетевым ресурсам в соответствии с правами в корпоративной информационной системе.

Сотрудники и третьи лица, имеющие право удаленного доступа к информационным ресурсам, должны соблюдать требование, исключающее одновременное подключение их компьютера к сети и к каким-либо другим сетям, не принадлежащим организации.

Все компьютеры, подключаемые посредством удаленного доступа к информационной сети, должны иметь программное обеспечение антивирусной защиты, имеющее последние обновления.

Доступ к сети Интернет обеспечивается только в производственных целях. Рекомендованные правила:

- сотрудники не должны использовать сеть Интернет для хранения корпоративных данных;
- работа сотрудников с Интернет-ресурсами допускается только режимом просмотра информации, исключая возможность передачи информации в сеть Интернет;

- сотрудникам, имеющим личные учетные записи, предоставленные публичными провайдерами, не разрешается пользоваться ими на оборудовании, принадлежащем предприятию;
- сотрудники перед открытием или распространением файлов, полученных через сеть Интернет, должны проверить их на наличие вирусов;
- запрещен доступ в Интернет через сеть для всех лиц, не являющихся сотрудниками, включая членов семьи сотрудников.

Сотрудникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения. Все изменения производят авторизованные специалисты по защите информации.

Специалисты по защите информации имеют право контролировать содержание всего потока информации, проходящей через канал связи к сети Интернет в обоих направлениях.

Пользователи портативных компьютеров, содержащих информацию, составляющую коммерческую тайну, обязаны обеспечить их надежное хранение в физически защищенных помещениях, запираемых ящиках рабочего стола, шкафах. В ситуациях, когда возрастает степень риска кражи портативных компьютеров, например, в гостиницах, аэропортах, в офисах деловых партнеров и т.д., пользователи обязаны ни при каких обстоятельствах не оставлять их без присмотра. Во время поездки в автомобиле портативный компьютер должен находиться в багажнике. На ночь его следует перенести из автомобиля в гостиничный номер.

При записи какой-либо информации на носитель для передачи его контрагентам или партнерам по бизнесу необходимо убедиться в том, что носитель чист, то есть не содержит никаких иных данных. Простое переформатирование носителя не дает гарантии полного удаления записанной на нем информации.

Рекомендуемые правила пользования электронной почтой. Электронные сообщения (удаленные или не удаленные) могут быть доступны или получены государственными органами или конкурентами по бизнесу для их использования в качестве доказательств в процессе судебного разбирательства или при ведении бизнеса, поэтому содержание электронных сообщений должно строго соответствовать корпоративным стандартам в области деловой этики.

Использование электронной почты в личных целях допускается в случаях, когда получение/отправка сообщения не мешает работе других пользователей и не препятствует бизнес-деятельности.

Сотрудникам запрещается направлять партнерам конфиденциальную информацию по электронной почте без использования систем шифрования. Строго конфиденциальная информация ни при каких обстоятельствах не подлежит пересылке третьим лицам по электронной почте.

Сотрудникам запрещается использовать публичные почтовые ящики электронной почты для осуществления какого-либо из видов корпоративной деятельности.

Использование сотрудниками публичных почтовых ящиков электронной почты осуществляется только при согласовании с Департаментом защиты информации при условии применения механизмов шифрования.

Сотрудники для обмена документами с бизнес-партнерами должны использовать только свой официальный адрес электронной почты.

Сообщения, пересылаемые по электронной почте, представляют собой постоянно используемый инструмент для электронных коммуникаций, имеющих тот же статус, что и письма и факсимильные сообщения. Электронные сообщения подлежат такому же утверждению и хранению, что и прочие средства письменных коммуникаций.

В целях предотвращения ошибок при отправке сообщений пользователи перед отправкой должны внимательно проверить правильность написания имен и адресов получателей. В случае получения сообщения лицом, вниманию которого это сообщение не предназначается, такое сообщение необходимо переправить непосредственному получателю. Если полученная таким образом информация носит конфиденциальный характер, то об этом следует незамедлительно проинформировать специалистов организации защиты информации.

Отправитель электронного сообщения, документа или лицо, которое его переадресовывает, должен указать свое имя и фамилию, служебный адрес и тему сообщения.

Ниже перечислены недопустимые действия и случаи использования электронной почты:

- рассылка сообщений личного характера, использующих значительные ресурсы электронной почты;
- групповая рассылка всем пользователям сообщений/писем;
- рассылка рекламных материалов, не связанных с деятельностью;
- подписка на рассылку, участие в дискуссиях и подобные услуги, использующие значительные ресурсы электронной почты в личных целях;
- поиск и чтение сообщений, направленных другим лицам (независимо от способа их хранения);
- пересылка любых материалов, как сообщений, так и приложений, содержание которых является противозаконным, непристойным, злонамеренным, оскорбительным, угрожающим, клеветническим, злобным или способствует поведению, которое может рассматриваться как уголовное преступление или административный проступок либо приводит к возникновению гражданско-правовой ответственности, беспорядков или противоречит корпоративным стандартам в области этики.

Ко всем исходящим сообщениям, направляемым внешним пользователям, пользователь может добавлять уведомление о конфиденциальности.

Вложения, отправляемые вместе с сообщениями, следует использовать с должной осторожностью. Во вложениях всегда должна указываться дата их подготовки, и они должны оформляться в соответствии с установленными процедурами документооборота.

Пересылка значительных объемов данных в одном сообщении может отрицательно повлиять на общий уровень доступности сетевой инфраструктуры для других пользователей. Объем вложений не должен превышать 2 Мб.

Сообщение об инцидентах информационной безопасности, реагирование и отчетность

Все пользователи должны быть осведомлены о своей обязанности сообщать об известных или подозреваемых ими нарушениях информационной безопасности, а также должны быть проинформированы о том, что ни при каких обстоятельствах они не должны пытаться использовать ставшие им известными слабые стороны системы безопасности.

В случае кражи переносного компьютера следует незамедлительно сообщить об инциденте директору организации защиты информации.

Пользователи должны знать способы информирования об известных или предполагаемых случаях нарушения информационной безопасности с использованием телефонной связи, электронной почты и других методов. Необходимо обеспечить контроль и учет сообщений об инцидентах и принятие соответствующих мер.

Если имеется подозрение или выявлено наличие вирусов или иных разрушительных компьютерных кодов, то сразу после их обнаружения сотрудник обязан:

- проинформировать специалистов организации информационных технологий;
- не пользоваться и не выключать зараженный компьютер;
- не подсоединять этот компьютер к компьютерной сети до тех пор, пока на нем не будет произведено удаление обнаруженного вируса и полное антивирусное сканирование специалистами организации информационных технологий.

Помещения с техническими средствами информационной безопасности

Конфиденциальные встречи (заседания) должны проходить только в защищенных техническими средствами информационной безопасности помещениях. Перечень помещений с техническими средствами информационной безопасности утверждается руководством.

Участникам заседаний запрещается входить в помещения с записывающей аудио/видеоаппаратурой, фотоаппаратами, радиотелефонами и мобильными телефонами без предварительного согласования с Департаментом защиты информации.

Аудио/видеозапись, фотографирование во время конфиденциальных заседаний может вести только сотрудник, который отвечает за подготовку заседания, после получения письменного разрешения руководителя группы организации встречи.

Доступ участников конфиденциального заседания в помещение для его проведения осуществляется на основании утвержденного перечня, контроль за которым ведет лицо, отвечающее за организацию встречи.

Управление сетью

Уполномоченные сотрудники отдела информационных технологий и защиты информации контролируют содержание всех потоков данных, проходящих через сеть.

Сотрудникам запрещается:

- нарушать информационную безопасность и работу сети;
- сканировать порты или систему безопасности;
- контролировать работу сети с перехватом данных;
- получать доступ к компьютеру, сети или учетной записи в обход системы идентификации пользователя или безопасности;
- использовать любые программы, скрипты, команды или передавать сообщения с целью вмешаться в работу или отключить пользователя оконечного устройства;
- передавать информацию о сотрудниках или списки сотрудников посторонним лицам;

Контроль и управление доступом теряют всякий смысл без идентификации пользователя системы. В последнее время начинают получать распространение биометрические системы контроля доступа. Они позволяют оценивать физиологические характеристики человека.

Большинство современных систем контроля и управления доступом имеют в своем составе ряд модулей, позволяющих осуществлять учет рабочего времени, интегрируемых с бухгалтерскими программами, базами данных бюро пропусков. Также возможно их совместное использование с системами охранно-пожарной сигнализации, видеонаблюдения.

3.4. Службы защиты информационной безопасности

Службы информационной безопасности осуществляют защиту автоматизированных систем двух видов – это информационно-компьютерная и физическая защита.

Задачей информационно-компьютерной защиты является предотвращение утечек информации по каналам связи с помощью информационных носителей, флеш-карт, защита информации от внешних хакерских и вирусных атак.

Задачей физической защиты является препятствие проникновению на защищаемый объект посторонних лиц и злоумышленников, охрана имущества от хищения, в том числе и устройств автоматизированных систем.

Службы информационной безопасности, используемые на предприятии, могут быть двух типов:

1) собственные,

2) внешние.

Собственные службы информационной безопасности создаются на предприятии и подчиняются его руководителю. Численность и вооружение этой службы может быть разным и зависит от финансовых возможностей предприятия, его разбросанности. Из опыта работы таких служб очевидно, что создавать крупные собственные службы целесообразно в концернах и объединениях, обладающих достаточно большими экономическими возможностями. В менее крупных чаще всего создаются небольшие отделы информационной безопасности, либо назначаются несколько ответственных за это.

Собственные службы информационной безопасности могут также осуществлять и физическую защиту.

Внешние службы информационной безопасности привлекаются с помощью договоров, различных соглашений со специализированными и частными охранными предприятиями. Крупные предприятия имеют свои собственные службы информационной безопасности, которые осуществляют как информационно-компьютерную, так и физическую защиту. Менее крупные организации и предприятия чаще всего имеют собственные службы информационно-компьютерной безопасности, а физическую защиту осуществляют привлечением специализированных охранных предприятий по договорам с оплатой их услуг.

Служба информационно-компьютерной безопасности представляет собой штатное подразделение, создаваемое для организации защиты информации и обеспечения ее функционирования. В крупных организациях её функции весьма широки и заключаются в следующем:

– планирование, организация и обеспечение функционирования системы защиты информации в процессе функционирования автоматизированной системы (АС);

– распределение между пользователями необходимых реквизитов защиты;

– наблюдение за функционированием системы защиты и ее элементов;

– организация проверок надежности функционирования системы защиты;

– обучение пользователей и персонала АС правилам безопасной обработки информации;

– контроль за соблюдением пользователями и персоналом АС установленных правил обращения с защищаемой информацией в процессе ее автоматизированной обработки;

– принятие мер при попытках НСД к информации и при нарушениях правил функционирования системы защиты.

Предпочтительно, чтобы организационно-правовой статус такой службы определялся следующим образом:

– численность службы защиты должна быть достаточной для выполнения всех перечисленных выше функций;

– служба защиты должна подчиняться тому лицу, которое в данном учреждении несет персональную ответственность за соблюдение правил обращения с защищаемой информацией;

– штатный состав службы защиты не должен иметь других обязанностей, связанных с функционированием АС;

– сотрудники службы защиты должны иметь право доступа во все помещения, где установлена аппаратура АС и право прекращать автоматизированную обработку информации при наличии непосредственной угрозы для защищаемой информации;

– руководителю службы защиты должно быть предоставлено право запрещать включение в число действующих новые элементы АС, если они не отвечают требованиям защиты информации.

При децентрализованном управлении каждая подсистема АС имеет своего сотрудника группы безопасности.

Службы физической защиты – это технические средства физической защиты, посты охраны, пропускные пункты, охранники, дежурные оперативные группы, контролеры, службы, отделы или группы информационной безопасности.

Технические средства физической защиты – устройства, приспособления, конструкции, аппараты, изделия, предназначенные для создания препятствий на пути движения злоумышленников.

В области применения технических средств защиты существует руководящий документ "Инженерно-техническая укрепленность. Технические средства охраны. Требования и нормы проектирования по защите объектов от преступных посягательств" (утв. МВД РФ 6 ноября 2002 г.) распространяются на вновь проектируемые, реконструируемые и технически перевооружаемые объекты различных форм собственности, охраняемые или подлежащие передаче под охрану подразделениям вневедомственной охраны при органах внутренних дел на территории Российской Федерации. Этот документ устанавливает порядок и способы оснащения объектов элементами инженерно-технической укрепленности и техническими средствами охраны с целью противодействия преступным посягательствам на них.

Все технические средства защиты объектов можно разделить на три категории: средства предупреждения, средства обнаружения и системы ликвидации угроз.

В общем плане по функциональному назначению все средства этой категории можно разделить на следующие группы:

- охранные и охранно-пожарные системы;
- охранное телевидение;
- охранное освещение;
- средства защиты от проникновения, контроль и управление доступом.

К средствам охранной и охранно-пожарным системам относятся устройства, предупреждающие возгорание. Пожар является наиболее серьезным источником угрозы информационной безопасности, он может возникнуть как случайно, например, от короткого замыкания, так и по вине персонала. Поскольку вся основная информация хранится на компьютерах или на бумажных носителях, то защита от возгорания становится неотъемлемой частью защиты информации.

Автоматические противопожарные системы – это довольно сложный комплекс специальных средств, оборудования и элементов, которые способны не только своевременно обнаружить очаг возгорания, но и ликвидировать его в автоматическом режиме. Таким образом, организация противопожарной безопасности является комплексом мероприятий, направленных на обеспечение пожаротушения, дымоудаления, контроль доступа и эвакуацию людей.

По исполнению охранно-пожарная сигнализация может быть трех основных типов:

1) автономная – при срабатывании такой системы сигнализации включается звуковое и (или) световое оповещение. Вся надежда при этом (весьма слабая) – что кто-то заметит это, отреагировав должным образом;

2) система охранно-пожарной сигнализации может быть выведена на пост физической ведомственной охраны (службы собственной безопасности объекта). Вариант более надежный, ибо подразумевает наличие человека, способного принять соответствующее решение в зависимости от ситуации;

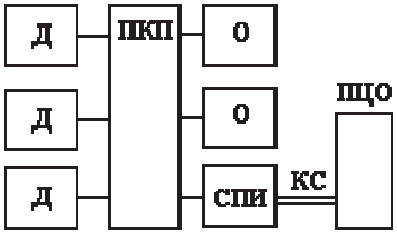
3) передача сигнала о срабатывании системы охранно-пожарной сигнализации пульту централизованной охраны, частному охранному предприятию (ЧОП), вневедомственной охране – это наиболее распространенный и надежный способ.

Кроме того, стоит отметить получивший в последнее время распространение способ передачи информации о состоянии сигнализации на объекте собственнику объекта по каналу GSM.

Структурная схема охранно-пожарной сигнализации приведена на схеме. Это наиболее полный вариант, учитывающий вывод сигнала на пульт централизованной охраны, который включает:

- охранно-пожарные датчики (извещатели) – Д;
- прибор приемно-контрольный охранно-пожарный – ПКП;

- оповещатели (звуковые, световые) – О;
- систему передачи извещений СПИ;
- канал связи (КС) с ПЦО.



В качестве средств защиты от пожара можно привести следующее оборудование.

Извещатель пожарный дымовой оптико-электронный адресно-аналоговый ДИП 212-92А. Внешний вид датчика представлен на рис. 1.

Рис. 1. Извещатель ДИП 212-92А

Основные технические характеристики:

- чувствительность извещателя, дБ/м – от 0,02 до 0,2;
- инерционность извещателя, с – не более 10;
- степень защиты оболочки – IP 41;
- напряжение в линии связи, В – от 8 до 28;
- потребляемый ток в дежурном режиме, мА – не более 0,5;
- потребляемый ток в режиме «Пожар», мА – не более 1;
- время технической готовности, с – не более 60;
- диапазон температур, °С – от -10 до +55;
- относительная влажность воздуха, % – до 93 при +40 °С;
- масса, кг – не более 0,2;
- температура транспортирования, °С – от -50 до +50;
- габариты, мм: диаметр – не более 100; высота – не более 50.

Дымовые датчики – используются для обнаружения загорания, сопровождающегося появлением дыма в производственных и жилых помещениях и передачи сигнала тревоги на прибор пожарной сигнализации.

В качестве тепловых датчиков используют извещатели пожарные тепловые ИП-114-5-А2 – одни из самых простых в установке и обслуживании и в то же время надежные и недорогие. Внешний вид датчика представлен на рис. 2.

Рис. 2. Извещатель пожарный тепловой ИП-114−5-А2

ИП-114−5-А2 – это датчик с нормально-замкнутыми контактами класса А2 с температурой срабатывания от 54 до 70 °С. Этот пожарный извещатель предназначен для контроля температуры газовоздушной среды помещений зданий и выдачи тревожного сигнала о пожаре в случае превышения температуры срабатывания извещателя. Его также допускается применять в искробезопасных цепях (шлейфах) приемно-контрольных приборов, имеющих соответствующую маркировку по взрывозащите.

В качестве средств для тушения пожара часто используют порошковые огнетушители ОП-2. Они применяются для тушения возгорания нефтепродуктов, горючих материалов (пожары класса А), горючих жидкостей (пожары класса В), а также для тушения возгорания электроустановок, находящихся под напряжением до 1000 В, для тушения возгораний в автомобилях. На сегодняшний день это самый распространенный тип огнетушителей. Одним из основных преимуществ порошковых огнетушителей является то, что их можно перезаряжать один раз в пять лет. Модель ОП-2 является компактной и мобильной, для быстрого тушения возгораний и пожаров.

Длина выброса струи порошка у него 2 м, диапазон температур эксплуатации довольно широк от -40 до +50 °С.

Следует отметить, что система сигнализации может содержать несколько приемно-контрольных приборов, систем передачи извещений, использующих различные каналы связи. Более того, с точки зрения повышения надежности охранно-пожарной сигнализации использовать несколько каналов связи, различных по физическому принципу действия, способу кодирования информации и прочее весьма целесообразно.

Необходимо обратить внимание на одно противоречие в вопросах обеспечения имущественной безопасности, которые решает охранная сигнализация, и безопасности пожарной. Так вот – охранную сигнализацию рекомендуется использовать совместно с элементами инженерно-технической укрепленности, затрудняющими доступ на охраняемый объект. Пожарная же безопасность, наоборот, предполагает обеспечение максимально легкой эвакуации людей, доступа пожарных расчетов для ликвидации возгораний. Это противоречие следует тоже учитывать при решении вопроса защиты объекта.

К средствам охранного телевидения чаще всего относят устройства видеонаблюдения (рис. 3). Системы видеонаблюдения позволяют осуществлять визуальный контроль за территорией, внутренними помещениями объекта.

Систему телевизионного наблюдения на объекте защиты и охраняемой территории с видеозаписью выбираем на основе категории значимости объекта. Согласно рекомендациям ГУВО МВД России Р 78.36.002-99, все объекты делятся по значимости на разные категории.

Правильный выбор телевизионных камер является принципиально самым важным моментом в проектировании системы, так как именно характеристиками камер определяются в конечном счете характеристики других компонентов системы. При выборе телекамеры и места ее установки учитываются:

- категория значимости зоны;
- геометрические размеры зоны;
- необходимость идентификации наблюдаемого предмета;
- освещенность объекта наблюдения;
- условия эксплуатации;
- вид наблюдения – скрытое или открытое.

В зависимости от технических характеристик оборудования системы видеонаблюдения она позволяет осуществлять:

- распознавание объекта,
- опознание знакомого человека,
- опознание незнакомого человека.

Характеристики системы видеонаблюдения в целом зависят от параметров входящего в ее состав оборудования и определяются техническим заданием на проектирование системы.

При использовании специальных программно-аппаратных средств возможно распознавание автомобильных номеров, лиц людей. Это позволяет использовать видеонаблюдение в интегрированных системах безопасности, системах контроля и управления доступом.

Рис. 3. Внешний вид видеокамер наблюдения

Установка систем видеонаблюдения должна производиться с учетом особенностей, определяемых конкретными условиями их применения. Например, видеонаблюдение в офисе устанавливается, главным образом, для контроля за действиями сотрудников, соблюдением трудовой дисциплины. Видеонаблюдение в магазине, кроме того, преследует цели предотвращения хищений, злоупотреблений со стороны работников, решения спорных вопросов с клиентами.

Для того чтобы правильно выбрать систему видеонаблюдения надо определить, какие задачи и в каких условиях она будет решать, затем выбирать оборудование, сообразуясь с его техническими характеристиками.

Различают следующие типы систем видеонаблюдения: цифровое, аналоговое.

Цифровое передает видеосигнал в цифровой форме, может работать в составе локальных вычислительных сетей или автономно. Камеры для такой системы видеонаблюдения являются самостоятельными сетевыми устройствами, могут использоваться в системах Wi-Fi видеонаблюдения, так что, если нужно беспроводное видеонаблюдение, то стоит выбрать эту систему. Цифровые системы видеонаблюдения дороже аналоговых, но позволяют достичь экономии при монтаже, если на объекте уже есть локальная сеть.

Качество изображения определяется камерами видеонаблюдения, однако практически любая система видеонаблюдения имеет устройства обработки записи видеоинформации:

- видеорегистратор,
- плата видеоввода,
- программное обеспечение для ПК,

которые также определяют качество изображения. Поэтому выбирать такой параметр как разрешение следует с учетом совместной работы видеокамеры и перечисленных программно-аппаратных средств видеозаписи.

Условия установки систем видеонаблюдения могут требовать приобретения дополнительного оборудования (усилителей, преобразователей сигнала, различных устройств защиты), дополнительных расчетов для уточнения ряда параметров устройств, входящих в состав системы видеонаблюдения.

К средствам охранного освещения предъявляются следующие требования. Периметр территории, здания охраняемого объекта должны быть оборудованы системой охранного освещения согласно ГОСТ 12.1.046-85. Охранное освещение должно обеспечивать необходимые условия видимости ограждения территории, периметра здания, зоны отторжения, тропы наряда (путей обхода), возможность автоматического включения дополнительных источников света на отдельном участке (зоне) охраняемой территории (периметра) при срабатывании охранной сигнализации, ручное управление работой освещения из помещения охраны.

Сеть охранного освещения по периметру объекта и на территории должна выполняться отдельно от сети наружного освещения и разделяться на самостоятельные участки в соответствии с участками охранной сигнализации периметра и/или охранного телевидения. Сеть охранного освещения должна подключаться к отдельной группе щита освещения, расположенного в помещении охраны или на КПП.

Осветительные приборы охранного освещения могут быть любого типа: подвесные, консольные, прожектора и другие типы.

Светильники охранного освещения по периметру территории должны устанавливаться не выше ограждения. Лампы охранного освещения должны быть защищены от механических повреждений.

К средствам физической защиты от проникновения, осуществляющим контроль и управление доступом, относятся устройства следующего типа. Автоматика для ворот, автоматические шлагбаумы, двери, автоматизированные парковки, дорожные блокираторы, турникеты, ограждения, охранные извещатели, реагирующие на открытие дверей, окон, а также на разбитие стекол, досмотровое и антитеррористическое оборудование, а также оружие различного исполнения и назначения для вооружения охранников.

3.5. Оснащение и вооружение служб безопасности

Службы физической защиты, посты охраны, охранники, дежурные оперативные группы, контролеры, военизированная охрана чаще всего имеют свои штатные средства защиты, предназначенные для противодействия злоумышленникам. Такие средства разделяют на пассивные и активные. К пассивным средствам относятся те, которые не наносят вреда нападавшему, а лишь защищают охранника. Это бронежилеты, резиновые дубинки, щиты, шлемы, специальные перчатки. В качестве активных средств применяют шокеры, газовые баллончики и оружие.

Применение этих средств регулируется федеральным законом «Об оружии» от 13.12.1996 № 150-ФЗ (принят ГД ФС РФ 13.11.1996, действующая редакция от 01.09.2013).

Согласно этому закону оружие – устройства и предметы, конструктивно предназначенные для поражения живой или иной цели, подачи сигналов. ФЗ «Об оружии» регулирует только оборот ручного (индивидуального) оружия. Это оружие в зависимости от целей его использования, а также по основным параметрам подразделяется:

- на гражданское,
- служебное,
- боевое.

Все гражданское и служебное оружие и патроны к нему подлежат обязательной государственной сертификации, которую проводит Госстандарт РФ. Он же осуществляет выпуск специальных сборников оружия, разрешенного к обороту на территории РФ. При этом физическим лицам разрешено приобретать только гражданское оружие. Оно используется в целях самообороны, для занятий спортом, охоты, для ношения с казачьей формой, а также с национальными костюмами народов РФ, атрибутика которых определяется Правительством РФ, либо для подачи сигналов. Гражданское огнестрельное оружие должно исключать ведение огня очередями и иметь емкость магазина (барабана) не более 10 патронов.

Граждане, достигшие 18 лет (в отдельных субъектах РФ этот возраст может быть снижен до 16 лет, но только для хранения или хранения и ношения охотничьего огнестрельного гладкоствольного оружия), могут приобретать оружие после получения лицензии. Впоследствии оружие необходимо зарегистрировать.

Виды гражданского оружия:

1) оружие самообороны:

- огнестрельное гладкоствольное длинноствольное оружие, в том числе с патронами травматического действия, соответствующими нормам Министерства здравоохранения РФ;
- огнестрельное бесствольное оружие отечественного производства с патронами травматического, газового и светозвукового действия, соответствующими нормам Министерства здравоохранения РФ;
- газовое оружие: газовые пистолеты и револьверы, в том числе патроны к ним, механические распылители, аэрозольные и другие устройства, снаряженные слезоточивыми или раздражающими веществами, разрешенными к применению Министерством здравоохранения РФ;
- электрошоковые устройства и искровые разрядники отечественного производства, имеющие выходные параметры, соответствующие требованиям государственных стандартов РФ и нормам Министерства здравоохранения РФ;

2) спортивное оружие:

- огнестрельное с нарезным стволом;
- огнестрельное гладкоствольное;
- холодное клинковое;
- метательное;
- пневматическое с дульной энергией свыше 3 Дж;

3) охотничье оружие:

- огнестрельное с нарезным стволом;
- огнестрельное гладкоствольное, в том числе с длиной нарезной части не более 140 мм;

- огнестрельное комбинированное (нарезное и гладкоствольное), в том числе со сменными и вкладными нарезными стволами;
- пневматическое с дульной энергией не более 25 Дж;
- холодное клинковое;

4) сигнальное оружие;

5) холодное клинковое оружие, предназначенное для ношения с казачьей формой, а также с национальными костюмами народов РФ, атрибутика которых определяется Правительством РФ.

Органы, уполномоченные выдавать лицензии на оружие – это отделы разрешительно-лицензионной работы при ОВД.

Документы, необходимые для получения лицензии на приобретение оружия:

– заявление (в нем указываются сведения о видах оружия, которое планируется приобрести, и меры, принятые для обеспечения учета и сохранности оружия);

– учредительные и регистрационные документы юридического лица;

– паспорт гражданина РФ или иные документы, удостоверяющие личность;

– медицинское заключение об отсутствии противопоказаний к владению оружием, связанных с нарушением зрения, психическим заболеванием, алкоголизмом или наркоманией по форме № 046-1, утв. Приказом Минздрава РФ от 11.09.2000 № 344;

– квитанции об оплате лицензионного сбора;

– 2 черно-белые фотографии 3х4 см;

– охотничий билет или членский охотничий билет для приобретения охотничьего огнестрельного оружия с нарезным стволом.

Сроки лицензии на приобретение и хранение оружия, лицензии на приобретение оружия и патронов к нему – 6 месяцев, рассмотрения заявления о выдаче лицензии – 1 месяц, действия лицензии на хранение или хранение и ношение оружия – 5 лет.

Пассивные средства защиты – это бронежилеты, шокеры, газовые баллончики, дубинки, щиты и шлемы.

Основу бронежилета составляет высокопрочная ткань кевлар (отечественный аналог ткани СВМ), сложенная в 5 - 40 слоев, нити такой ткани "работают" на растяжение, поглощая энергию пули. В слоях ткани оставляют специальные карманы-ниши, в которые вкладывают пластины из легкой брони. В зависимости от назначения бронежилеты различаются по степени (по площади) и уровню защиты, массе и характеру камуфляжа. По стойкости к воздействию поражающих факторов и уровню защиты в соответствии с ГОСТ Р 50744-95 "Бронеодежда. Классификация и общие технические требования" существует восемь классов защиты: 1, 2, 2А, 3, 4, 5, 6 и специальный класс.

Средства 6 класса предназначены для защиты от пуль автоматического оружия, в том числе снайперской винтовки СВД со стальным термоупрочненным сердечником.

Средства 5 класса – для защиты от автоматных пуль, в том числе от АКМ со стальным термоупрочнённым сердечником; пистолетных пуль и пуль охотничьих ружей всех отечественных систем и калибров; холодного оружия и метаемых предметов.

Средства 4 класса – для защиты от автоматных пуль, в том числе от АК-74 со стальным термоупроченным сердечником, снайперской винтовки СВД со стальным сердечником; охотничьих ружей и пистолетных пуль; холодного оружия и метаемых предметов.

Средства 3 класса – для защиты от автоматных пуль, в том числе от АК-74 и АКМ со стальным сердечником, охотничьих ружей, пистолетных пуль, холодного оружия и метаемых предметов.

Средства 2 класса – для защиты от пуль пистолетов специального малокалиберного ПСМ, ТТ, имеющих стальной сердечник, охотничьих ружей, холодного оружия, метаемых предметов.

Средства класса 2А – для защиты от свинцовых пуль охотничьих ружей (12 калибр), холодного оружия, метаемых предметов;

Средства 1 класса – для защиты от пуль пистолетов ПМ, револьверов типа "наган" и других отечественных, имеющих равную или меньшую дульную энергию, холодного оружия, метаемых предметов.

Средства специального класса предназначены для защиты от холодного оружия (нож, заточка и т.д.), метаемых предметов.

Полицейские дубинки используются для нанесения ударов и защиты от них, а также для контроля и удержания противника. В зависимости от модели дубинки, её конструкция, материал, вес, длина и толщина могут быть различными. Ранее полицейские дубинки изготавливали из прочных пород дерева, в настоящее время их чаще всего делают из резины и полимерного синтетического материала, реже из пластика, ещё реже – металлические.

Резиновые дубинки бывают гибкие и негибкие, в последние может быть вставлен металлический стержень-сердечник или же трубка, по которой перекатываются стальные шарики. Металлические дубинки – чаще всего телескопические, различной гибкости, длиной от 20 см в сложенном до 60 см в боевом положении (раздвигаться они могут вручную или же автоматически, под действием пружины).

Во многих западных странах в ходу дубинка, имеющая металлический стержень, окруженный резиной. Оканчивается она гибким участком из резины или кожи (иногда со свинцом). С помощью этого оружия, как правило, наносят оглушающие удары.

Наконец, на вооружении правоохранительных органов ряда западных стран находятся спецсредства в виде полицейских дубинок, при нажатии на спусковую кнопку «стреляющих» зарядом ирританта. Также существуют модели дубинок со встроенным электрошокером.

Большинство современных дубинок обычно имеют выделенную рукоять и ременную петлю, благодаря которой дубинка не выскакивает из рук владельца. Рукоять, как правило, рассчитана на одну руку.

Перчатки для перехвата ножа обычно имеют металлическое покрытие с внутренней стороны в виде прочной металлической сетки. Такой перчаткой можно перехватить нож за лезвие, не повредив руки.

Активные средства нетравматического действия – это газовые баллончики с аэрозольным наполнением (рис. 4) и шокеры.

Газовые баллончики – гражданское газовое оружие самообороны, аэрозольное устройство, снаряженное слезоточивыми или раздражающими веществами (ирритантами), предназначенное для самообороны от людей и агрессивных животных (собак, а в некоторых странах производятся специальные баллончики от медведей, увеличенного объёма и дальности действия). Газовые баллончики являются эффективным и самым популярным средством самообороны, просты и удобны в применении, обладают небольшими габаритами и массой и могут быть успешно использованы без продолжительных тренировок и подготовки. Не требуют специальных разрешений, доступны для покупки в специализированных магазинах всем совершеннолетним гражданам РФ.

Рис. 4. Внешний вид газовых баллончиков

Баллончики разделяются по типу используемого в них вещества и варианту распыления. Внутри может содержаться либо слезоточивый газ (SC), либо вытяжка из жгучего перца (OC). Тот и другой состав действуют на слизистые органов дыхания и глаза, вызывая спазмы горла, обильное слезотечение, жжение, кашель. Кроме того, выпускаются перцовые баллончики с синтетической вытяжкой перца – морфолидомпеларгоновой

кислоты (МПК). По своему воздействию МПК схож с природным экстрактом, но считается несколько более слабым. По способу распыления баллончики делятся на струйные и аэрозольные. Первый выдает концентрированную струю и требует определенной меткости, а второй распыляет между владельцем и нападающим защитное облако сравнительно большой площади.

Применение газовых баллончиков ограничено местом, где происходит нападение. Так, на свежем воздухе газовый баллончик можно относительно безопасно применять для самого себя, а в закрытых помещениях гарантированно можно надышаться раздражающим веществом. Помимо этого, нужно так же учитывать направление и скорость ветра при распылении раздражающего вещества, чтобы не только попасть по нападающему, но и чтобы не попасть на себя.

Струйными баллончиками можно пользоваться и в закрытых помещениях, и при сильном ветре, даже встречном. Помимо этого струйные газовые баллончики имеют большую дальность действия. Их можно использовать в подъездах, в лифтах и так далее, конечно, слизистая охранника и в этом случае будет раздражена, но явно не так, как при распылении аэрозольного баллончика.

Необходимо учитывать, что некоторые типы начинки не действуют на собак и людей в состоянии алкогольного опьянения.

Спектр электрошокерных устройств (ЭШУ), отличающихся характеристиками и ценой, очень широк. Применение их на территории Российской Федерации регулирует ГОСТ Р 50940-96 "Устройства электрошоковые. Общие технические условия". Настоящий стандарт распространяется на электрошоковые устройства отечественного производства, предназначенные для использования в целях самообороны, и защитные электрошоковые устройства отечественного производства, предназначенные для защиты (охраны) стационарных и подвижных объектов гражданского и ведомственного назначения от несанкционированного проникновения и воздействия.

Биофизическое действие электрошокера связано не только с болью от поражения током. Энергия, накопленная в шокере, при контакте дуги с кожей преобразуется в переменное электрическое напряжение со специально рассчитанной частотой, вынуждающей мышцы в зоне контакта сокращаться чрезвычайно быстро. Эта ненормальная сверхактивность мышц приводит к молниеносному разложению сахара крови, который питает мышцы. Иными словами, мышцы в зоне контакта на какое-то время теряют работоспособность. Параллельно импульсы блокируют деятельность нервных волокон, по которым мозг управляет данными мышцами.

Основной параметр, характеризующий свойства электрошокеров, – напряжение на электродах. В России, согласно принятому в 1996 г. стандарту, установлены три группы электрошокеров: 1-я – с напряжением хо-

лостого хода от 50 до 60 кВ, 2-я – с напряжением от 35 до 50 кВ, 3-я – с напряжением менее 35 кВ. Электрошокеры третьей группы – это скорее средство оказания психологического воздействия, чем реальное оружие. Большинство выпускаемых для продажи отечественных электрошокеров относится ко второй группе. Зарубежные производители электрошокеров объявляют напряжение 200-250 кВ.

Шокеры выпускаются в двух базовых конфигурациях: прямые (рис. 5) и Г-образные. Не существует никаких научных доводов, какая форма лучше. Одни предпочитают Г-образные, так как им кажется, что таким шокером легче прикоснуться к противнику. Другие выбирают прямые, как дающие максимальную свободу движений, относительно короткие или длинные, напоминающие полицейскую дубинку.

Примененный электрошокер оставляет на обнаженной коже хорошо заметный красный след, причем след этот больше в случае, если электроды не касались кожи. Электрическая дуга приводит к распространению отпечатка на большую поверхность. Под электродами образуются яркие красные пятна диаметром 3 - 5 мм, иногда с припухлостями. Но абсолютно все следы воздействия на коже исчезают максимум через 2 ч, и лишь в одном случае следы сохранялись более суток. Но, так или иначе, никакие исследования не могут отыскать отпечатков или нарушений в тканях спустя 48 ч независимо от того, к какой части тела прикладывалось воздействие. Инструкции по пользованию советуют для достижения полного поражения противника удерживать работающий электрошокер в контакте с ним 2 - 3 с (что, кстати, расходится со стандартом). По мнению производителей, мгновенного касания недостаточно для поражения противника. Но обязательным условием при этом является удержание в течение указанного времени самого противника. Как показали исследования, наиболее эффективна защита с помощью электрошокеров от нападения животных (агрессивных собак и т.п.), поскольку их нервная система более чувствительна к воздействию электрического тока, нежели нервная система человека.

Основные характеристики ЭШУ – напряжение (измеряется в вольтах «В», киловольтах (1000 В) «кВ») и сила тока (измеряется в амперах «А», миллиамперах (1/1000 А) мА и т.д.). При перемножении этих величин получается мощность, измеряемая в ваттах (Вт). Напряжение не несет на себе каких-либо поражающих факторов. Зато от его величины будет зависеть размер электрической дуги и, соответственно, пробивная способность через множество слоев одежды. Диапазон напряжения электрошокеров лежит в пределах 50 - 200 кВ. Эффект поражения создает прежде всего значение силы тока, проходящего через организм человека.

К основным поражающим факторам электрошокера относят:

- болевой шок, который может сохраняться еще некоторое время после прекращения воздействия электрошокера. В результате сильных боле-

вых ощущений человек перестает оказывать активные попытки нападения или бегства;

- судорожное сокращение мышц под действием электрического разряда приводит к их временной парализации;

- возможна потеря ориентации, заторможенность реакций, а в некоторых случаях даже потеря сознания.

Согласно ГОСТ Р 50940-96 средняя мощность электрошокера не должна превышать 3 Вт, поэтому приходится подбирать производителям такие значения силы тока и напряжения, чтобы в итоге при их перемножении не было больше 3 Вт. Для органов внутренних дел и внутренних войск МВД России величина максимальной выходной мощности немного выше и составляет 10 Вт.

Существуют миниатюрные разрядники 1-го класса, умещающиеся на ладони. Это скорее изделия, производящие отпугивающее действие при незначительном болевом эффекте. Малогабаритные разрядники 2-го класса – это изделия с более высокой электрической мощностью, которые при воздействии обеспечивают вполне ощутимый болевой эффект, проявляющийся в течение 2...10 с после прекращения воздействия. Достоинствами изделий данного класса являются миниатюрность (умещаются в кармане), надежность, отсутствие необходимости перезаряжать источник питания (достаточно сменить батарейку), относительно низкая стоимость. Недостатки: отсутствие эффекта "удлинения руки", отсутствие нейтрализующего воздействия. Еще один недостаток большинства ЭШУ 2-го класса – наличие остаточного напряжения на выходных электродах после отключения прибора, что небезопасно для владельца.

Рис. 5. Внешний вид электрошокеров

Малогабаритные разрядники 3-го класса (их еще часто называют "электрошоковыми дубинками") наиболее популярны среди сотрудников частных охранных агентств. Главные их достоинства – обеспечение

нейтрализующего воздействия и эффекта "удлинения руки" при габаритах и массе, позволяющих носить изделия в кейсе, сумке или в руке (будучи упакованными в капроновый чехол, они не отличаются по внешнему виду от мужских или женских складных зонтиков).

Эти изделия снабжены встроенной аккумуляторной батареей и зарядным устройством (встроенным или внешним). Используемые аккумуляторные батареи обеспечивают от 100 до 200 циклов воздействия (каждый цикл воздействия, то есть "выстрел", обычно не превышает 3 с), после чего их необходимо перезарядить (процесс перезаряда составляет от 8 до 14 ч). Примером ЭШУ 3-го класса являются хорошо известные изделия серии "ЯНА" и искровые разрядники АИР-107 "Скорпион" и АИР-140 "Мальвина".

Хорошо зарекомендовал себя стреляющий электрошокер «Каракурт-А» (рис. 6) – отличное безопасное оружие для помещений с большим количеством людей. Форма пистолетной рукоятки – испытанная веками форма, делающая оружие удобным. Его можно использовать как стреляющий, установив на него картриджи «БТЭР» или «КС». Носить «Каракурт» незаметно для окружающих можно в кармане или в поясном чехле. Источником питания служит Ni-MH аккумулятор, который следует подзаряжать раз в год, если им долго не пользоваться или после каждого применения. Ниже (на рис. 6) показан внешний вид электрошокера «Каракурт» с картриджем дистанционного действия.

Рис. 6. Внешний вид электрошокера «Каракурт»

Особым представителем ЭШУ 3-го класса является разрядник "Эйр Тэйзер". Это изделие принципиально отличается от всех других наличием выбрасываемых на расстояние до четырех метров внешних электродов, электрическое напряжение на которые подается с помощью миниатюрных токоведущих проводников (аналогичных леске, "выстреливаемой" катушкой спиннинга), что позволяет защищаться на дистанции. Такой "выстрел" можно произвести один раз, после чего следует либо сменить картридж,

содержащий барабан с токоведущими проводами, и средство выброса – пружину или пневматическое устройство, либо пользоваться устройством, как обычным разрядником.

ЭШУ 4-го класса – это изделия с повышенными массогабаритными характеристиками и выходной мощностью, предназначенные для применения сотрудниками организаций с особыми уставными задачами (вместо резиновых и пластиковых палок).

ЭШУ 5-го класса – это оружие специального назначения.

Активные средства травматического действия – это травматическое и огнестрельное оружие. Для физической защиты чаще всего используют огнестрельное травматическое оружие (огнестрельное оружие ограниченного поражения), иногда служебное.

Огнестрельное оружие ограниченного поражения с патронами травматического действия – это газовые пистолеты и револьверы с возможностью стрельбы патронами с резиновой пулей. До этого считалось как травматическое. С 1 июля 2011 г. для обозначения данной категории оружия Федеральным законом «Об оружии» было введено понятие «огнестрельного оружия ограниченного поражения» (ОООП); может быть бесствольное и под патрон центрального воспламенения. Выбор таких пистолетов очень разнообразен, но чаще всего в России применяются из бесствольных ПБ-4 ОСА, ПБ-2 "Эгида", МР-461 "Стражник", "Кордон". Под патрон центрального воспламенения – ИЖ-78-9Т (и его модификации), ИЖ-79-9Т "Макарыч" (и его модификации), ВПО-501 "Лидер", револьвер ММРТ-2 "Овод".

Первый образец гражданского травматического оружия – пистолет ПБ-4 ОСА был сертифицирован в 1999 г. В 2004 г. был сертифицирован первый образец травматического оружия под патрон центрального воспламенения – "газовый пистолет с возможностью стрельбы резиновой пулей" ИЖ-79-9Т "Макарыч". По состоянию на 2013 г. в РФ зарегистрировано свыше 730 тыс. единиц ООПП.

Эффективность "Осы" (рис. 7) обеспечивается большим диаметром ее пули – 18 мм с установленным внутриметаллическим стержнем. Её выстрел с расстояния 2 м равносилен силе удара кулака боксера тяжелого веса.

Рис. 7. Внешний вид бесствольного травматического пистолета "Оса"

Для физической защиты охранников вооружают иногда служебным оружием. Это оружие, предназначено для использования должностными лицами, которым законодательством Российской Федерации разрешено ношение, хранение и применение указанного оружия, в целях самообороны или для использования возложенных на них федеральным законом обязанностей по защите жизни и здоровья граждан, собственности, по охране природы и природных ресурсов, ценных и опасных грузов, специальной корреспонденции. К служебному оружию относится огнестрельное гладкоствольное и нарезное короткоствольное оружие отечественного производства с дульной энергией не более 300 Дж, а также огнестрельное гладкоствольное длинноствольное оружие. Служебное оружие должно исключать ведение огня очередями, нарезное служебное оружие должно иметь отличия от боевого ручного стрелкового оружия по типам и размерам патрона, а от гражданского – по следообразованию на пуле и гильзе. Емкость магазина (барабана) служебного оружия должна быть не более 10 патронов. Пули патронов к огнестрельному гладкоствольному и нарезному короткоствольному оружию не могут иметь сердечников из твердых материалов. Патроны к служебному оружию должны соответствовать требованиям государственных стандартов.

Контроль и управление доступом теряют всякий смысл без идентификации пользователя системы. В последнее время начинают получать распространение биометрические системы контроля доступа. Они позволяют оценивать физиологические характеристики человека.

Большинство современных систем контроля и управления доступом имеют в своем составе ряд модулей, позволяющих осуществлять учет рабочего времени, интегрируемых с бухгалтерскими программами, базами данных бюро пропусков. Также возможно их совместное использование с системами охранно-пожарной сигнализации, видеонаблюдения.

4. ДОКУМЕНТИРОВАННОЕ СОПРОВОЖДЕНИЕ МЕР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Согласно установленным российским законодательством правилам любое предприятие должно иметь комплект типовых документов по информационной безопасности – средства для документирования всех ключевых областей обеспечения информационной безопасности. Таким комплектом может быть «Руководство по защите информации» или «Положение о порядке организации и проведения работ по защите информации». В этих документах должен предусматриваться порядок защиты информации, а также порядок разработки, ввода в действие и эксплуатацию объектов информатизации, ответственность должностных лиц за своевременность и качество формирования требований по технической защите информации.

В учреждении (на предприятии) также должен быть документально оформлен перечень сведений конфиденциального характера, подлежащих защите в соответствии с нормативными правовыми актами, а также разработана соответствующая разрешительная система доступа персонала к такого рода сведениям.

Наличие этих документов и проведение различных мероприятий, согласно этой документации поможет избежать неприятностей при проверках различными инстанциями контролирующими сферу информационной безопасности. Ниже приведены перечни документов, необходимых для обеспечения безопасности обработки персональных данных и безопасного функционирования информационной системы.

4.1. Перечень документов, необходимых для обеспечения защиты персональных данных

Для обеспечения защиты персональных данных необходим следующий перечень документов:

- План мероприятий по организации защиты персональных данных;
- Положение о (защите) персональных данных (ПДн) предприятия;
- Приказ о введении в действие «Положения о персональных данных»;
- Приказ о назначении лиц, ответственных за обеспечение безопасности ПДн;
- Доработанные должностные инструкции всех лиц, ответственных за обеспечение безопасности ПДн;
- Приказ о создании комиссии по классификации ИСПДн;
- Акт классификации ИСПДн на предприятии;
- Модель угроз безопасности ИСПДн;
- Модель нарушителя ИСПДн;
- Приказ об определении мест хранения материальных носителей ПДн, обрабатываемых без использования средств автоматизации;
- Приказ об определении мест хранения материальных носителей ПДн, обрабатываемых с использованием средств автоматизации;
- Приказ о создании комиссии по уничтожению ПДн и материальных носителей ПДн;
- Журнал учета материальных носителей ПДн, обрабатываемых с использованием средств автоматизации;
- Акт уничтожения (обезличивания) ПДн субъекта;
- Акт уничтожения материального носителя ПДн;
- Приказ о допуске работников (ответственных исполнителей) к обработке ПДн на предприятии;

- Доработанные должностные инструкции всех работников, допускаемых к обработке ПДн;
- Приказ о создании комиссии по проведению проверок состояния защиты (контролю защищенности) ИСПДн;
- Инструкция по проведению проверок состояния защиты ИСПДн;
- План внутренних проверок состояния защиты ИСПДн на текущий год;
- Инструкция администратора информационной безопасности ИСПДн;
- Инструкция администратора ИСПДн;
- Инструкция по антивирусной защите ИСПДн;
- Инструкция по резервному копированию и восстановлению баз данных ИСПДн;
- Инструкция по модификации программного обеспечения и технических средств ИСПДн;
- Порядок парольной защиты ИСПДн;
- Инструкция администратора информационной безопасности по внесению изменению в списки уполномоченных пользователей ИСПДн;
- Инструкция пользователю по действиям в нештатных ситуациях;
- Положение об использовании сети Интернет на предприятии;
- Инструкция по обработке ПДн посетителей;
- Журнал учета посетителей предприятия;
- Журнал учета письменных запросов субъектов к ПДн;
- Журнал учета средств криптографической защиты, используемых на предприятии;
- Приказ о вводе в промышленную эксплуатацию системы защиты ИСПДн.

4.2. Документация общеинструктивного характера отдела информационных технологий

На предприятии в должностных инструкциях должна быть отражена специфика предприятия информационных технологий. Необходимы следующие должностные инструкции:

1) должностная инструкция начальника отдела информационных технологий;

2) должностная инструкция инженера-электроника отдела информационных технологий;

3) положение о конфиденциальной информации;

4) положение об использовании информационной системы;

5) положение об использовании мобильных устройств и носителей информации;

6) положение об использовании программного обеспечения;
7) положение об использовании сети интернет;
8) положение об использовании электронной почты;
9) положение об отделе информационных технологий;
10) трудовой договор.

А также:

1) должностная инструкция инженера-программиста;
2) должностная инструкция администратора информационных систем предприятия;
3) должностная инструкция инженера по безопасности информации;
4) должностная инструкция оператора ПЭВМ;
5) должностная инструкция техника-программиста;
6) инструкция администратора информационной безопасности;
7) инструкция администратора.

Для документации, касающейся серверного помещения, необходимы следующие документы, разработанные на основе «Специальных требований и рекомендаций по технической защите конфиденциальной информации» (СТР-К), принятых Государственной технической комиссией при Президенте Российской Федерации, решение коллегии Гостехкомиссии России № 7.2/02.03.2001 г.:

1) приказ о назначении комиссии по сопровождению аттестации автоматизированной системы;
2) перечень автоматизированных систем, используемых для обработки конфиденциальной информации и защищаемых помещений, в которых проводятся конфиденциальные мероприятия;
3) перечень сведений конфиденциального характера;
4) акт классификации автоматизированной системы (АС);
5) схема границы контролируемой зоны;
6) перечень лиц, обслуживающих автоматизированную систему;
7) приказ о назначении администратора информационной безопасности (уполномоченного по защите информации);
8) данные по уровню подготовки кадров, обеспечивающих защиту информации;
9) инструкция по обеспечению защиты конфиденциальной информации, обрабатываемой в автоматизированных системах;
10) состав программного обеспечения автоматизированной системы;
11) перечень лиц, имеющих право самостоятельного доступа в помещение №____ с автоматизированной системой;
12) перечень лиц, имеющих право самостоятельного доступа к штатным средствам автоматизированной системы;
13) технический паспорт автоматизированной системы;

14) перечень защищаемых ресурсов автоматизированной системы и уровень их конфиденциальности;

15) матрица доступа субъектов автоматизированной системы к ее защищаемым информационным ресурсам;

16) описание настроек системы разграничения доступа системы защиты информации от несанкционированного доступа автоматизированной системы;

17) описание технологического процесса обработки информации в автоматизированной системе.

4.3. Инструкция начальника отдела по защите информации

В случае создания специального отдела по защите информации, необходимо разработать должностную инструкцию начальника отдела по защите информации следующего характера.

I Общие положения

1. Назначение на должность начальника отдела по защите информации производится приказом руководителя организации.

2. Требования к квалификации. Высшее профессиональное (техническое) образование и стаж работы по защите информации на инженерно-технических и руководящих должностях не менее 5 лет.

3. Начальник отдела по защите информации должен знать:

– действующее законодательство о государственной тайне и защите информации;

– постановления правительства, определяющие основные направления экономического и социального развития отрасли;

– руководящие, нормативные и методические материалы по вопросам, связанным с обеспечением защиты информации;

– перспективы развития, специализацию и направления деятельности предприятия и их подразделений;

– специфику выпускаемой на предприятиях отрасли продукции и технологические особенности ее изготовления;

– характер взаимодействия подразделений в процессе исследований и разработок и порядок прохождения служебной информации;

– организацию комплексной защиты информации в отрасли, на предприятии;

– перспективы и направления развития технических средств защиты информации;

– методы и средства контроля охраняемых сведений, выявления каналов утечки информации, организацию технической разведки;

– порядок финансирования, методы планирования и организации проведения научных исследований и разработок, выполнения работ по защите информации;

– порядок заключения договоров на проведение специальных исследований и проверок, работ по защите технических средств передачи, обработки, отображения и хранения информации;

– достижения науки и техники в стране и за рубежом в области технической разведки и защиты информации;

– экономику, организацию производства, труда и управления;

– действующие системы оплаты труда и материального стимулирования; правила и нормы охраны труда.

II Должностные обязанности

Организует разработку и внедрение организационных и технических мероприятий по комплексной защите информации на предприятиях, ведущих работы, содержание которых составляет государственную или коммерческую тайну, обеспечивает соблюдение режима проводимых работ и сохранение конфиденциальности документированной информации.

Возглавляет разработку проектов перспективных и текущих планов работы, составление отчетов об их выполнении.

Руководит проведением работ по организации, координации, методическому руководству и контролю их выполнения по вопросам защиты информации и разработкой технических средств контроля, определяет перспективы их развития.

Обеспечивает взаимодействие и необходимую кооперацию соисполнителей работ по вопросам организации и проведения научно-исследовательских и опытно-конструкторских разработок, организует и контролирует выполнение плановых заданий, договорных обязательств, а также сроки, полноту и качество работ, выполняемых соисполнителями.

Организует работу по заключению договоров на работы по защите информации, принимает меры по обеспечению финансирования работ, в том числе выполняемых по договорам.

Обеспечивает участие подразделения в разработке технических заданий на выполняемые на предприятии исследования и разработки, формулирует цели и задачи работы по созданию безопасных информационных технологий, отвечающих требованиям комплексной защиты информации.

Организует проведение специальных исследований и контрольных проверок по выявлению демаскирующих признаков и возможных каналов утечки информации, в том числе по техническим каналам, разрабатывает меры по их устранению и предотвращению, а также работу по составлению актов и другой технической документации о степени защищенности технических средств и помещений.

Контролирует соблюдение нормативных требований по надежной защите информации, обеспечивает комплексное использование технических средств, методов и организационных мероприятий.

Организует рассмотрение применяемых и предлагаемых методов защиты информации, промежуточных и конечных результатов исследований и разработок.

Совершенствует планирование, контроль и организацию выполнения работ, обеспечивает использование в них достижений отечественной и зарубежной науки и техники, передового опыта.

Обеспечивает выполнение плановых заданий с наименьшими затратами материальных и финансовых ресурсов, рациональное расходование фонда заработной платы.

Согласовывает проектную и другую техническую документацию на вновь строящиеся и реконструируемые здания и сооружения в части выполнения требований по защите информации.

Определяет потребность подразделения в оборудовании, материальных, финансовых и других ресурсах, необходимых для проведения работ, и контролирует рациональное использование и сохранность аппаратуры, приборов и другого оборудования.

Обеспечивает высокий научно-технический уровень работ, эффективность и качество исследований и разработок.

Осуществляет контроль за выполнением предусмотренных мероприятий, анализ материалов контроля, выявление нарушений, разрабатывает и участвует в реализации мер по устранению выявленных недостатков по защите информации.

Организует проведение аттестации объектов, помещений, технических средств, программ, алгоритмов на предмет соответствия требованиям защиты информации по соответствующим классам безопасности, обеспечивает представление в установленном порядке действующей отчетности.

Участвует в подборе кадров, оценке деятельности и аттестации работников подразделения.

Определяет направления деятельности подразделений, входящих в состав отдела, организует и координирует их работу.

Осуществляет рациональную расстановку кадров с учетом квалификации и деловых качеств работников, принимает меры по повышению их квалификации и творческой активности.

Обеспечивает ведение делопроизводства в соответствии с установленным порядком, соблюдение действующих инструкций по режиму работ и своевременно принимает меры по предупреждению нарушений.

Следит за безопасным проведением работ, соблюдением правил и норм охраны труда.

Руководит работниками подразделения.

III Права

Начальник отдела (лаборатории, сектора) по защите информации имеет право:

1. Издавать распоряжения в пределах своей компетенции.

2. Вносить на рассмотрение руководства предложения по совершенствованию работы, связанной с предусмотренными настоящей должностной инструкцией обязанностями.

3. Сообщать руководителю организации о всех выявленных в процессе исполнения своих должностных обязанностей недостатках и вносить предложения по их устранению.

4. Подписывать и визировать документы в пределах своей компетенции.

5. Вносить на рассмотрение руководителя организации:

5.1. Представления о назначении, перемещении и освобождении от занимаемых должностей подчиненных ему работников.

5.2. Предложения:

- о поощрении отличившихся работников;

- о наложении взысканий на нарушителей производственной, технологической и трудовой дисциплины.

IV Ответственность

Начальник отдела (лаборатории, сектора) по защите информации несет ответственность:

1. За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей должностной инструкцией, – в пределах, определенных действующим трудовым законодательством Российской Федерации.

2. За правонарушения, совершенные в процессе осуществления своей деятельности, – в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.

3. За причинение материального ущерба – в пределах, определенных действующим трудовым и гражданским законодательством Российской Федерации.

5. АППАРАТНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Под аппаратными средствами защиты понимаются специальные средства, непосредственно входящие в состав технического обеспечения и выполняющие функции защиты как самостоятельно, так и в комплексе с другими средствами, например с программными. Можно выделить некоторые наиболее важные элементы аппаратной защиты:

1) защита от сбоев в электропитании;

2) защита от сбоев серверов, рабочих станций и локальных компьютеров, сетевых карт и т.д.;

3) защита от сбоев дисковых систем, устройств для хранения информации;
4) защита от утечек информации, несанкционированного доступа.

5.1. Защита от сбоев в электропитании и бросков напряжения

Для защиты от сбоев в электропитании используют:
- источники бесперебойного питания (UPS);
- резервные бензиновые или дизель-генераторы;
- резервные линии электропитания.

Источники бесперебойного питания различны по своим техническим и потребительским характеристикам, могут обеспечить питание всей локальной сети или отдельного компьютера в течение какого-то промежутка времени, достаточного для восстановления подачи напряжения или для сохранения информации.

В противном случае используется следующая функция подобных устройств – компьютер получает сигнал, что UPS перешел на работу от собственных аккумуляторов, и время такой автономной работы ограничено. Тогда компьютер выполняет действия по корректному завершению всех выполняющихся программ и отключается.

Большинство источников бесперебойного питания (рис. 8) одновременно выполняют функции и стабилизатора напряжения, что является дополнительной защитой от скачков напряжения в сети. Многие современные сетевые устройства – серверы, концентраторы и т.д. – оснащены собственными дублированными системами электропитания.

Рис. 8. Внешний вид источников бесперебойного питания

Крупные организации имеют собственные аварийные электрогенераторы или резервные линии электропитания. Эти линии подключены к разным подстанциям, и при выходе из строя одной них электроснабжение осуществляется с резервной подстанции. Ниже показан внешний вид некоторых генераторов небольшой мощности (рис. 9).

Для защиты источника питания от бросков напряжения применяют сетевые фильтры.

Рис. 9. Внешний вид бензиновых генераторов небольшой мощности

Основное назначение сетевых фильтров состоит в защите системы от бросков питания. UPS необходим для защиты от провалов питания, повышения напряжения и отключения питания. Большинство из них может справляться с повышением напряжения до 800 В. Чтобы подавлять более сильные броски питания, нужен сетевой фильтр. Большинство сетевых фильтров отводят броски питания через заземление, что не всегда желательно. Другие фильтры используют для этого конденсаторы, а заземление используется для защиты самого фильтра. Защита от бросков питания должна предохранять от пиковых выбросов до 6000 В. Фильтры часто оборудуются EMI (средства подавления электромагнитных помех) и RFI (средства подавления радиопомех). Однако блоки питания большинства настольных систем обычно уже включают в себя такой тип фильтрации, поэтому к таким средствам нужно подходить скептически.

5.2. Защита от сбоев процессоров

Один из методов такой защиты – это резервирование особо важных компьютерных подсистем. Для резервирования процессоров применяют симметричное мультипроцессирование.

В системе используется более двух процессоров, и в случае сбоя одного из них, второй продолжает работу так, что пользователи вычислительной системы даже ничего не замечают. Естественно, на такую защиту требуется гораздо больше средств и она стоит дороже.

Использование аппаратной защиты может быть и таким:

1) установка на разъем специальной заглушки, содержащей микросхему и, возможно, элемент питания. Программа проверяет наличие этой заглушки путем проведения специального протокола обмена между ними.

Снятие защиты заключается либо в имитации заглушки, либо в ее воспроизводстве, либо в обнаружении и нейтрализации подпрограммы проверки ее наличия;

2) наличие платы защиты, вставляемой в слот ПЭВМ. Эту защиту практически невозможно обойти, но такая плата слишком дорога для широкого применения.

5.3. Защита от сбоев устройств хранения информации

Организация надежной и эффективной системы резервного копирования и дублирования данных является одной из важнейших задач по обеспечению сохранности информации. Для защиты от сбоев устройств хранения информации применяют:

- компакт-диски многоразового использования;
- флешки;
- резервные переносные жесткие диски.

В крупных корпоративных сетях устанавливается специализированный архивационный сервер.

В небольших сетях, где установлены один-два сервера, чаще всего применяется установка системы резервного копирования непосредственно в свободные слоты серверов.

Специалисты рекомендуют хранить дубликаты архивов наиболее ценных данных в другом здании, на случай пожара или стихийного бедствия.

В некоторых случаях, когда подобные сбои и потеря информации могут привести к неприемлемой остановке работы, применяется система зеркальных винчестеров. Резервная копия информации формируется в реальном времени, то есть в любой момент времени при выходе из строя одного винчестера система сразу же начинает работать с другим.

Вместе с тем кроме аппаратных средств резервного копирования данных существуют и чисто программные средства архивации.

6. ТЕХНИЧЕСКАЯ РАЗВЕДКА И ПРОТИВОДЕЙСТВИЕ

Одним из важных средств добывания информации является техническая разведка, проводимая с помощью разнообразных специальных технических устройств. Вид применяемых технических средств разведки зависит, прежде всего, от физической природы и особенностей демаскирующих признаков объектов, являющихся источниками информации.

По используемым техническим средствам в технической разведке различают следующие основные виды разведки:

- оптико-электронную,
- радиоэлектронную,

– электромагнитную,

– компьютерную,

– гидроакустическую.

Оптико-электронная разведка – это разведка с помощью видеосистем и оптических систем с электронными схемами обработки полученных изображений.

Радиоэлектронная разведка − это процесс получения информации в результате приема и анализа электромагнитных излучений (ЭМИ) радиодиапазона, создаваемых работающими радиоэлектронными средствами (РЭС). Такая разведка в частности активно использовалась в Великую отечественную войну. Радисты прослушивали эфир, запоминали почерк работы радистов дивизий Вермахта и по их исчезновению или появлению устанавливали передислокацию этих дивизий.

Электромагнитная разведка перехватывает и анализирует электромагнитные излучения от кабелей, проводов и других излучателей.

Компьютерная разведка добивается своей цели с помощью специального программного обеспечения, позволяющего получить несанкционированный доступ к информации по каналам связи, компьютерным сетям.

Под гидроакустической разведкой понимается получение информации путем приема и анализа акустических сигналов инфразвукового, звукового и ультразвукового диапазонов, распространяющихся в водной среде от надводных и подводных объектов.

В целом техническая разведка использует следующие факторы:

- подслушивание разговоров в помещении или автомашине с помощью предварительно установленных "радиожучков" или диктофонов;
- контроль телефонов, телефаксных линий связи, радиотелефонов и радиостанций;
- дистанционный съем информации с различных технических средств в первую очередь с мониторов и печатающих устройств компьютеров и другой электронной техники;
- лазерное облучение оконных стекол в помещении, где ведутся "интересные разговоры" или, например, направленное радиоизлучение, которое может заставить "откликнуться и заговорить" детали в телевизоре, в радиоприемнике или другой технике.

6.1. Источники информации для технической разведки

Источниками информации для технической разведки являются:

– физические поля, возникающие в результате функционирования объектов разведки;

– производственные отходы и химические выбросы объектов разведки;

– видовые и конструктивные особенности объектов разведки.

Формы представления информации зависят от ее характера и физических носителей, на которых она представлена. Основными формами информации, подлежащими защите, являются:

– документальные,
– акустические,
– телекоммуникационные,
– видовые.

Носителем информации в оптическом канале является электромагнитное поле (фотоны) в диапазоне 0,46 – 0,76 мкм (видимый свет) и 0,76 – 13 мкм (инфракрасные излучения).

В радиоэлектронном канале утечки информации в качестве носителей используются электрические, магнитные и электромагнитные поля в радиодиапазоне, а также электрический ток (поток электронов), распространяющийся по металлическим проводам. Диапазон колебаний носителя этого вида чрезвычайно велик: от звукового диапазона до десятков ГГц.

В соответствии с видами носителей информации радиоэлектронный канал целесообразно разделить на два подвида: электромагнитный канал, носителями информации в котором являются электрическое, магнитное и электромагнитное поля, и электрический канал, носитель информации в котором электрический ток.

Носителями информации в акустическом канале являются упругие акустические волны в инфразвуковом (менее 16 Гц), звуковом (16 Гц – 20 кГц) и ультразвуковом (свыше 20 кГц) диапазонах частот, распространяющиеся в атмосфере, воде и твердой среде.

Когда речь идет о распространении за пределы организации отходов производства, следует отличать технический канал утечки от агентурного, в рамках которого вынос носителя с информацией производится проникшим к источнику злоумышленником, завербованным сотрудником организации или сотрудником, стремящимся продать информацию любому ее покупателю. Граница между агентурным и техническим каналом утечки достаточно условна, однако при утечке информации в агентурном канале переносчиком информации является лицо, сознающее противоправные действия, а в техническом вещественном канале носители вывозятся из организации с целью освобождения ее от отходов, или отходы распространяются в результате действия природных сил. В качестве таких сил могут быть воздушные потоки, разносящие выбрасываемые трубами газообразные отходы, или водные потоки рек или водоемов, куда сбрасываются недостаточно очищенные жидкие или взвешенные в воде твердые частицы демаскирующих веществ.

Каждый из технических каналов имеет свои особенности, которые необходимо знать и учитывать для обеспечения эффективной защиты информации от ее утечки.

Технический канал утечки информации, состоящий из передатчика, среды распространения и приемника, является простым или одноканальным. Однако возможны варианты, когда утечка информации происходит более сложным путем – по нескольким последовательным или параллельным каналам. В этом случае канал можно назвать составным. При этом используется свойство информации переписываться с одного носителя на другой. Например, если в кабинете ведется конфиденциальный разговор, то утечка возможна не только по акустическому каналу через стены, двери, окна, но и по оптическому – путем съема информации лазерным лучом со стекла окна или по радиоэлектронному каналу связи с использованием установленной в кабинете радиозакладки. В двух последних вариантах образуется составной канал, образованный из последовательно соединенных акустического и оптического (на лазерном луче) или акустического и радиоэлектронного (радиозакладка – среда распространения – радиоприемник) каналов. Такие каналы корректно назвать акусто-оптическим и акусто-радиоэлектронным соответственно. Для повышения дальности канала утечки может также использоваться ретранслятор, совмещающий функции приемника одного канала утечки информации и передатчика следующего канала. Например, для повышения дальности подслушивания с использованием радио закладки можно разместить ретранслятор слабого сигнала закладного устройства в портфеле, сдаваемый якобы на хранение в камеру хранения закрытого предприятия, а принимать и регистрировать более мощный сигнал ретранслятора на удалении в несколько километров в безопасном месте. Такой составной канал называется акусто-радиоэлектронный. По частоте проявления каналы делятся на постоянные и эпизодические. В постоянном канале утечка информации носит достаточно регулярный характер. Например, наличие в кабинете источника опасного сигнала может привести к передаче из кабинета речевой информации до момента обнаружения этого источника. Регулярность получения информации через такой канал делает его весьма ценным, поэтому разведка дорожит регулярным источником информации и защищает его от контрразведки. К эпизодическим каналам относятся каналы, утечка информации в которых имеет кратковременный, часто случайный характер.

По способу создания каналы утечки могут быть специально организованные и случайные. Организованные каналы создаются злоумышленником для регулярного добывания информации. Например, для подслушивания на большом расстоянии от источника речевой информации организуется канал утечки из помещения путем размещения в нем закладного устройства. Характеристики (частота излучения, вид модуляции, мощность передатчика и др.) этого канала известны злоумышленнику. Эти знания позволяют ему непрерывно или в определенное время прослушивать все разговоры, ведущиеся в помещении.

Побочные электромагнитные излучения и наводки создают предпосылки для образования случайных каналов утечки информации, параметры которых априори злоумышленнику не известны. Если ему удастся настроить свой приемник на частоту побочного излучения, то возникает случайный канал утечки информации. Такой канал может быть весьма информативным, но случайный характер его образования и времени работы (когда включено излучающее техническое средство) снижает его полезность для злоумышленника.

По техническому каналу утечки информация может передаваться не только в открытом виде, она может быть и закрытой. С целью повышения скрытности сигнал на выходе перспективных закладных устройств закрывается, а канал утечки, использующий эти устройства, является технически закрытым. При перехвате функциональных каналов связи, по которым передается шифрованная информация, образуется шифрованный канал утечки информации.

Возможности передачи информации по техническим каналам зависит от многих факторов: энергии сигнала, степени его ослабления в среде распространения, чувствительности и разрешающей способности приемника злоумышленника, уровня помех в канале и др.

6.2. Противодействие технической разведке

Для противодействия технической разведке используют следующие меры. Пространственное зашумление:

– пространственное электромагнитное зашумление с использованием генераторов шума или создание прицельных помех (при обнаружении и определении частоты излучения закладного устройства или побочных электромагнитных излучений ТСПИ) с использованием средств создания прицельных помех;

– создание акустических и вибрационных помех с использованием генераторов акустического шума;

– подавление диктофонов в режиме записи с использованием подавителей диктофонов;

– линейное зашумление;

– линейное зашумление линий электропитания;

– линейное зашумление посторонних проводников и соединительных линий, имеющих выход за пределы контролируемой зоны;

– уничтожение закладных устройств;

– уничтожение закладных устройств, подключенных к линии, с использованием специальных генераторов импульсов (выжигателей «жучков»).

Выявление портативных электронных устройств перехвата информации (закладных устройств) осуществляется проведением специальных обследований, а также специальных проверок объектов и выделенных помещений.

Специальные обследования объектов ТСПИ и выделенных помещений проводятся путем их визуального осмотра без применения технических средств.

6.3. Защита от утечек информации по соединительным кабелям

Компьютеры соединяются в сеть при помощи кабелей, проложенных зачастую на большие расстояния. В этом случае не исключается возможность подсоединения к ним злоумышленников для доступа к секретной информации, поэтому предпочтительна прокладка кабелей на контролируемой территории.

Прохождение электрических сигналов по цепям ПК и соединительным кабелям сопровождается возникновением побочных электромагнитных излучений (ПЭМИ) в окружающей среде. Распространение побочных электромагнитных излучений за пределы контролируемой территории на десятки, сотни, а иногда и тысячи метров, создает предпосылки для утечки информации, так как возможен ее перехват с помощью специальных технических средств контроля.

При контроле защиты информации ПК используются специально разработанные тестовые программы, а также специальная аппаратура контроля уровня излучения, которые определяют режим работы ПК, обеспечивающий совместно с другими техническими средствами скрытый режим работы для различных средств разведки.

7. ПРОГРАММНЫЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Программная защита информации сводится к созданию компьютерных программ, которые ограничивают доступ к информации, следят за её сохранностью и конфиденциальностью.

Все программное обеспечение, установленное на компьютерном оборудовании предприятия, является собственностью и должно использоваться исключительно в производственных целях, поэтому сотрудникам запрещается устанавливать на предоставленном в пользование компьютерном оборудовании нестандартное, нелицензионное программное обеспечение или программное обеспечение, не имеющее отношения к их производственной деятельности. Если в ходе выполнения технического обслуживания будет обнаружено не разрешенное к установке программное обеспечение, то оно должно быть удалено, а сообщение о нарушении направлено руководителю сотрудника и в отдел защиты информации.

Все компьютеры, подключенные к корпоративной сети, должны быть оснащены системой антивирусной защиты, утвержденной руководителем.

Сотрудники не должны:

- блокировать антивирусное программное обеспечение;
- устанавливать другое антивирусное программное обеспечение;
- изменять настройки и конфигурацию антивирусного программного обеспечения.

7.1. Защита информации разработчика и пользователя

По принадлежности информацию разделяют на информацию разработчика и информацию пользователя, поскольку принципы и цели защиты у них диаметрально противоположны.

Информация разработчика в основном защищается от несанкционированного копирования в целях сохранения авторских прав и коммерческой ценности. Разработчик программного обеспечения не боится, если вирус повредит разработанную им выходную программу, поскольку ее исходный вариант на языке программирования у него всегда хранится отдельно. В случае ее повреждения программист снова создаст новую, скомпилировав из исходных файлов.

Информация пользователя защищается не только от несанкционированного копирования, но и от атак хакеров, вирусов. Пользователь боится вирусных атак, поскольку программа им приобретена у разработчика, и в случае ее повреждения возобновить ее он уже не сможет. Ему придется снова покупать ее у разработчика.

Для защиты программного обеспечения от копирования разработчики применяют различные варианты схем защиты.

Защиту от несанкционированного копирования можно осуществить следующими способами:

- применением диска с дефектом,
- использованием ключевого диска,
- установкой серийного номера,
- применением счётчика числа копий,
- защитой от дезассамблирования,
- использованием технических отличий компьютеров,
- введением пароля.

При применении диска с дефектом защищенные программы поставляются на дисках, которые записаны каким-либо нестандартным образом или имеют физическое повреждение (например, прожженную лазером дырку). Такие диски нельзя скопировать – их копии не будут полностью соответствовать оригиналам. При своей работе защищенные программы проверяют, находятся ли они на «правильном» диске, т.е. имеет ли этот диск особенности, которые были предусмотрены поставщиком программы.

При применении ключевого диска защищенные программы копируются на жесткий диск. Программу можно неограниченное число раз копировать на жесткий диск, но при запуске копии программы с жесткого диска необходимо, чтобы в дисковод был вставлен оригинальный диск с программой («ключевой» диск). При запуске программа предварительно опрашивает этот диск, и только убедившись, что диск с лицензионной записью, начинает работу.

При защите с помощью серийного номера используется наличие уникального номера в каждом экземпляре программы. При размножении в нее заносится номер, который затем проставляется на экземпляре программы. При обнаружении копии программы у незарегистрированного пользователя можно найти источник похищения. По идеологии защита с использованием серийного номера близка к защите с помощью пароля.

При защите счетчиком установленных копий программы продают с заранее обговоренным числом копий, которые можно получить с дистрибутивной (поставочной) дискеты. Как правило, для такого продукта существует программа установки (инсталляции), которая при очередном копировании уменьшает счетчик числа копий. Если же основную программу скопировать без программы установки, то такая копия в лучшем случае не будет работать. Нельзя также скопировать и всю дискету с установочной программой, так как программа установки проверяет оригинальность дискеты, на которой она записана. В основном такую защиту применяют на игровых программах. Этот вид защиты может сочетаться с защитой серийным номером.

Программная защита от дезассемблирования делается следующим образом. Практически любую защиту можно снять или обойти, поэтому необходимо принять меры, чтобы для "взлома" программы требовались такие же затраты, как и на создание программы, подобной защищаемой, или же покупка программы была бы дешевле. Программу компилируют так, что обратное дезассамблирование не дает реальных результатов и в дальнейшем для получения исходника требуется достаточно большое время.

При использовании технических отличий в машине для программной защиты учитываются индивидуальные особенности в технических данных каждой машины. Как правило, каждая модель ПЭВМ имеет свои индивидуальные особенности. Это можно использовать для проверки уникальности компьютера, на котором установлена программа. Например, тактовая частота работы ПК имеет различия, доходящие до +0,001 и даже +0,01 МГц. Если точно измерить частоту, то можно проверить уникальность ПЭВМ. Или ППЗУ (ROM) одинаково только для машин одного класса одной и той же фирмы. Поэтому подсчет контрольной суммы ПЗУ может ограничить использование программы одной модификацией машины.

Информация пользователя защищается следующими способами:

1) антивирусными программами (от атак хакеров и вирусных атак);
2) программами управления доступом к информации;
3) средствами архивации данных (защитой от потерь);
4) криптографическими средствами (шифровкой информации);
5) средствами идентификации и аутентификации пользователей;
6) протоколированием и аудитом;
7) программой защиты сетей.

Возможны также их комбинации. В целом на сегодня наиболее существенной задачей защиты информации является защита от компьютерных вирусов.

7.2. Программная защита управления доступом к информации

Программы управления доступом к информации разделяются на общие и специальные.

К общим относятся программы, входящие в состав операционной системы, которые позволяют создавать свою рабочую область в долговременной памяти компьютера (рабочий стол), вход в которую защищен специальным паролем, выбранным пользователем. К таким относятся общеизвестные Windows 2000, NT, XP и другие, подобные им.

К специальным относятся программы, которые создаются применительно к конкретным условиям пользователя или сети.

На сегодня наиболее распространена программная защита паролями. Система парольного доступа сейчас используется повсеместно. Главное достоинство парольной аутентификации – простота и привычность. Пароли давно встроены в операционные системы и иные сервисы. При правильном использовании пароли могут обеспечить приемлемый для многих организаций уровень безопасности. В большинстве систем пользователи могут задавать собственные пароли произвольно, но при этом следует помнить о недопустимости использования фамилий, имен, инициалов своих близких. Пароли, сконструированные на основе номеров телефонов, дат рождений, адресов и т.п., легко расшифровать. Хакеры обычно имеют словари наиболее распространенных паролей. Кроме того, пароль не должен быть очень коротким, так как существуют алгоритмы их быстрой расшифровки. Рекомендуется выбирать пароль не менее чем из семи символов.

Существуют специальные программы (утилиты), позволяющие реализовать механизм так называемого устаревания паролей. Такие системы принуждают пользователя периодически менять пароли. Для многочисленных непривилегированных пользователей этот механизм вряд ли стоит рекомендовать, так как их будет раздражать необходимость часто запоми-

нать новые пароли, и они будут их лишь чередовать (а это еще более опасно, чем иметь один пароль – непривычный набор на клавиатуре легче подсмотреть). Но пароли администратора должны периодически меняться (лучше без использования утилит, а по специальному плану).

Теоретически наиболее безопасный пароль состоит из случайной последовательности букв, знаков препинания и цифр. Но такой пароль трудно запомнить, и администратор его вводит очень медленно, особенно вначале. Медленный ввод пароля при считывании его с бумажки, не обеспечивает оптимального уровня безопасности системы.

Считается, что наиболее надежен пароль, набранный на разных регистрах и содержащий как строчные, так и прописные буквы, а также знаки препинания и спецсимволы.

Замена пароля должна проводиться по плану, который также не афишируется. Иногда применяется разовый пароль.

Тем не менее по совокупности характеристик парольная защита не столь надежна. Надежность паролей основывается на способности помнить их и хранить в тайне. Ввод пароля можно подсмотреть путем подглядывания за легальным пользователем, когда тот вводит пароль, дающий ему право на работу с ОС (даже если во время ввода пароль не высвечивается на экране дисплея, хакер может легко узнать пароль, просто следя за перемещением пальцев пользователя по клавиатуре). Возможно получение пароля из файла, в котором этот пароль был сохранен "ленивым" пользователем, не желающим затруднять себя вводом пароля для идентификации себя при сетевом подключении (как правило, такой пароль хранится в файле в незашифрованном виде). Некоторые пользователи, чтобы не забыть, часто записывают его на календарях, в записных книжках или на оборотной стороне компьютерных клавиатур (особенно часто подобная ситуация встречается, если администраторы заставляют пользователей применять длинные, трудно запоминаемые пароли), что облегчает поиск пароля. Возможна также кража внешнего носителя парольной информации (дискеты или электронного ключа, на которых хранится пароль пользователя для входа в ОС).

Пароль можно угадать методом грубой силы, используя, быть может, словарь. Если файл паролей зашифрован, но доступен для чтения, его можно перекачать к себе на компьютер и попытаться подобрать пароль, запрограммировав полный перебор. Пароли уязвимы по отношению к электронному перехвату – это наиболее принципиальный недостаток, который нельзя компенсировать улучшением администрирования или обучением пользователей. Практически единственный выход – использование криптографии для шифрования паролей перед передачей по линиям связи.

Основная проблема парольной защиты – противоречие между его надежностью, частой заменой и запоминанием. Чем длиннее пароль,

включающий идентификацию регистров, цифры и разные алфавиты, тем труднее он запоминается в памяти человека. Это вынуждает пользователей записывать его, что уже становится поводом для его кражи.

Тем не менее следующие меры позволяют значительно повысить надежность парольной защиты:

- наложение технических ограничений (пароль должен быть не слишком коротким, он должен содержать буквы, цифры, знаки пунктуации и т.п.);
- управление сроком действия паролей, их периодическая смена;
- ограничение доступа к файлу паролей;
- ограничение числа неудачных попыток входа в систему, что затруднит применение метода грубой силы;
- обучение и воспитание пользователей;
- использование программных генераторов паролей, которые, основываясь на несложных правилах, могут порождать только благозвучные и, следовательно, запоминающиеся пароли.

Перечисленные меры целесообразно применять всегда, даже если наряду с паролями используются другие методы аутентификации, основанные, например, на применении токенов.

Токен – это предмет или устройство, владение которым подтверждает подлинность пользователя. Различают токены с памятью (пассивные, которые только хранят, но не обрабатывают информацию) и интеллектуальные токены (активные).

Самой распространенной разновидностью токенов с памятью являются карточки с магнитной полосой. Для использования подобных токенов необходимо устройство чтения, снабженное также клавиатурой и процессором. Обычно пользователь набирает на этой клавиатуре свой личный идентификационный номер, после чего процессор проверяет его совпадение с тем, что записано на карточке, а также подлинность самой карточки. Таким образом, здесь фактически применяется комбинация двух способов защиты, что существенно затрудняет действия злоумышленника.

Необходима обработка аутентификационной информации самим устройством чтения, без передачи в компьютер – это исключает возможность электронного перехвата.

Иногда (обычно для физического контроля доступа) карточки применяют сами по себе, без запроса личного идентификационного номера.

Как известно, одним из самых мощных средств в руках злоумышленника является изменение программы аутентификации, при котором пароли не только проверяются, но и запоминаются для последующего несанкционированного использования.

Интеллектуальные токены характеризуются наличием собственной вычислительной мощности. Они подразделяются на интеллектуальные

карты, стандартизованные ISO и прочие токены. Карты нуждаются в интерфейсном устройстве, прочие токены обычно обладают ручным интерфейсом (дисплеем и клавиатурой) и по внешнему виду напоминают калькуляторы. Чтобы токен начал работать, пользователь должен ввести свой личный идентификационный номер.

По принципу действия интеллектуальные токены можно разделить на следующие категории:

• *статический обмен паролями*: пользователь обычным образом доказывает токену свою подлинность, затем токен проверяется компьютерной системой;

• *динамическая генерация паролей*: токен генерирует пароли, периодически изменяя их. Компьютерная система должна иметь синхронизированный генератор паролей. Информация от токена поступает по электронному интерфейсу или набирается пользователем на клавиатуре терминала;

• *запросно-ответные системы*: компьютер выдает случайное число, которое преобразуется криптографическим механизмом, встроенным в токен, после чего результат возвращается в компьютер для проверки. Здесь также возможно использование электронного или ручного интерфейса. В последнем случае пользователь читает запрос с экрана терминала, набирает его на клавиатуре токена (возможно, в это время вводится и личный номер), а на дисплее токена видит ответ и переносит его на клавиатуру терминала.

Главным достоинством интеллектуальных токенов является возможность их применения при аутентификации по открытой сети. Генерируемые или выдаваемые в ответ пароли постоянно меняются, и злоумышленник не получит заметных дивидендов, даже если перехватит текущий пароль. С практической точки зрения, интеллектуальные токены реализуют механизм одноразовых паролей.

Еще одним достоинством является потенциальная многофункциональность интеллектуальных токенов. Их можно применять не только для целей безопасности, но и, например, для финансовых операций.

В последнее время все больше применяются программы, идентифицирующие биометрические параметры самого пользователя - рисунок папиллярных линий пальцев, цвет радужной оболочки глаз, голос.

Набирает также популярность аутентификация путем выяснения координат пользователя. Идея состоит в том, чтобы пользователь посылал координаты спутников системы GPS (Global Positioning System), находящихся в зоне прямой видимости. Сервер аутентификации знает орбиты всех спутников, поэтому может с точностью до метра определить положение пользователя. Поскольку орбиты спутников подвержены колебаниям, предсказать которые крайне сложно, подделка координат оказывается практически невозможной. Ничего не даст и перехват координат - они постоянно меняются. Непрерывная передача координат не требует от пользо-

вателя каких-либо дополнительных усилий, поэтому он может без труда многократно подтверждать свою подлинность. Аппаратура GPS сравнительно недорога и апробирована, поэтому в тех случаях, когда легальный пользователь должен находиться в определенном месте, данный метод проверки подлинности представляется весьма привлекательным.

7.3. Специальные программы защиты информации

Для защиты компьютера от несанкционированного доступа используются различные программные средства защиты. Выбор в пользу тех или иных средств защиты информации от несанкционированного доступа (СЗИ от НСД) при проектировании системы защиты информационных систем – ключевая процедура, определяющая будущий уровень защищенности информационной системы и легитимность дальнейшей ее эксплуатации с точки зрения российского законодательства.

Требование законодательства Российской Федерации, обязывающее обязательное использование сертифицированных программных продуктов в качестве средств защиты информации, особенно при обработке конфиденциальной информации и персональных данных, определяется целым рядом положений законодательных и нормативных актов в области защиты информации. В частности:

- Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К) – основной нормативный документ, регламентирующий вопросы, связанные с технической защитой конфиденциальной информации в России;
- Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных (утв. постановлением Правительства РФ от 17 ноября 2007 г. № 781);
- Закон РФ № 5485-I «О государственной тайне» от 21 июля 1993 г.

В большинстве случаев выбор средств защиты информации (СЗИ) должен осуществляться в рамках имеющейся номенклатуры сертифицированных решений. В настоящее время сертифицированы сотни программных и программно-аппаратных средств защиты информации от несанкционированного доступа. Ознакомиться с ними можно на официальном сайте Федеральной службы по техническому и экспортному контролю (ФСТЭК России) в разделе Государственный реестр сертифицированных средств защиты информации.

При всем разнообразии сертифицированных средств защиты сложно сделать правильный выбор. Необходимо учитывать множество факторов, в частности: стойкость и функциональность средств защиты информации, соответствие требованиям Руководящих документов по защите ресурсов автоматизированных систем, совместимость с операционными системами

и прикладным ПО, подготовку персонала и многое другое. Кроме того, ни одно средство защиты информации не позволяет обеспечить выполнение всех технических требований к защите автоматизированных систем, поэтому необходимо учитывать и корректность совместного функционирования выбранных СЗИ.

За последнее время, по тем или иным причинам, на рынке сертифицированных средств защиты информации, появились кампании, продукты которых отличаются особым, повышенным спросом. Наиболее популярные средства защиты информации:

- Аккорд (ОКБ САПР);
- Secret Net в комплекте с аппаратной платой Соболь PCI (код безопасности);
- Dallas Lock (НПП ИТБ);
- Страж NT,

и другие. На сегодня рынок таких программ достаточно широк, и поэтому выбор программы конкретного типа определяется архитектурой данной автоматизированной системы.

СЗИ «Аккорд» является надежным программно-аппаратным средством, основными недостатками которого являются отсутствие возможности преобразования диска и автоматической зачистки удаляемых файлов.

Secret Net является сертифицированным средством защиты информации от несанкционированного доступа и позволяет привести автоматизированные системы в соответствие с требованиями регулирующих документов.

Ключевые возможности его от НСД следующие:

– аутентификация пользователей;

– разграничение доступа пользователей к информации и ресурсам автоматизированной системы;

– доверенная информационная среда;

– контроль утечек и каналов распространения конфиденциальной информации;

– контроль устройств компьютера и отчуждаемых носителей информации на основе централизованных политик, исключающих утечки конфиденциальной информации;

– централизованное управление системой защиты, оперативный мониторинг, аудит безопасности;

– масштабируемая система защиты, возможность применения Secret Net (сетевой вариант) в организации с большим количеством филиалов.

Dallas Lock – сертифицированное программное решение, которое предоставляет надежную защиту от обхода загрузки. Из рассмотренных продуктов только Dallas Lock позволяет обеспечить сертифицированную защиту мобильных пользователей.

Страж NT. Программа предназначена для защиты информации от несанкционированного доступа при работе в многопользовательских автоматизированных системах (АС) и информационных системах персональных данных (ИСПДн).

Имеет следующие подсистемы.

1) подсистема контроля устройств – возможность контроля устройств, подключенных к компьютеру путём задания дескрипторов безопасности для групп однотипных устройств;

2) подсистема преобразования информации на отчуждаемых носителях – дополнительный механизм защиты съемных носителей (дискет и флеш-накопителей) путем прозрачного преобразования всей информации, записываемой на носитель. Преобразование информации осуществляется с применением функции гаммирования с обратной связью алгоритма криптографического преобразования ГОСТ 28147-89;

3) подсистема создания и применения шаблонов настроек – новый механизм, предназначенный для облегчения настройки СЗИ. Механизм позволяет создавать списки настроек и свободно тиражировать их на другие компьютеры;

4) подсистема учёта носителей информации – полностью переработана подсистема работы с носителями информации. В новой версии существует возможность регистрировать как отчуждаемые носители, так и отдельные тома жестких дисков;

5) подсистема регистрации – все события СЗИ доступны для просмотра из одной программы. Усовершенствованы функции сортировки и поиска отдельных событий СЗИ;

6) подсистема маркировки и учёта документов, выдаваемых на печать – новая программа настройки маркировки документов позволяет более гибко задавать состав и порядок служебной информации, выводимой на печать;

7) подсистема управления пользователями – добавлены новые функции работы с идентификаторами и возможность редактировать пользователей на удалённых рабочих станциях;

8) подсистема настройки системы защиты – настройка системы защиты реализована в виде единого центра настройки.

8. ТИПОВЫЕ ХАКЕРСКИЕ АТАКИ И ПРОТИВОДЕЙСТВИЕ

Хакерская атака – это попытка использовать несовершенство системы безопасности жертвы для получения информации или для нанесения вреда системе. Причиной любой удачной хакерской атаки является недостаточная компетенция администратора системы безопасности в частности, несовершенство программного обеспечения и слабое внимание к вопросам безопасности организации или пользователя в целом.

Кто такие хакеры? Хотя в последнее время термин "хакер" можно довольно часто встретить на страницах компьютерной прессы, однако до сих пор не сложилось единого мнения о том, кого именно следует именовать хакером. Чаще всего так называют любого высококлассного специалиста в области компьютерной техники и всего, что с ней связано. Однако имеются серьезные разногласия относительно того, как эти компьютерные энтузиасты применяют свои уникальные познания на практике – легально или в преступных целях.

В целом хакером предпочтительно именовать лицо, стремящееся обойти защиту компьютерной системы вне зависимости от того, преследуются по закону его действия или нет.

Статистика компьютерных преступлений свидетельствует о том, что уровень профессиональной подготовки хакера отличается удивительным разнообразием. Им может стать обычный школьник, случайно обнаруживший программу взлома на одном из специализированных хакерских серверов в Internet. В то же время отмечено и появление настоящих хакерских банд, главарями которых являются компьютерные специалисты высочайшей квалификации.

Естественно, наибольшую угрозу безопасности компьютерных систем представляют высококвалифицированные специалисты-компьютерщики. Для такого хакера характерны следующие черты и особенности поведения:

- он всегда в курсе последних новинок компьютерной техники, устройств связи и программных средств;
- перед тем, как атаковать компьютерную систему, взломщик всеми способами пытается собрать максимум информации о ней, включая данные об используемом программном обеспечении и личных качествах ее администраторов;
- добывая нужную информацию, он не брезгует агентурными и оперативно-техническими методами (например, устанавливая подслушивающие устройства в местах, часто посещаемых обслуживающим персоналом компьютерных систем, которые намеревается взломать);
- перед попыткой взлома компьютерной системы он апробирует методы, которые планируется применить для атаки, на заранее подготовленной модели с теми же средствами обеспечения безопасности, что и в атакуемой системе;
- сама атака компьютерной системы осуществляется по возможности быстро, чтобы ее администраторы не смогли зафиксировать факт совершения атаки и не успели предпринять меры по ее отражению, а также по выявлению личности атакующего и его местонахождения;

- хакер не пользуется изощренными методами взлома защиты компьютерной системы, памятуя о том, что чем сложнее алгоритм атаки, тем вероятнее возникновение ошибок и сбоев при его реализации;
- чтобы минимизировать время, необходимое для взлома, и количество возможных ошибок, хакер обычно атакует компьютерную систему при помощи заранее написанных программ;
- хакер никогда не действует под собственным именем и тщательно скрывает свой сетевой адрес; у него имеется тщательно продуманный план, позволяющий замести следы или оставить ложный след (например, одновременно он может специально вести заведомо обреченную на провал атаку из другого места, благодаря которой журнал аудита атакуемой компьютерной системы окажется забитым зарегистрированными событиями);
- хакеры широко применяют программные закладки, которые самоуничтожаются либо при их обнаружении, либо по истечении некоторого фиксированного периода времени.

Различают следующие виды хакерских атак:

1) шпионские, предназначенные для несанкционированного съёма (воровства) информации;
2) вредоносные, предназначенные для нанесения вреда автоматизированной системе.

8.1. Типичные шпионские атаки для воровства информации

Программой-шпионом (альтернативные названия – Spy, Spy-Ware, Spy Trojan) принято называть программы, которые могут самостоятельно устанавливаться или запускаться на компьютере без уведомления пользователя, не получая его согласия и не предоставляя ему возможности управления, и передающее кому-либо информацию о пользователе без его согласия. Например, шпионские программы могут отслеживать поведение пользователя в сети или собирать сведения о пользователе, включая сведения, идентифицирующие пользователя лично, и другую важную информацию. Чаще всего они не проявляют себя после установки на компьютер.

Различают следующие виды подобных атак.

1) клавиатурные шпионы (кейлоггеры);
2) снифферы;
3) программы взлома паролей;
4) фишинг;
5) сетевая разведка;
6) сборка "мусора";
7) кража пароля.

8.1.1. Клавиатурные шпионы (кейлоггеры)

Кейлоггер – одна из наиболее распространенных разновидностей программных закладок. В переводе с английского *keylogger* – это регистратор нажатий клавиш. Все кейлоггеры можно условно разделить на программные и аппаратные.

Первые – это специально написанные программы, предназначенные для отслеживания нажатий клавиш на клавиатуре и ведения журнала нажатых клавиш.

Вторые представляют собой небольшие устройства, которые могут быть закреплены на клавиатуре, проводе или в системном блоке компьютера. Сюда же относятся системы видеонаблюдения за клавиатурой.

Программные кейлоггеры (*keyloggers*, *keyloggers*, *keystrokeloggers*, *keyrecorders*, *keytrappers*, *keycaptureprograms* и множество других вариантов названия). Первоначально предназначались исключительно для записи информации о нажатиях клавиш клавиатуры, в том числе и системных, в специализированный журнал регистрации (Log-файл), который впоследствии изучался человеком, уставившим эту программу. Log-файл может отправляться по сети на сетевой диск, ftp сервер в сети Интернет, по Email и др. В последнее время программные продукты, имеющие данное название, выполняют много дополнительных функций – это перехват информации из окон, перехват кликов мыши, "фотографирование" снимков экрана и активных окон, ведение учета всех полученных и отправленных Email, мониторинг файловой активности, мониторинг системного реестра, мониторинг очереди заданий, отправленных на принтер, перехват звука с микрофона и видеоизображения с веб-камеры, подключенных к компьютеру и др. Кейлоггеры могут быть встроены в коммерческие, бесплатные и условно-бесплатные программы, троянские программы, вирусы и черви. В качестве примера можно привести недавнюю нашумевшую эпидемию червя Mydoom, который содержал в себе кейлоггер. Эта эпидемия вызвала целую волну публикаций, показывающих особую актуальность проблемы защиты от программ-шпионов.

Большинство существующих на данный момент кейлоггеров считаются «легальными» и свободно продаются, так как разработчики декларируют множество причин для использования кейлоггеров. Например:

- для родителей: отслеживание действий детей в Интернете и оповещение родителей в случае попыток зайти на сайты «для взрослых» (parentalcontrol);
- для ревнивых супругов: отслеживание действий своей половины в сети в случае подозрения на «виртуальную измену»;
- для службы безопасности организации: отслеживание фактов нецелевого использования персональных компьютеров, их использования

в нерабочее время, отслеживание фактов набора на клавиатуре критичных слов и словосочетаний, которые составляют коммерческую тайну организации, и разглашение которых может привести к материальному или иному ущербу для организации;

- для различных служб безопасности: проведение анализа и расследования инцидентов, связанных с использованием персональных компьютеров.

Однако любой легальный кейлоггер может использоваться во вредоносных целях, и в последнее время именно кража информации пользователей различных систем онлайновых платежей стала, к сожалению, главным применением кейлоггеров (для этих же целей вирусописателями постоянно разрабатываются новые троянцы-кейлоггеры). Кроме того, многие кейлоггеры прячут себя в системе (т.к. имеют функции руткита), что значительно облегчает их использование в преступных целях.

Принципиальная идея кейлоггера состоит в том, чтобы внедриться между любыми двумя звеньями в цепи прохождения сигнала от нажатия пользователем клавиш на клавиатуре до появления символов на экране.

Наиболее популярные технические подходы к построению программных кейлоггеров следующие:

- системная ловушка на сообщения о нажатии клавиш клавиатуры (устанавливается с помощью функции Win APISe tWindows Hook, для того чтобы перехватить сообщения, посылаемые оконной процедуре, – чаще всего пишется на C);
- циклический опрос клавиатуры (с помощью функции Win APIGet (Async) Key State, Get Keyboard State – чаще всего пишется на Visual Basic, реже на Borland Delphi);
- драйвер-фильтр стека клавиатурных драйверов ОС Windows (требует специальных знаний, пишется на C).

Все клавиатурные шпионы делятся на три типа – **имитаторы, фильтры и заместители.**

Имитаторы – клавиатурные шпионы этого типа работают по следующему алгоритму. Злоумышленник внедряет в операционную систему программный модуль, который имитирует приглашение пользователю зарегистрироваться для того, чтобы войти в систему. Затем внедренный модуль (в принятой терминологии – имитатор) переходит в режим ожидания ввода пользовательского идентификатора и пароля. После того как пользователь идентифицирует себя и введет свой пароль, имитатор сохраняет эти данные там, где они доступны злоумышленнику. Далее имитатор инициирует выход из системы (что в большинстве случаев можно сделать программным путем), и в результате перед глазами у ничего не подозревающего пользователя появляется ещё одно, но на этот раз уже настоящее приглашение для входа в систему.

Обманутый пользователь, видя, что ему предлагается еще раз внести пароль, приходит к выводу о том, что он допустил какую-то ошибку во время предыдущего ввода пароля, и послушно повторяет всю процедуру входа в систему заново. Некоторые имитаторы для убедительности выдают на экран монитора правдоподобное сообщение о якобы совершенной пользователем ошибке. Например, такое: "НЕВЕРНЫЙ ПАРОЛЬ. ПОПРОБУЙТЕ ЕЩЕ РАЗ".

Написание имитатора не требует от его создателя каких-либо особых навыков. Единственная трудность, с которой он может столкнуться, состоит в том, чтобы отыскать в документации соответствующую программную функцию, реализующую выход пользователя из системы.

Перехват пароля зачастую облегчают сами разработчики операционных систем, которые не затрудняют себя созданием усложненных по форме приглашений пользователю зарегистрироваться для входа в систему. Подобное пренебрежительное отношение характерно для большинства версий операционной системы UNIX, в которых регистрационное приглашение состоит из двух текстовых строк, выдаваемых поочередно на экран терминала: **login:** **password:**

Подделать такое приглашение не трудно. Однако само по себе усложнение внешнего вида приглашения не создает для хакера, задумавшего внедрить в операционную систему имитатор, каких-либо непреодолимых препятствий. Для этого требуется прибегнуть к более сложным и изощренным мерам защиты. В качестве примера операционной системы, в которой такие меры в достаточно полном объеме реализованы на практике, можно привести Windows NT.

Системный процесс WinLogon, отвечающий в операционной системе Windows NT за аутентификацию пользователей, имеет свой собственный рабочий стол – совокупность окон, одновременно видимых на экране дисплея. Этот рабочий стол называется *столом аутентификации.* Никакой другой процесс, в том числе и имитатор, не имеет доступа к рабочему столу аутентификации и не может расположить на нем свое окно.

После запуска Windows NT на экране компьютера возникает так называемое начальное окно рабочего стола аутентификации, содержащее указание нажать на клавиатуре клавиши <Ctrl>+<Alt>+<Del>. Сообщение о нажатии этих клавиш передается только системному процессу WinLogon, а для остальных процессов, в частности, для всех прикладных программ, их нажатие происходит совершенно незаметно. Далее производится переключение на другое, так называемое *регистрационное* окно рабочего стола аутентификации. В нем-то как раз и размещается приглашение пользователю ввести свое идентификационное имя и пароль, которые будут восприняты и проверены процессом WinLogon.

Для перехвата пользовательского пароля внедренный в Windows NT имитатор обязательно должен уметь обрабатывать нажатие пользователем клавиш <Ctrl>+<Alt>+<Del>. В противном случае произойдет переключение на регистрационное окно рабочего стола аутентификации, имитатор станет неактивным и не сможет ничего перехватить, поскольку все символы пароля, введенные пользователем, минуют имитатор и станут достоянием исключительно системного процесса WinLogon. Как уже говорилось, процедура регистрации в Windows NT устроена таким образом, что нажатие клавиш <Ctrl>+<Alt>+<Del> проходит бесследно для всех процессов, кроме WinLogon, и поэтому пользовательский пароль поступит именно ему.

Конечно, имитатор может попытаться воспроизвести не начальное окно рабочего стола аутентификации (в котором высвечивается указание пользователю одновременно нажать клавиши <Ctrl>+<Alt>+<Del>), а регистрационное (где содержится приглашение ввести идентификационное имя и пароль пользователя).

Однако при отсутствии имитаторов в системе регистрационное окно автоматически заменяется на начальное по прошествии короткого промежутка времени (в зависимости от версии Windows NT он может продолжаться от 30 с до 1 мин), если в течение этого промежутка пользователь не предпринимает никаких попыток зарегистрироваться в системе. Таким образом, сам факт слишком долгого присутствия на экране регистрационного окна должен насторожить пользователя Windows NT и заставить его тщательно проверить свою компьютерную систему на предмет наличия в ней программных закладок.

Фильтры – "охотятся" за всеми данными, которые пользователь операционной системы вводит с клавиатуры компьютера. Самые элементарные фильтры просто сбрасывают перехваченный клавиатурный ввод на жесткий диск или в какое-то другое место, к которому имеет доступ злоумышленник. Более изощренные программные закладки этого типа подвергают перехваченные данные анализу и отфильтровывают информацию, имеющую отношение к пользовательским паролям.

Фильтры являются резидентными программами, перехватывающими одно или несколько прерываний, которые связаны с обработкой сигналов от клавиатуры. Эти прерывания возвращают информацию о нажатой клавише и введенном символе, которая анализируется фильтрами на предмет выявления данных, имеющих отношение к паролю пользователя.

В общем случае можно утверждать, что если в операционной системе разрешается переключать клавиатурную раскладку во время ввода пароля, то для этой операционной системы возможно создание фильтра. Поэтому, чтобы обезопасить ее от фильтров, необходимо обеспечить выполнение следующих трех условий:

1) во время ввода пароля переключение раскладок клавиатуры не разрешается;

2) конфигурировать цепочку программных модулей, участвующих в работе с паролем пользователя, может только системный администратор;

3) доступ к файлам этих модулей имеет исключительно системный администратор.

Соблюсти первое из этих условий в локализованных для России версиях операционных систем принципиально невозможно. Дело в том, что средства создания учетных пользовательских записей на русском языке являются неотъемлемой частью таких систем. Только в англоязычных версиях систем Windows NT и UNIX предусмотрены возможности, позволяющие поддерживать уровень безопасности, при котором соблюдаются все три перечисленных условия.

Заместители – полностью или частично подменяют собой программные модули операционной системы, отвечающие за аутентификацию пользователей. Подобного рода клавиатурные шпионы могут быть созданы для работы в среде практически любой многопользовательской операционной системы. Трудоемкость написания заместителя определяется сложностью алгоритмов, реализуемых подсистемой аутентификации, и интерфейсов между ее отдельными модулями. Также при оценке трудоемкости следует принимать во внимание степень документированности этой подсистемы. В целом можно сказать, что задача создания заместителя значительно сложнее задачи написания имитатора или фильтра, поэтому фактов использования подобного рода программных закладок злоумышленниками пока отмечено не было. Однако в связи с тем, что в настоящее время все большее распространение получает операционная система Windows NT, имеющая мощные средства защиты от имитаторов и фильтров, в самом скором будущем от хакеров следует ожидать более активного использования заместителей в целях получения несанкционированного доступа к компьютерным системам.

Поскольку заместители берут на себя выполнение функций подсистемы аутентификации, перед тем как приступить к перехвату пользовательских паролей они должны выполнить следующие действия:

- подобно компьютерному вирусу внедриться в один или несколько системных файлов;
- использовать интерфейсные связи между программными модулями подсистемы аутентификации для встраивания себя в цепочку обработки введенного пользователем пароля.

Для того чтобы защитить систему от внедрения заместителя, ее администраторы должны строго соблюдать адекватную политику безопасности. Подсистема аутентификации должна быть одним из самых защищенных элементов операционной системы. Это значит, что администратор

должен вести самый тщательный контроль целостности исполняемых системных файлов и интерфейсных функций, используемых подсистемой аутентификации для решения своих задач.

Но и эти меры могут оказаться недостаточно эффективными. Ведь машинный код заместителя выполняется в контексте операционной системы, и поэтому заместитель может предпринимать особые меры, чтобы максимально затруднить собственное обнаружение. Например, он может перехватывать системные вызовы, используемые администратором для выявления программных закладок, с целью подмены возвращаемой ими информации. Или фильтровать сообщения, регистрируемые подсистемой аудита, чтобы отсеивать те, которые свидетельствуют о его присутствии в компьютере.

Для лучшего понимания работы кейлоггеров следует знать принципы работы клавиатуры как физического устройства. В настоящее время большинство клавиатур выполнено в виде отдельного устройства, подключаемого к компьютеру с помощью одного из разъемов, чаще всего PS/2 или USB. Существуют два микроконтроллера, обеспечивающие процесс обработки клавиатурного ввода: один – на материнской плате ПК, второй – в самой клавиатуре. Таким образом, клавиатура персонального компьютера сама по себе является компьютерной системой. Она построена на основе микроконтроллера 8042, который постоянно сканирует нажатия клавиш на клавиатуре независимо от активности на центральном процессоре x86.

За каждой клавишей клавиатуры закреплен определенный номер, однозначно связанный с распайкой клавиатурной матрицы и не зависящий напрямую от обозначений, нанесенных на поверхность клавиш. Этот номер называется скан-кодом (название подчеркивает тот факт, что компьютер сканирует клавиатуру для поиска нажатой клавиши). Скан-код – это случайное значение, выбранное IBM еще тогда, когда она создавала первую клавиатуру для ПК. Скан-код не соответствует ASCII-коду клавиши, одной и той же клавише могут соответствовать несколько значений ASCII-кода.

На самом деле клавиатура генерирует два скан-кода для каждой клавиши – когда пользователь нажимает клавишу и когда отпускает. Наличие двух скан-кодов важно, так как некоторые клавиши имеют смысл только тогда, когда они нажаты (Shift, Control, Alt). Ниже (на рис. 10) показана упрощенная схема клавиатуры.

Когда пользователь нажимает клавишу на клавиатуре, он замыкает электрический контакт. В результате при следующем сканировании микроконтроллер фиксирует нажатие определенной клавиши и посылает в центральный компьютер скан-код нажатой клавиши и запрос на прерывание. Аналогичные действия выполняются и тогда, когда оператор отпускает нажатую ранее клавишу.

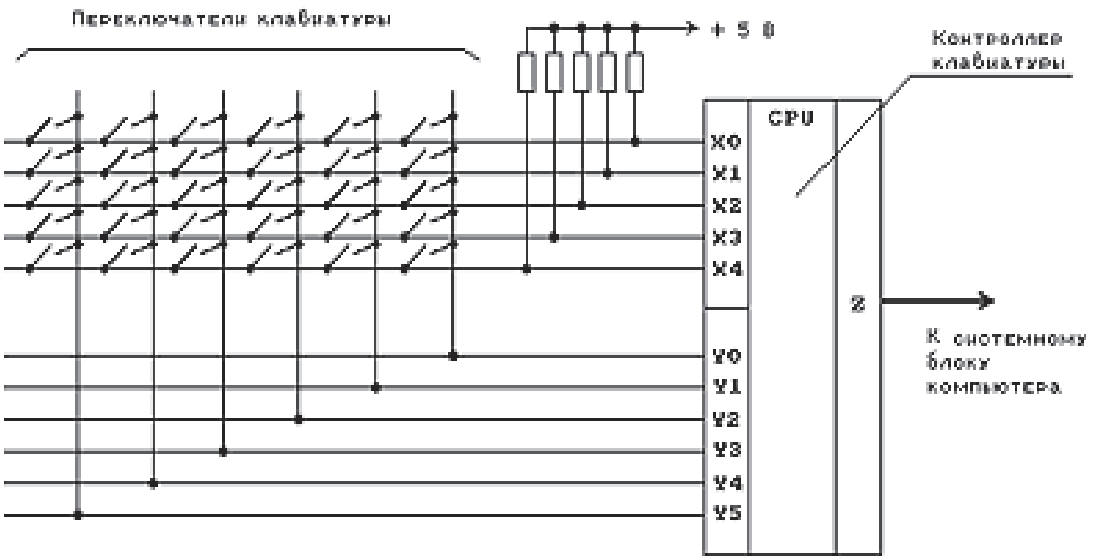


Рис. 10. Упрощенная схема клавиатуры

Второй микроконтроллер получает скан-код, производит преобразование скан-кода, делает его доступным на порту ввода-вывода 60h и затем генерирует аппаратное прерывание центрального процессора. После этого процедура обработки прерывания может получить скан-код из указанного порта ввода-вывода.

Следует отметить, что клавиатура содержит внутренний 16-байтовый буфер, через который она осуществляет обмен данными с компьютером.

Взаимодействие с системным контроллером клавиатуры происходит через порт ввода-вывода 64h. Считав байт из этого порта, можно определить статус контроллера клавиатуры, записав байт – послать контроллеру команду.

Взаимодействие с микроконтроллером в самой клавиатуре происходит с помощью портов ввода-вывода 60h и 64h. Биты 0 и 1 в байте статуса (порт 64h в режиме чтения) предоставляют возможность управлять процедурой взаимодействия: перед записью данных в эти порты бит 0 порта 64h должен быть выставлен в 0. Когда данные доступны для чтения из порта 60h, бит 1 порта 64h равен 1. Биты включения/выключения клавиатуры в командном байте (порт 64h в режиме записи) определяют, является ли клавиатура активной, и будет ли контроллер клавиатуры вызывать прерывание в системе, когда пользователь нажмет клавишу.

Байты, записанные в порт 60h, посылаются контроллеру клавиатуры, а байты, записанные в порт 64h, посылаются системному контроллеру клавиатуры. Байты, считываемые из порта 60h, приходят от клавиатуры. Порт 60h при чтении содержит скан-код последней нажатой клавиши, а в режиме записи он используется для расширенного управления клавиатурой.

При использовании порта 60h на запись программа дополнительно получает следующие возможности:

- установка времени ожидания перед переходом клавиатуры в режим автоповтора;
- установка периода генерации скан-кода в режиме автоповтора;
- управление светодиодами, расположенными на лицевой панели клавиатуры - ScrollLock, NumLock, CapsLock.

Резюмируя сказанное, отметим, что для чтения данных, вводимых с клавиатуры, достаточно уметь считывать значения портов ввода-вывода 60h и 64h. Однако в ОС Windows приложениям пользовательского режима запрещено работать с портами, поэтому эту задачу выполняют драйвера операционной системы.

Методы защиты от кейлоггеров. Большинство антивирусных компаний добавляют известные кейлоггеры в свои базы, и метод защиты от них не отличается от метода защиты от любого другого вредоносного программного обеспечения. Однако так как большинство антивирусных продуктов относит кейлоггеры к классу потенциально опасного программного обеспечения, то следует удостовериться, что при настройках по умолчанию используемый антивирусный продукт детектирует наличие программ данного класса. Если это не так, то для детектирования кейлоггеров необходимо выставить подобную настройку вручную. Это позволит защититься от большинства широко распространяемых кейлоггеров.

Рассмотрим подробнее методы защиты от неизвестных кейлоггеров или кейлоггера, изготовленного специально для атаки конкретной системы.

Так как основной целью использования кейлоггеров является получение конфиденциальной информации (номера банковских карт, паролей и т.п.), то разумными методами защиты от неизвестных кейлоггеров являются следующие:

1) использование одноразовых паролей / двухфакторная аутентификация;
2) использование систем проактивной защиты, предназначенных для обнаружения программных кейлоггеров;
3) использование виртуальных клавиатур.

Одноразовый пароль действует только один раз, при этом часто ограничивается и период времени, в течение которого им можно воспользоваться. Поэтому, даже если такой пароль будет перехвачен, злоумышленник уже не сможет воспользоваться им для получения доступа к конфиденциальной информации.

Для получения одноразовых паролей могут использоваться специальные аппаратные устройства:

- в виде брелка (например, AladdineToken NG OTP);
- в виде «калькулятора» (например, RSA SecurID 900 SigningToken). На рис. 11 показан внешний вид таких устройств.

Рис. 11. Внешний вид аппаратных устройств

Для получения одноразовых паролей могут также использоваться системы, основанные на посылке SMS с мобильного телефона, зарегистрированного в системе, и получения в ответ PIN-кода, который нужно вводить вместе с персональным кодом при аутентификации.

В случае использования устройства генерации пароля в виде брелка, алгоритм получения доступа к защищенной информационной системе таков:

1) пользователь подключается к Интернету и открывает диалоговое окно для ввода персональных данных;

2) далее пользователь нажимает на кнопку ключа для генерации одноразового пароля, после этого пароль на 15 с появляется на ЖК-дисплее брелка;

3) пользователь вводит в диалоговом окне свой логин, персональный PIN-код и сгенерированное значение одноразового пароля (обычно PIN-код и ключ вводятся последовательно в одно поле passcode);

4) введенные значения проверяются на стороне сервера, после чего принимается решение о том, имеет ли право их владелец на работу с закрытыми данными.

При использовании устройства в виде калькулятора для генерации пароля пользователь набирает свой PIN-код на «клавиатуре» устройства и нажимает кнопку «>».

Генераторы одноразовых паролей широко применяются в банковской системе Европы, Азии, США и Австралии. Например, Lloyds TCB, один из самых крупных банков Великобритании, еще в ноябре 2005 г. перешел на использование генераторов одноразовых паролей.

Но в данном случае компании приходится нести значительные затраты, так как необходимо приобрести и распространить среди клиентов генераторы одноразовых паролей, а также разработать/приобрести соответствующее программное обеспечение.

Более дешевым решением является использование систем проактивной защиты на стороне клиентов банка (провайдера и т.д.), которые могут предупредить пользователя об установке или активизации программных кейлоггеров.

Главный недостаток этого способа – необходимость активного участия пользователя для определения дальнейших действий с подозрительным кодом. Если пользователь недостаточно технически подготовлен, то вследствие его некомпетентного решения кейлоггер может быть пропущен.

Если же участие пользователя в принятии решения системой проактивной защиты минимизировать, то кейлоггер может быть пропущен вследствие недостаточно жесткой политики безопасности системы. В то же время, если политика безопасности слишком жесткая, повышается опасность блокирования полезных программ, использующих перехват ввода с клавиатуры для легальных целей.

Последний из рассматриваемых способов защиты как от программных, так и от аппаратных кейлоггеров – использование виртуальной клавиатуры. Виртуальная клавиатура представляет собой программу, показывающую на экране изображение обычной клавиатуры, в которой с помощью мыши можно «нажимать» определенные клавиши.

Идея экранной клавиатуры не нова: в ОС Windows содержится встроенная экранная клавиатура, вызываемая через меню Start > Programs > Accessories > Accessibility > On-Screen Keyboard.

Однако встроенная в Windows экранная клавиатура плохо применима для обмана кейлоггеров, так как она создавалась не как средство защиты, а для помощи людям с ограниченными возможностями, и передача данных после ввода с помощью данной клавиатуры может быть очень легко перехвачена вредоносной программой. Экранная клавиатура, которая может быть использована для того, чтобы обойти кейлоггеры, должна быть разработана специальным образом, исключающим перехват вводимых данных на любой стадии их ввода и передачи.

Кроме того, для надежной защиты от клавиатурных шпионов администратор операционной системы должен соблюдать политику безопасности, при которой только администратор может:

- конфигурировать цепочки программных модулей, участвующих в процессе аутентификации пользователей;
- осуществлять доступ к файлам этих программных модулей;
- конфигурировать саму подсистему аутентификации.

Аппаратные кейлоггеры. Аппаратные кейлоггеры (*keystroke recording device*, *hard ware keylogger* и пр.) представляют собой миниатюрные приспособления (рис. 12), которые могут быть прикреплены между клавиатурой и компьютером или встроены в саму клавиатуру. Они регистрируют все нажатия клавиш, сделанные на клавиатуре. Процесс регистрации абсолютно невидим для конечного пользователя. Аппаратные кейлоггеры не требуют установки какой-либо программы на компьютере интересующего объекта, чтобы успешно перехватывать все нажатия клавиш.

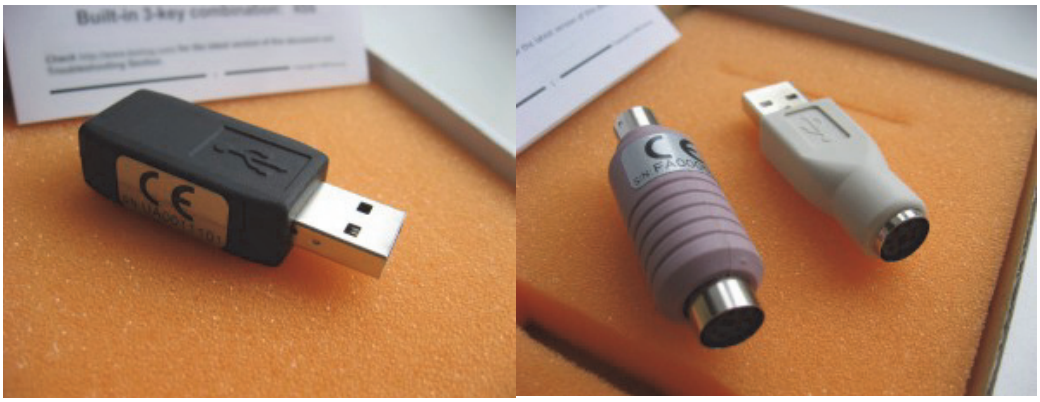


Рис. 12. Аппаратные кейлоггеры для USB-клавиатуры

Существуют три основных разновидности реализации аппаратных кейлоггеров: кейлоггер, встраиваемый в саму клавиатуру; кейлоггер, встраиваемый в разрыв кабеля, соединяющего клавиатуру и системный блок; кейлоггер, встраиваемый в системный блок компьютера. Самым распространенным является второй тип аппаратных кейлоггеров, один из самых известных примеров которых – Key Ghost USB Keylogger.

Такое устройство может быть тайно прикреплено к ПК объекта кем угодно – коллегой, уборщицей, посетителем и т.д. Когда аппаратный кейлоггер прикрепляется, абсолютно не имеет значения, в каком состоянии находится компьютер – включенном или выключенном. Затем атакующий может снять устройство в любой удобный момент, а его содержимое (записанные нажатия клавиш) скачать, когда ему это будет удобно. Объемы внутренней энергонезависимой памяти данных устройств позволяют записывать до 10 миллионов нажатий клавиш.

Данные устройства могут быть выполнены в любом виде, так что даже специалист не в состоянии иногда определить их наличие при проведении информационного аудита.

Особо известны на рынке следующие аппаратные кейлоггеры – KeyKatcher, KeyGhost, MicroGuard, HardwareKeyLogger, производителями которых являются компании AllenConceptsInc., Amecisco, KeyGhostLtd., MicroSpyLtd.

Современные аппаратные кейлоггеры представляют собой встроенные приспособления, которые выглядят, как оборудование для ПК. Сложнее всего обнаружить (и обезвредить) внутренний аппаратный кейлоггер, у которого аппаратный модуль перехвата нажатий клавиш встроен в корпус клавиатуры.

Современный внутренний аппаратный кейлоггер представляет собой встроенное приспособление, которое выглядит, как клавиатура ПК. Небольшое устройство, внедренное в разрыв шнура клавиатуры и покрытое теплоизоляционным материалом.

Его можно включить между компьютером и клавиатурой, и он начнёт записывать всё, что на ней набирается, никак себя не проявляя. А если нажать секретную комбинацию клавиш, то кейлоггер просто опознается системой как флешка, на которой будет лежать текстовый лог-файл, пара конфигурационных файлов с настройками устройства и простенькая программа для более удобного чтения лога. Всё предельно просто и функционально.

Интересно то, что для подключения устройства не нужно выключать компьютер (включать его тоже не нужно), клавиатура продолжает нормально работать.

8.1.2. Анализаторы протоколов

Анализатор трафика, или сниффер (от англ. *tosniff* – нюхать) – сетевой анализатор трафика, программа или программно-аппаратное устройство, предназначенное для перехвата и последующего анализа, либо только анализа сетевого трафика, предназначенного для других узлов, поэтому Sniffing (сниффинг – прослушивание сети).

Если вместо коммутаторов в сети установлены концентраторы, полученные пакеты рассылаются всем компьютерам в сети, а дальше уже компьютеры определяют, для них этот пакет или нет. Если взломщик получит доступ к компьютеру, который включен в такую сеть, или получит доступ к сети непосредственно, то вся информация, передаваемая в пределах сегмента сети, включая пароли, станет доступна. Взломщик просто поставит сетевую карту в режим прослушивания и будет принимать все пакеты независимо от того, ему ли они предназначались. Можно использовать как консольные снифферы, например TcpDump (встроенный в *NIX системах), WinDump (для Windows, но не встроенный), а так же с визуализированным интерфейсом, например Iris.

В настоящее время сети Ethernet завоевали огромную популярность, однако технология Ethernet не лишена существенных недостатков. Основной из них – передаваемая информация не защищена. Компьютеры, подключенные к сети Ethernet, оказываются в состоянии перехватывать информацию, адресованную своим соседям. Причиной тому является принятый в сетях Ethernet так называемый *широковещательный механизм обмена сообщениями.* Компьютер сети Ethernet, желающий передать какое-либо сообщение по общему каналу, должен удостовериться, что этот канал в данный момент свободен. В начале передачи компьютер прослушивает несущую частоту сигнала, определяя, не произошло ли искажения сигнала в результате возникновения коллизий с другими компьютерами, которые ведут передачу одновременно с ним. При наличии коллизии компьютер прерывает передачу и "замолкает". По истечении некоторого случайного пе-

риода времени он пытается повторить передачу. Если компьютер, подключенный к сети Ethernet, ничего не передает сам, он тем не менее продолжает "слушать" все сообщения, передаваемые по сети другими компьютерами. Заметив в заголовке поступившей порции данных свой сетевой адрес, компьютер копирует эти данные в свою базу. Таким образом, принятый в подавляющем большинстве Ethernet-сетей алгоритм передачи данных требует от каждого компьютера, подключенного к сети, непрерывного "прослушивания" всего без исключения сетевого трафика.

В дополнение к этому подавляющее большинство современных Ethernet-адаптеров допускают функционирование в особом режиме, называемом *беспорядочным* (promiscuous). При использовании данного режима адаптер копирует в локальную память компьютера все без исключения передаваемые по сети кадры данных.

Специализированные программы, переводящие сетевой адаптер в беспорядочный режим и собирающие весь трафик сети для последующего анализа, называются *анализаторами протоколов.* Администраторы сетей широко применяют анализаторы протоколов для осуществления контроля за работой этих сетей и определения их перегруженных участков, отрицательно влияющих на скорость передачи данных. К сожалению, анализаторы протоколов используются и злоумышленниками, которые с их помощью могут перехватывать чужие пароли и другую конфиденциальную информацию.

Анализаторы протоколов представляют серьезную опасность. Само присутствие в компьютерной сети анализатора протоколов указывает на то, что в ее защитных механизмах имеется брешь. Установить анализатор протоколов мог посторонний человек, который проник в сеть извне (например, если сеть имеет выход в Internet). Но это могло быть и делом рук злоумышленника, имеющего легальный доступ к сети.

Специалисты в области компьютерной безопасности относят атаки на компьютеры при помощи анализаторов протоколов к так называемым *атакам второго уровня.* Это означает, что компьютерный взломщик уже сумел проникнуть сквозь защитные барьеры сети и теперь стремится развить свой успех. При помощи анализатора протоколов он может попытаться перехватить регистрационные имена и пароли пользователей, их секретные финансовые данные (например, номера кредитных карточек) и конфиденциальные сообщения (к примеру, электронную почту).

Анализаторы протоколов существуют для любой платформы. Но даже если окажется, что для какой-то платформы анализатор протоколов пока еще не написан, с угрозой, которую представляет атака на компьютерную систему при помощи анализатора протоколов, по-прежнему приходится считаться. Дело в том, что анализаторы протоколов исследуют не конкретный компьютер, а протоколы, поэтому анализатор протоколов мо-

жет обосноваться в любом узле сети и оттуда перехватывать сетевой трафик, который в результате широковещательных передач попадает в каждый компьютер, подключенный к сети.

Использование анализатора протоколов на практике не является такой уж легкой задачей, как это может показаться. Чтобы добиться от него хоть какой-то пользы, компьютерный взломщик должен хорошо знать сетевые технологии. Просто установить и запустить анализатор протоколов нельзя, поскольку даже в небольшой локальной сети из пяти компьютеров трафик составляет тысячи и тысячи пакетов в час. И за короткое время выходные данные анализатора протоколов заполнят жесткий диск полностью. Поэтому компьютерный взломщик обычно настраивает анализатор протоколов так, чтобы он перехватывал только первые 200 – 300 байт каждого пакета, передаваемого по сети. Обычно именно в заголовке пакета размещается информация о регистрационном имени и пароле пользователя, которые, как правило, больше всего интересуют взломщика. Тем не менее, если в распоряжении взломщика имеется достаточно пространства на жестком диске, то увеличение объема перехватываемого трафика пойдет ему только на пользу. В результате он может дополнительно узнать много интересного.

На серверах в сети Internet есть множество анализаторов протоколов, которые отличаются лишь набором доступных функций. Например, поиск по запросам protocol analyzer и sniffer на сервере **www.softseek.com** сразу делает ссылки на добрый десяток программных пакетов.

Анализатор протоколов Network Monitor входит в состав операционной системы Windows NT 4.0 Server корпорации Microsoft. Для его установки следует в **Панели управления** (Control Panel) дважды щелкнуть на пиктограмме **Сеть** (Network), затем перейти на вкладку **Службы** (Senice), нажать кнопку **Добавить** (Add) и в появившемся диалоговом окне выбрать Network Monitor Toolsand Agent. После установки Network Monitor можно запустить из папки Network Analysis Tools раздела **Администрирование** (Administrative Tools) в меню **Программы** (Programs).

Защита от анализаторов протоколов

– Обзаведитесь сетевым адаптером, который буферизует каждое отправляемое по сети сообщение в памяти и посылает его по мере возможности точно по адресу. В результате надобность в "прослушивании" сетевым адаптером всего трафика для того, чтобы выбирать из него сообщения, адресатом которых является данный компьютер, отпадает.

– Не допускайте несанкционированной установки анализаторов протоколов на компьютеры сети. Для этого следует применять средства из арсенала, который повсеместно используется для борьбы с программными закладками и, в частности, – с троянскими программами.

– Шифруйте весь трафик сети. Имеется широкий спектр программных пакетов, которые позволяют делать это достаточно эффективно и надежно.

Особую известность среди компьютерных пользователей приобрела серия программных пакетов, предназначенных для защиты передаваемых по сети данных путем шифрования и объединенных присутствием в их названии аббревиатуры PGP, которая означает Pretty Good Privacy. Бесплатно распространяемые версии программ шифрования из этой серии можно отыскать в Internet по адресу **htt p://www.pgpi.org.**

Некоторые разновидности подобной атаки могут быть следующие.

IP Hijack (IP хайджек). Если есть физический доступ к сети, то взломщик может «врезаться» в сетевой кабель и выступить в качестве посредника при передаче пакетов, тем самым он будет слушать весь трафик между двумя компьютерами. Очень неудобный способ, который часто себя не оправдывает, за исключением случаев, когда никакой другой способ не может быть реализован. Подобное включение само по себе неудобно, хотя есть устройства, которые немного упрощают эту задачу, в частности они следят за нумерацией пакетов, чтобы избежать сбоя и возможного выявления вторжения в канал. Такой способ используется для обмана банкоматов, но такой случай технически сложнее, потому что недопустим разрыв связи между банком и банкоматом, а «врезание» в канал без его разрыва – задача только для высококвалифицированного специалиста. Кроме этого, теперь банкоматы устанавливаются гораздо лучше, что исключает возможность свободного физического доступа к кабелю. Защита от него – следить за доступом к кабелям, шифровать трафик.

Dummy ARP (ложный ARP). ARP сервер, маршрутизатор или коммутатор знают, какие IP принадлежат MAC адресам (т.е. сетевым картам). При возможности физического доступа к сети, взломщик может подделать ARP ответ и выдать себя за другой компьютер в сети, получив его IP. Тем самым все пакеты, предназначенные тому компьютеру, будет получать он. Это возможно, если тот компьютер выключен, иначе это действие вызовет конфликт IP адресов (в одной сети не могут быть 2 компьютера с одним и тем же IP адресом). Защита – использование ПО, которое информирует об изменении MAC адресов у IP, следить за лог-файлами ARP сервера.

Dummy DNS Server (ложный DNS сервер). Если настройки сети поставлены в автоматический режим, то при включении в сеть компьютер «спрашивает» (т.е. отправляет широковещательный пакет), кто будет его DNS сервером, к которому он в дальнейшем будет отправлять DNS запросы. При наличии физического доступа к сети, взломщик может перехватить такой широковещательный запрос и ответить, что его компьютер будет DNS сервером. После этого он сможет отправлять обманутую жертву по любому маршруту. Например, жертва хочет пройти на сайт банка и перевести деньги, взломщик может отправить её на свой компьютер, где будет сфабрикована форма ввода пароля. После этого пароль будет принадлежать взломщику. Достаточно сложный способ, потому что взломщику необходимо ответить жертве раньше, чем DNS сервер.

Рекомендации: по возможности ограничьте доступ к сети посторонних.

IP-Spoofing (спуфинг или подмена IP адреса). Атакующий подменяет свой реальный IP фиктивным. Это необходимо, если доступ к ресурсу имеют только определённые IP адреса. Взломщику нужно изменить свой реальный IP на «привилегированный» или «доверенный», чтобы получить доступ. Этот способ может быть использован по-другому. После того как два компьютера установили между собой соединение, проверив пароли, взломщик может вызвать на жертве перегрузку сетевых ресурсов специально сгенерированными пакетами. Тем самым он может перенаправить трафик на себя и таким образом обойти процедуру аутентификации. Рекомендации: их может быть много, по той причине, что приёмов достаточно много. Но стоит упомянуть, что угрозу снизит (но возможно затруднит легимитивные соединения) уменьшение времени ответного пакета с установленными флагами SYN и ACK, а также увеличит максимальное количество SYN-запросов на установление соединения в очереди (tcp_max_backlog). Также можно использовать SYN-Cookies.

Hostspoofing (подмена хоста). Очень сложная техника, требующая физического доступа к сети. Каждый компьютер знает маршрутизатор, на который он отправляет все пакеты, которые потом маршрутизатором доставляются по назначению. При смене маршрутизатора каждому компьютеру высылается redirect уведомление, после чего компьютеры начинают посылать пакеты новому маршрутизатору. Взломщик может сфабриковать подобное уведомление и выдать себя за маршрутизатор, таким образом, он получит контроль над трафиком в пределах сегмента сети.

Для защиты необходим контроль над доступом к сети и моментом смены маршрутизатора. Например, можно следить, весь ли прошлый трафик (т.е. старые соединения) «появились» на новом маршрутизаторе.

Back Connect/Pipes/Reverse (обратный сеанс или реверс). Это вспомогательный приём, но сам по себе он очень интересный. Например, взломщик не хочет каждый раз выполнять много действий ради одной команды. Он может упростить задачу, используя этот приём. Суть его в том, что взломщик вынуждает атакуемый компьютер подключиться к компьютеру взломщика. Например, на атакуемом компьютере можно выполнить команду telnet [ip.адрес взломщика] [порт]. После этого взломщик, по сути дела, получает командную строку (командную оболочку или Шелл/Shell) на атакуемом компьютере.

Soft warevul nerabilities (ошибки ПО). Использование ошибок в программном обеспечении. Эффект может быть разный. От получения несущественной информации до получения полного контроля над системой. Атаки через ошибки ПО самые популярные во все времена. Старые ошибки исправляются новыми версиями, но в новых версиях появляются новые ошибки, которые опять могут быть использованы.

8.1.3. Парольные взломщики

Взломщик паролей – это любая программа, которая может расшифровывать пароли или каким-либо другим способом снимать парольную защиту (например, расшифровать файл без знания правильного пароля). Если механизмы парольной защиты используют слабое шифрование, то иногда можно восстановить изначальный пароль или подобрать другой, который считается верным.

Целью взлома пароля может являться помощь пользователю в восстановлении забытого пароля, получение несанкционированного доступа к системе или же профилактическая мера, когда системные администраторы проверяют, насколько легко взламываются пароли.

Для стойких алгоритмов (когда атакующий может только генерировать и проверять пароли) существуют два основных метода: атака перебором и по словарю. Атака перебором, или **метод «грубой силы»**, (англ. *bruteforce*) используется тогда, когда нет никакой дополнительной информации о пароле, и атакующий просто пробует все возможные пароли. Эффективность этого метода зависит от мощности процессора и его быстродействия. В табл. 1 представлено оценочное время полного перебора паролей в зависимости от их длины. Предполагается, что в пароле могут использоваться 36 различных символов (латинские буквы одного регистра плюс цифры), а скорость перебора составляет 100 000 паролей в секунду (класс атаки B, типичный для восстановления пароля из Кэша Windows (.PWL файлов) на Pentium 100).

Таблица 1

Количество знаков	**Количество вариантов**	**Стойкость**	**Время перебора**
1	36	5 бит	менее секунды
2	1296	10 бит	менее секунды
3	46 656	15 бит	менее секунды
4	1 679 616	21 бит	17 секунд
5	60 466 176	26 бит	10 минут
6	2 176 782 336	31 бит	6 часов
7	78 364 164 096	36 бит	9 дней
8	$2{,}821\ 109\ 9 \times 10^{12}$	41 бит	11 месяцев
9	$1{,}015\ 599\ 5 \times 10^{14}$	46 бит	32 года
10	$3{,}656\ 158\ 4 \times 10^{15}$	52 бита	1 162 года
11	$1{,}316\ 217\ 0 \times 10^{17}$	58 бит	41 823 года
12	$4{,}738\ 381\ 3 \times 10^{18}$	62 бита	1 505 615 лет

Таким образом, пароли длиной до 8 символов включительно в общем случае не являются надежными.

Зачастую, с целью проще запомнить пароль, в качестве его устанавливают имя знакомого человека, любимого животного и т.д., что значительно облегчает его взлом злоумышленнику. Если взломщик знает, что пароль – это некое существующее слово, то он может использовать атаку по словарю. Тогда в качестве паролей-кандидатов проверяются только слова из словаря. В словаре содержится менее 100 000 слов, так что их можно проверить очень быстро – в большинстве случаев это занимает всего несколько секунд.

Самая мощная – "атака на основе правил". Она может быть использована в тех случаях, когда взломщик обладает какой-либо информацией о пароле, который он хочет взломать. Например, ему известно, что пароль состоит из слова и одно- или двузначного числа. Он пишет правило, и программа генерирует только подходящие пароли (user1, mind67, snapshot99 и т.д.). Или другой пример: атакующий знает, что первая буква в верхнем регистре, вторая – гласная и что пароль не длиннее 6 символов. Такая информация может уменьшить количество возможных паролей в 20 - 30 раз. Этот метод включает все атаки - перебором, по словарю и по слогам.

И, наконец, некоторые слабые алгоритмы позволяют использовать атаку "по известному открытому тексту". Это означает, что взломщик имеет несколько файлов или фрагментов файлов в расшифрованном виде и хочет расшифровать другие. Сильные криптоалгоритмы успешно противостоят этому типу атак – знание расшифрованного файла ничего не даст взломщику.

Как работает парольный взломщик? Криптографические алгоритмы, применяемые для шифрования паролей пользователей в современных операционных системах, в подавляющем большинстве случаев являются слишком стойкими, чтобы можно было надеяться отыскать методы их дешифрования, которые окажутся более эффективными, чем тривиальный перебор возможных вариантов. Поэтому парольные взломщики иногда просто шифруют все пароли с использованием того же самого криптографического алгоритма, который применяется для их засекречивания в атакуемой операционной системе, и сравнивают результаты шифрования с тем, что записано в системном файле, где находятся шифрованные пароли ее пользователей. При этом в качестве вариантов паролей парольные взломщики используют символьные последовательности, автоматически генерируемые из некоторого набора символов. Данный способ позволяет взломать все пароли, если известно их представление в зашифрованном виде и они содержат только символы из данного набора. Максимальное время, которое потребуется для взлома пароля, можно вычислить по следующей формуле:

$$t = c / s,$$

где t – время перебора, c – количество комбинаций символов (паролей), $c = x \wedge y$, x – число возможных символов, y – количество символов в пароле; s – скорость перебора.

Пример: полное время перебора пароля длиной в 12 символов, с использованием букв латинского алфавита и цифр, со скоростью перебора в 5 миллионов паролей в секунду, будет равно:

$$t = ((26 + 10) \wedge 12) / 5\,000\,000,$$

$$t = 4738381338321616896 / 5\,000\,000,$$

$$t \sim 947676267664 \text{ (секунды), или } \sim 30\,050 \text{ лет.}$$

Из приведенной формулы видно, что за счет очень большого числа перебираемых комбинаций, которое растет экспоненциально с увеличением числа символов в исходном наборе, такие атаки парольной защиты операционной системы могут занимать слишком много времени. Однако хорошо известно, что большинство пользователей операционных систем не затрудняют себя выбором стойких паролей, поэтому для более эффективного подбора паролей парольные взломщики обычно используют так называемые словари, представляющие собой заранее сформированный список слов, наиболее часто применяемых на практике в качестве паролей.

Для каждого слова из словаря парольный взломщик использует одно или несколько правил. В соответствии с этими правилами слово изменяется и порождает дополнительное множество опробуемых паролей. Производится попеременное изменение буквенного регистра, в котором набрано слово, порядок следования букв в слове меняется на обратный, в начало и в конец каждого слова приписывается цифра 1, некоторые буквы заменяются на близкие по начертанию цифры (в результате, например, из слова password получается pa55wOrd). Это повышает вероятность подбора пароля, поскольку в современных операционных системах, как правило, различаются пароли, набранные заглавными и строчными буквами, а пользователям этих систем настоятельно рекомендуется выбирать пароли, в которых буквы чередуются с цифрами.

Одни парольные взломщики поочередно проверяют каждое слово из словаря, применяя к нему определенный набор правил для генерации дополнительного множества опробуемых паролей. Другие предварительно обрабатывают весь словарь при помощи этих же правил, получая новый словарь большего размера, и затем из него черпают проверяемые пароли. Учитывая, что обычные словари человеческих языков состоят всего из нескольких сотен тысяч слов, а скорость шифрования паролей достаточно высока, парольные взломщики, осуществляющие поиск с использованием словаря, работают достаточно быстро.

Взлом парольной защиты операционной системы UNIX

В операционной системе UNIX информацию о пароле любого пользователя можно отыскать в файле passwd, находящемся в каталоге etc. Эта информация хранится в зашифрованном виде и располагается через двоеточие сразу после имени соответствующего пользователя. Например, запись, сделанная в файле passwd относительно пользователя с именем bill, будет выглядеть примерно так:

bill:5fg63fhD3d5g:9406:12:Bill Spencer:/home/fsg/will:/bin/bash

Здесь 5fg63fhD3d5g – это и есть информация о пароле пользователя bill.

При первоначальном задании или изменении пользовательского пароля операционная система UNIX генерирует два случайных байта (в приведенном выше примере 5 и f), к которым добавляются байты пароля. Полученная в результате байтовая строка шифруется при помощи специальной криптографической процедуры Crypt2 (в качестве ключа используется пароль пользователя) и в зашифрованном виде (g63fliD3d5g) вместе с двумя случайными байтами (5f) записывается в файл /etc/passwd после имени пользователя и двоеточия.

Если злоумышленник имеет доступ к парольному файлу операционной системы UNIX, то он может скопировать этот файл на свой компьютер и затем воспользоваться одной из программ для взлома парольной защиты UNIX.

Существует множество программ взлома паролей операционной системы UNIX. Они устойчивы к сбоям электропитания компьютеров, на которых работают, позволяют планировать время своей работы, при выполнении монополизируют процессор для достижения максимальной производительности, не только взламывают пароли операционной системы UNIX, но и помогают преодолеть парольную защиту других программ, которые требуют, чтобы пользователь зарегистрировался путем ввода своего имени и соответствующего пароля.

Взлом парольной защиты операционной системы Windows NT. Одним из основных компонентов системы безопасности Windows NT является *диспетчер учетных записей* пользователей. Он обеспечивает взаимодействие других компонентов системы безопасности, приложений и служб Windows NT с базой данных учетных записей пользователей (Security Account Management Database, SAM). Эта база обязательно имеется на каждом компьютере с операционной системой Windows NT. В ней хранится вся информация, используемая для аутентификации пользователей Windows NT при интерактивном входе в систему и при удаленном доступе к ней по компьютерной сети.

База данных SAM представляет собой один из кустов (hive) системного реестра (registry) Windows NT. Этот куст принадлежит ветви (subtree) HKEY_LOCAL_MACHINE и называется SAM. Он располагается в катало-

ге \wmnt_root\System32\ConfIg (winnt_root – условное обозначение каталога с системными файлами Windows NT) в отдельном файле, который тоже называется SAM.

Информация в базе данных SAM хранится в основном в двоичном виде. Доступ к ней обычно осуществляется через диспетчер учетных записей. Изменять записи, находящиеся в базе данных SAM, при помощи программ, позволяющих напрямую редактировать реестр Windows NT (REGEDT или REGEDT32), не рекомендуется. По умолчанию этого и нельзя делать, т. к. доступ к базе данных SAM запрещен для всех без исключения категорий пользователей операционной системы Windows NT.

Именно в учетных записях базы данных SAM находится информация о пользовательских именах и паролях, которая необходима для идентификации и аутентификации пользователей при их интерактивном входе в систему. Как и в любой другой современной многопользовательской операционной системе, эта информация хранится в зашифрованном виде. В базе данных SAM каждый пароль пользователя обычно бывает представлен в виде двух 16-байтовых последовательностей, полученных разными методами.

При использовании первого метода строка символов пользовательского пароля хэшируется с помощью функции MD4. В итоге из символьного пароля, введенного пользователем, получается 16-байтовая последовательность – хэшированный пароль Windows NT. Данная последовательность затем шифруется по DES-алгоритму, и результат шифрования сохраняется в базе данных SAM. При этом в качестве ключа используется так называемый относительный идентификатор пользователя (RelativeIdentifier, RID), который представляет собой автоматически увеличивающийся порядковый номер учетной записи данного пользователя в базе данных SAM.

Для совместимости с другим программным обеспечением корпорации Microsoft (Windowsfor Workgroups, Windows 95/98 и LanManager) в базе данных SAM хранится также информация о пароле пользователя в стандарте LanManager. Для ее формирования используется второй метод. Все буквенные символы исходной строки пользовательского пароля приводятся к верхнему регистру, и, если пароль содержит меньше 14 символов, то он дополняется нулями. Из каждой 7-байтовой половины преобразованного таким образом пароля пользователя отдельно формируется ключ для шифрования фиксированной 8-байтовой последовательности по DES-алгоритму. Полученные в результате две 8-байтовые половины хэшированного пароля LanManager еще раз шифруются по DES-алгоритму (при этом в качестве ключа используется RID пользователя) и помещаются в базу данных SAM.

Информация о паролях, занесенная в базу данных SAM, служит для аутентификации пользователей Windows NT. При интерактивном или се-

тевом входе в систему введенный пользователем пароль сначала хэшируется и шифруется, а затем сравнивается с 16-байтовой последовательностью, записанной в базе данных SAM. Если они совпадают, то пользователю разрешается вход в систему.

Обычно в базе данных SAM хранятся в зашифрованном виде оба хэшированных пароля. Однако в некоторых случаях операционная система вычисляет только один из них. Например, если пользователь домена Windows NT изменит свой пароль, работая на компьютере с Windows for Workgroups, то в его учетной записи останется только пароль Lan Manager. А если пользовательский пароль содержит более 14 символов или если эти символы не входят в так называемый *набор поставщика оборудования* (original equipment manufacturer, OEM), то в базу данных SAM будет занесен только пароль Windows NT.

Возможные атаки на базу данных SAM. Обычно основной целью взломщиков парольной защиты операционной системы являются административные полномочия. Их можно получить, узнав хэшированием или в символьном виде пароль администратора системы, который хранится в базе данных SAM. Поэтому именно на базу данных SAM бывает направлен главный удар взломщика парольной защиты Windows NT.

По умолчанию в операционной системе Windows NT доступ к файлу \winnt_root\System32\Config\SAM заблокирован для всех без исключения ее пользователей. Тем не менее с помощью программы NTBACKUP любой обладатель права на резервное копирование файлов и каталогов Windows NT может перенести этот файл с жесткого диска на флешку. Резервную копию реестра также можно создать утилитой REG BAK из Windows NT ResourceKit. Кроме того, несомненный интерес для любого взломщика представляют резервная копия файла SAM (SAM.SAV) в каталоге \winnt_root\System32\Config и сжатая архивная копия SAM (файл SAM._) в каталоге \winnt_root\Repair.

При наличии физической копии файла SAM извлечь хранимую в нем информацию не представляет никакого труда. Загрузив файл SAM в реестр любого другого компьютера с Windows NT (например, с помощью команды LoadHive программы REGEDT32), можно в деталях изучить учетные записи пользователей, чтобы определить значения RID пользователей и шифрованные варианты их хэшированных паролей. Зная RID пользователя и имея зашифрованную версию его хэшированного пароля, компьютерный взломщик может попытаться расшифровать этот пароль, чтобы использовать его, например, для получения сетевого доступа к другому компьютеру.

Для восстановления пользовательских паролей операционной системы Windows NT в символьном виде существуют специальные парольные взломщики, которые выполняют как прямой подбор паролей, так и поиск по словарю, а также используют комбинированный метод взлома парольной зашиты.

Защита системы от парольных взломщиков. Итак, одна из главных задач системного администратора Windows NT состоит в защите от несанкционированного доступа к той информации, которая хранится в базе данных SAM. С этой целью ему, прежде всего, необходимо ограничить физический доступ к компьютерам сети и прежде всего – к контроллерам доменов. Дополнительно, при наличии соответствующих программно-аппаратных средств, следует установить пароли BIOS на включение компьютеров и на изменение настроек BIOS. Затем, используя настройки BIOS, рекомендуется отключить загрузку компьютеров с гибких и компакт-дисков. А для обеспечения контроля доступа к файлам и папкам операционной системы Windows NT системный раздел жесткого диска должен иметь формат NTFS.

Системные администраторы также должны внимательно следить за тем, где и как хранятся диски аварийного восстановления (Emergency Repair Disks) и архивные копии, если на последних присутствует дубликат системного реестра Windows NT.

8.1.4. Фишинг

Фишинг (англ. *phishing* – рыбная ловля, выуживание) – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям. Это достигается путём проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей. В письме часто содержится прямая ссылка на сайт, внешне неотличимый от настоящего, либо на сайт с редиректом. После того как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приёмами побудить пользователя ввести на поддельной странице свои логин и пароль, которые он использует для доступа к определённому сайту, что позволяет мошенникам получить доступ к аккаунтам и банковским счетам (рис. 13). Это одна из разновидностей социальной инженерии, основанная на незнании пользователями основ сетевой безопасности: в частности, многие не знают простого факта – сервисы не рассылают писем с просьбами сообщить свои учётные данные, пароль и прочее.

Целью фишеров чаще всего являются клиенты банков и электронных платёжных систем. Фишеры могут определить, какими услугами пользуется жертва, и применять целенаправленную рассылку.

Социальные сети также представляют большой интерес для фишеров, позволяя собирать личные данные пользователей. По оценкам специалистов, более 70 % фишинговых атак в социальных сетях успешны.

Техника фишинга. Человек всегда реагирует на значимые для него события, поэтому фишеры стараются своими действиями встревожить пользователя и вызвать его немедленную реакцию. К примеру, электронное письмо с заголовком «чтобы восстановить доступ к своему банковскому счёту …», как правило, привлекает внимание и заставляет человека пройти по веб-ссылке для получения более подробной информации.

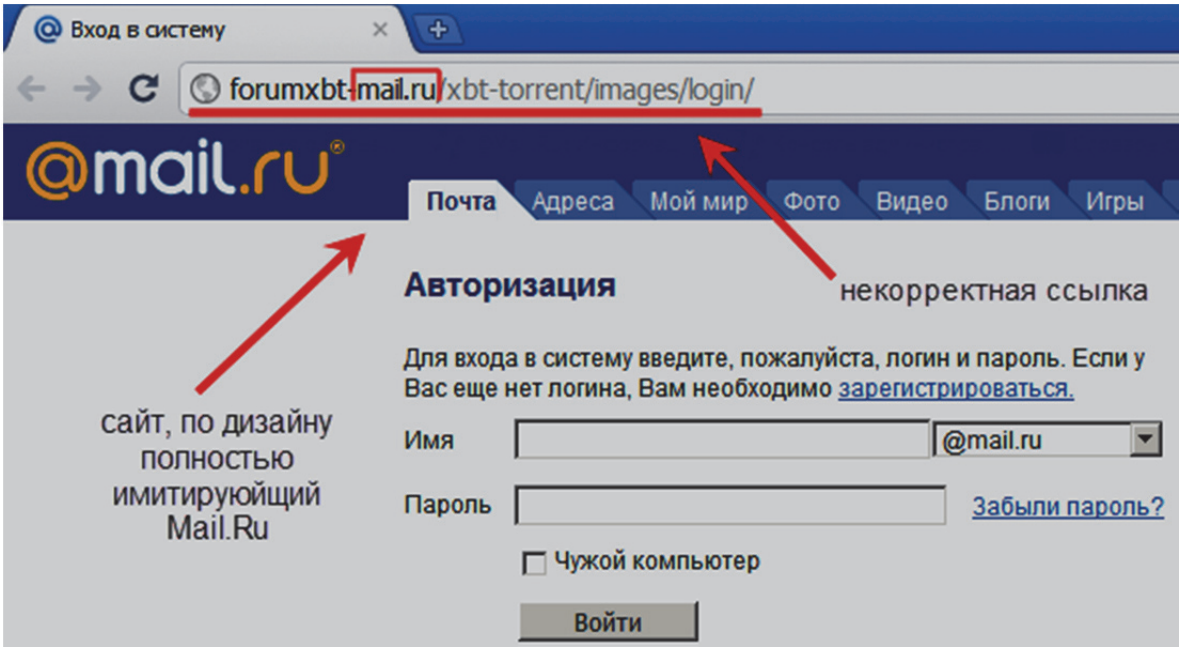


Рис. 13. Пример фишингового письма от Mail.ru,
где веб-ссылка ведёт на фишинговый сайт

Фишинговые сообщения могут содержать:

- сведения, вызывающие тревогу, или угрозы, например, закрытия ваших банковских счетов;
- обещания большой денежной выгоды с минимальными усилиями или вовсе без них;
- сведения о сделках, которые слишком хороши для того, чтобы быть правдой;
- запросы о пожертвованиях от лица благотворительных организаций после сообщений в новостях о стихийных бедствиях;
- грамматические и орфографические ошибки.

Наиболее популярные фишинговые уловки, о которых вам необходимо знать.

Мошенничество с использованием бренда Microsoft или других известных компаний. В таких мошеннических схемах используются поддельные сообщения электронной почты или веб-сайты, содержащие название корпорации Microsoft. В них вам могут сообщать о победе в каком-либо конкурсе, проводимом компанией, о том, что Microsoft требуются

ваши учетные данные и пароль, о том, что к вам обращается представитель Microsoft, чтобы помочь в решении проблем с компьютером, и т.п. Подобные мошеннические схемы от лица службы технической поддержки также могут производиться по телефону.

Подложные лотереи. Вы можете получить сообщения, в которых говорится о том, что вы выиграли в лотерею, которая проводится корпорацией Microsoft. Внешне эти сообщения могут выглядеть так, как будто они были отправлены от лица одного из высокопоставленных сотрудников компании. Понятно, что никаких лотерей Microsoft не существует.

Ложные антивирусы и программы для обеспечения безопасности – это программы, которые выглядят так, как будто они обеспечивают безопасность вашего ПК, хотя, на самом деле, все обстоит совсем наоборот. Такие программы генерируют ложные уведомления о различных угрозах, а также пытаются завлечь пользователя в мошеннические транзакции. С ними можно столкнуться в электронной почте, онлайн объявлениях, в социальных сетях, в результатах поисковых систем и даже во всплывающих окнах на компьютере, которые имитируют системные сообщения.

Большинство методов фишинга сводится к тому, чтобы замаскировать поддельные ссылки на фишинговые сайты под ссылки настоящих организаций. Адреса с опечатками или субдомены часто используются мошенниками.

Например http://www.yourbank.example.com/ похож на адрес банка Yourbank, а на самом деле он ссылается на фишинговую составляющую сайта example.com. Другая распространённая уловка заключается в использовании внешне правильных ссылок, в реальности ведущих на фишинговый сайт. Например, http://ru.wikipedia.org/wiki/Правда приведёт не на статью «Правда», а на статью «Ложь».

Один из старых методов обмана заключается в использовании ссылок, содержащих символ «@», который применяется для включения в ссылку имени пользователя и пароля. Например, ссылка http://www.google.com@members.tripod.com/ приведёт не на www.google.com, а на members.tripod.com от имени пользователя www.google.com. Эта функциональность была отключена в Internet Explorer, а Mozilla Firefox и Opera выдают предупреждение и предлагают подтвердить переход на сайт. Но это не отменяет использование в HTML-теге `<a>` значения href, отличного от текста ссылки.

Ещё одна проблема была обнаружена при обработке браузерами Интернациональных Доменных Имён: адреса, визуально идентичные официальным, могли вести на сайты мошенников.

Обход фильтров. Фишеры часто вместо текста используют изображения, что затрудняет обнаружение мошеннических электронных писем антифишинговыми фильтрами. Но специалисты научились бороться и с этим видом фишинга. Так, фильтры почтовых программ могут автомати-

чески блокировать изображения, присланные с адресов, не входящих в адресную книгу. К тому же появились технологии, способные обрабатывать и сравнивать изображения с сигнатурами однотипных картинок, используемых для спама и фишинга.

Обман не заканчивается на посещении жертвой фишингового сайта. Некоторые фишеры используют JavaScript для изменения адресной строки. Это достигается либо путём размещения картинки с поддельным URL поверх адресной строки либо закрытием настоящей адресной строки и открытием новой с поддельным URL.

Злоумышленник может использовать уязвимости в скриптах подлинного сайта. Этот вид мошенничества (известный как межсайтовый скриптинг) наиболее опасен, так как пользователь авторизуется на настоящей странице официального сайта, где всё, – от веб-адреса до сертификатов, выглядит подлинным. Подобный фишинг очень сложно обнаружить без специальных навыков.

Для противостояния антифишинговым сканерам фишеры начали использовать веб-сайты, основанные на технологии Flash. Внешне подобный сайт выглядит как настоящий, но текст скрыт в мультимедийных объектах.

Сегодня фишинг выходит за пределы интернет-мошенничества, а поддельные веб-сайты стали лишь одним из множества его направлений. Письма, которые якобы отправлены из банка, могут сообщать пользователям о необходимости позвонить по определённому номеру для решения проблем с их банковскими счетами. Эта техника называется вишинг (голосовой фишинг). Позвонив на указанный номер, пользователь заслушивает инструкции автоответчика, которые указывают на необходимость ввести номер своего счёта и PIN-код. К тому же вишеры могут сами звонить жертвам, убеждая их, что они общаются с представителями официальных организаций, используя фальшивые номера. В конечном счёте человека также попросят сообщить его учётные данные.

Набирает свои обороты и SMS-фишинг, также известный как смишинг (англ. *SMiShing* – от «SMS» и «фишинг»). Мошенники рассылают сообщения, содержащие ссылку на фишинговый сайт, – входя на него и вводя свои личные данные, жертва аналогичным образом передаёт их злоумышленникам. В сообщении также может говориться о необходимости позвонить мошенникам по определённому номеру для решения «возникших проблем». Встречается и следующий вид SMS-фишинга: на подставном сайте для получения какой-либо услуги просят отправить SMS на предложенный номер или ввести свой номер сотового телефона. В первом случае с телефонного счёта абонента списывается крупная (возможно, максимальная предусмотренная контрактом) сумма, во втором случае номер добавляется в базу адресов рассылки SMS-спама и может использоваться для дальнейших фишинговых действий.

Борьба с фишингом. Существуют различные методы для борьбы с фишингом, включая законодательные меры и специальные технологии, созданные для защиты от фишинга. Один из методов борьбы с фишингом заключается в том, чтобы научить людей различать фишинг и бороться с ним. Можно снизить угрозу фишинга, немного изменив своё поведение. Так, в ответ на письмо с просьбой «подтверждения» учётной записи (или любой другой обычной просьбой фишеров) специалисты советуют связаться с компанией, от имени которой отправлено сообщение, для проверки его подлинности. Кроме того, эксперты рекомендуют самостоятельно вводить веб-адрес организации в адресную строку браузера вместо использования любых гиперссылок в подозрительном сообщении.

Практически все подлинные сообщения организаций содержат в себе упоминание информации, недоступной для фишеров. Например, всегда обращаются к своим адресатам по именам, а письмо с общим обращением «Уважаемый клиент …» может расцениваться как попытка фишинга. Людям можно объяснить, что подозрительны любые письма, не содержащие какой-либо конкретной личной информации.

Для защиты от фишинга производители основных браузеров договорились о применении одинаковых способов информирования пользователей о том, что они открыли подозрительный сайт, который может принадлежать мошенникам. Новые версии браузеров уже обладают такой возможностью, которая соответственно именуется «антифишинг».

Другим направлением борьбы с фишингом является создание списка фишинговых сайтов и последующая сверка с ним. Подобная система существует в браузерах Internet Explorer, Mozilla Firefox, Google Chrome, Safari и Opera. Firefox использует антифишинговую систему Google. Opera использует чёрные списки Phish Tank и Geo Trust и списки исключений Geo Trust.

8.1.5. Сетевая разведка

Сетевой разведкой (Portsscan) называется сбор информации о сети с помощью общедоступных данных и приложений. При подготовке атаки против какой-либо сети хакер, как правило, пытается получить о ней как можно больше информации. Это получение и обработка данных об информационной системе клиента, ресурсах информационной системы, используемых устройств и программного обеспечения и их уязвимостях, средств защиты, а также о границе проникновения в информационную систему.

В ходе такой разведки злоумышленник не производит никаких деструктивных действий. Он может производить сканирование портов, запросы DNS, эхо-тестирование открытых портов, наличие и защищённость прокси-серверов. В результате можно получить информацию о существу-

ющих в системе DNS-адресах, кому они принадлежат, какие сервисы на них доступны, уровень доступа к этим сервисам для внешних и внутренних пользователей.

DNS (*Domain Name System*) – это распределенная база данных, поддерживающая иерархическую систему имен для идентификации узлов в сети Internet. Служба DNS предназначена для автоматического поиска IP-адреса по известному символьному имени узла. Спецификация DNS определяется стандартами RFC 1034 и 1035. DNS требует статической конфигурации своих таблиц, отображающих имена компьютеров в IP-адрес.

Протокол DNS является служебным протоколом прикладного уровня. Этот протокол несимметричен – в нем определены DNS-серверы и DNS-клиенты. DNS-серверы хранят часть распределенной базы данных о соответствии символьных имен и IP-адресов. Эта база данных распределена по административным доменам сети Internet. Клиенты сервера DNS знают IP-адрес сервера DNS своего административного домена и по протоколу IP передают запрос, в котором сообщают известное символьное имя и просят вернуть соответствующий ему IP-адрес.

Сетевая разведка проводится в форме запросов DNS, эхо-тестирования (pingsweep) и сканирования портов. Запросы DNS помогают понять, кто владеет тем или иным доменом и какие адреса этому домену присвоены. Эхо-тестирование адресов, раскрытых с помощью DNS, позволяет увидеть, какие хосты реально работают в данной среде. Получив список хостов, хакер использует средства сканирования портов, чтобы составить полный список услуг, поддерживаемых этими хостами. И, наконец, хакер анализирует характеристики приложений, работающих на хостах. В результате добывается информация, которую можно использовать для взлома.

Современная сетевая разведка в зависимости от целей деятельности, масштаба и характера, поставленных для выполнения задач делится:

- на стратегическую.
- тактическую (оперативную).

Тактическая разведка обеспечивает действия атакующих. К ним относятся как злоумышленники, так и специалисты, проводящие тестирование информационной системы. Тактическая разведка выявляет данные:

- о технической оснастке;
- программном оснащении;
- уязвимости почтовых серверов;
- сервисах и почтовых клиентах;
- границах сегментов сети;
- используемых каналах связи (тип, пропускная способность);
- государственной (географической, коммерческой) принадлежности сети и/или сервера, что облегчает принятие оптимальных решений по планированию и проведению атаки на информационные системы.

Эти сведения добываются перехватом информации, передаваемой радиоэлектронными средствами.

Действия хакера зависят от задачи, поставленной им, будь то изменение информации, кража, повышение полномочий и удержание системы. Алгоритм действия сетевой разведки чаще всего следующий:

- обработка данных, выбор уязвимой точки для проникновения;
- эксплуатация уязвимости, проникновение в систему.

Возможные пути получения данных:

- получение информации от whois-серверов;
- просмотр информации DNS серверов исследуемой сети для выявления записей, определяющих маршруты электронной почты (MX записи);
- информация об электронной почте, представленная на сайте исследуемой компании. К ней относятся адреса электронной почты для связи, опубликованные вакансии для системных администраторов и администраторов электронной почты, в которых зачастую есть информация о типах используемых почтовых серверов;
- информация об электронной почте (адресах) и вакансиях, сохранившаяся в поисковых системах (google.com, yandex.ru) и в базах компаний, запоминающих состояния веб-ресурсов на определенный срок.

После определения границ атаки атакующие переходят к получению данных о целевой почтовой системе. Для этого используется чаще всего сканирование портов (сервисов) на выявленных внешних серверах, которое проводится с целью:

- определить доступность сервиса из различных подсетей, расположенных по всему миру;
- выявить почтовые сервисы на нестандартных портах;
- получить и проанализировать информацию, выдаваемую почтовыми сервисами при соединении. Banner grabbing – так этот метод принято называть среди специалистов по сетевой разведке;
- проверить сервис (SMTP, POP3, POP3pw, IMAP) для определения типа и версии, допуская возможность, что администратор системы изменил информацию, выдаваемую сервисами, или сервис не выводит информацию о своем типе и версии;
- отправить письма на несуществующие почтовые адреса для получения NDR (non delivery report) и информации о пути прохождения письма.

Противодействие сетевой разведке. Полностью избавиться от сетевой разведки невозможно. Если, к примеру, отключить эхо ICMP и эхо-ответ на периферийных маршрутизаторах, то можно избавиться от эхо-тестирования, но при этом теряются данные, необходимые для диагностики сетевых сбоев. Кроме того, сканировать порты можно без предварительного эхо-тестирования. Этой займет больше времени, так как сканировать придется и несуществующие IP-адреса. Системы IDS на уровне сети и

хостов обычно хорошо справляются с задачей уведомления администратора о ведущейся сетевой разведке, что позволяет лучше подготовиться к предстоящей атаке и оповестить провайдера (ISP), в сети которого установлена система.

8.1.6. "Сборка мусора"

Если в ОС допускается восстановление ранее удаленных объектов, то хакер может воспользоваться этой возможностью для восстановления объектов, удаленных другими пользователями. В простейшем случае хакеру достаточно просмотреть чужую “мусорную корзину”. Если хакер использует для сборки мусора программную закладку, то он может “собирать мусор” не только на дисках компьютера, но и в оперативной памяти.

8.2. Типичные хакерские атаки для нанесения вреда системе

Успех реализации того или иного алгоритма хакерской атаки в значительной степени зависит от архитектуры и конфигурации конкретной операционной системы, являющейся объектом этой атаки.

В общем случае программное обеспечение любой универсальной компьютерной системы состоит из трех основных компонентов: операционной системы, сетевого программного обеспечения (СПО) и системы управления базами данных (СУБД), поэтому все попытки взлома защиты компьютерных систем можно разделить на три группы:

1) атаки на уровне операционной системы;
2) атаки на уровне сетевого программного обеспечения;
3) атаки на уровне систем управления базами данных.

Атаки на уровне операционной системы. Защищать операционную систему довольно трудно – внутренняя структура ОС чрезвычайно сложна, и поэтому соблюдение адекватной политики безопасности является трудной задачей.

Бытует мнение, что самые эффективные атаки на операционные системы могут быть организованы только с помощью сложнейших средств, основанных на самых последних достижениях науки и техники, а хакер должен быть программистом высочайшей квалификации. Это не совсем так.

Разумеется, пользователю следует быть в курсе всех новинок в области компьютерной техники. Да и высокая квалификация – совсем не лишнее. Однако искусство хакера состоит отнюдь не в том, чтобы уметь взламывать любую самую "крутую" компьютерную защиту. Нужно просто суметь найти слабое место в конкретной системе защиты. При этом простейшие методы взлома оказываются ничуть не хуже самых изощренных, поскольку, чем проще алгоритм атаки, тем больше вероятность ее завершения без ошибок и сбоев.

Нередко применяются следующие методы атаки операционной системы:

– превышение полномочий (используя ошибки в программном обеспечении или в администрировании операционной системы, хакер получает полномочия, превышающие полномочия, предоставленные ему согласно действующей политике безопасности);

– запуск программы от имени пользователя, имеющего необходимые полномочия, или в качестве системной программы (драйвера, сервиса, демона и т. д.);

– подмена динамически загружаемой библиотеки, используемой системными программами, или изменение переменных среды, описывающих путь к таким библиотекам;

– модификация кода или данных подсистемы защиты самой операционной системы;

– отказ в обслуживании (целью этой атаки является частичный или полный вывод из строя операционной системы);

– захват ресурсов (хакерская программа производит захват всех имеющихся в операционной системе ресурсов, а затем входит в бесконечный цикл);

– бомбардировка запросами (хакерская программа постоянно направляет операционной системе запросы, реакция на которые требует привлечения значительных ресурсов компьютера);

– использование ошибок в программном обеспечении или администрировании.

Атаки на уровне сетевого программного обеспечения (СПО). СПО является наиболее уязвимым, потому что канал связи, по которому передаются сообщения, чаще всего не защищен, и всякий, кто может иметь доступ к этому каналу, соответственно, может перехватывать сообщения и отправлять свои собственные.

Поэтому на уровне СПО возможны следующие хакерские атаки:

– **прослушивание сегмента локальной сети** (в пределах одного и того же сегмента локальной сети любой подключенный к нему компьютер в состоянии принимать сообщения, адресованные другим компьютерам сегмента, а следовательно, если компьютер хакера подсоединен к некоторому сегменту локальной сети, то ему становится доступен весь информационный обмен между компьютерами этого сегмента);

– **перехват сообщений на маршрутизаторе** (если хакер имеет привилегированный доступ к сетевому маршрутизатору, то он получает возможность перехватывать все сообщения, проходящие через этот маршрутизатор, и хотя тотальный перехват невозможен из-за слишком большого объема, чрезвычайно привлекательным для хакера является выборочный перехват сообщений, содержащих пароли пользователей и их электронную почту);

– **создание ложного маршрутизатора** (путем отправки в сеть сообщений специального вида хакер добивается, чтобы его компьютер стал маршрутизатором сети, после чего получает доступ ко всем проходящим через него сообщениям);

– **навязывание сообщений** (отправляя в сеть сообщения с ложным обратным сетевым адресом, хакер переключает на свой компьютер уже установленные сетевые соединения и в результате получает права пользователей, чьи соединения обманным путем были переключены на компьютер хакера);

– **отказ в обслуживании** (хакер отправляет в сеть сообщения специального вида, после чего одна или несколько компьютерных систем, подключенных к сети, полностью или частично выходят из строя).

Поскольку хакерские атаки на уровне СПО спровоцированы открытостью сетевых соединений, разумно предположить, что для отражения этих атак необходимо максимально защитить каналы связи и тем самым затруднить обмен информацией по сети для тех, кто не является легальным пользователем. Ниже перечислены некоторые способы такой защиты:

– **максимальное ограничение размеров компьютерной сети** (чем больше сеть, тем труднее ее защитить);

– **изоляция сети от внешнего мира** (по возможности следует ограничивать физический доступ к компьютерной сети извне, чтобы уменьшить вероятность несанкционированного подключения хакера);

– **шифрование сетевых сообщений** (тем самым можно устранить угрозу перехвата сообщений, правда, за счет снижения производительности СПО и роста накладных расходов);

– **электронная цифровая подпись сетевых сообщений** (если все сообщения, передаваемые по компьютерной сети, снабжаются электронной цифровой подписью, и при этом неподписанные сообщения игнорируются, то можно забыть про угрозу навязывания сообщений и про большинство угроз, связанных с отказом в обслуживании);

– **использование брандмауэров** (брандмауэр является вспомогательным средством защиты, применяемым только в том случае, если компьютерную сеть нельзя изолировать от других сетей, поскольку брандмауэр довольно часто не способен отличить потенциально опасное сетевое сообщение от совершенно безвредного, и в результате типичной является ситуация, когда брандмауэр не только не защищает сеть от хакерских атак, но и даже препятствует ее нормальному функционированию.

Атаки на уровне систем управления базами данных. Защита СУБД является одной из самых простых задач. Это связано с тем, что СУБД имеют строго определенную внутреннюю структуру, и операции над элементами СУБД заданы довольно четко. Есть четыре основных действия – поиск, вставка, удаление и замена элемента. Другие операции являются вспомога-

тельными и применяются достаточно редко. Наличие строгой структуры и четко определенных операций упрощает решение задачи защиты СУБД. В большинстве случаев хакеры предпочитают взламывать защиту компьютерной системы на уровне операционной системы и получать доступ к файлам СУБД с помощью средств операционной системы. Однако в случае, если используется СУБД, не имеющая достаточно надежных защитных механизмов, или плохо протестированная версия СУБД, содержащая ошибки, или если при определении политики безопасности администратором СУБД были допущены ошибки, то становится вполне вероятным преодоление хакером защиты, реализуемой на уровне СУБД.

Кроме того, имеются два специфических сценария атаки на СУБД, для защиты от которых требуется применять специальные методы. В первом случае результаты арифметических операций над числовыми полями СУБД округляются в меньшую сторону, а разница суммируется в некоторой другой записи СУБД (как правило, эта запись содержит личный счет хакера в банке, а округляемые числовые поля относятся к счетам других клиентов банка). Во втором случае хакер получает доступ к полям записей СУБД, для которых доступной является только статистическая информация. Идея хакерской атаки на СУБД – так хитро сформулировать запрос, для которого собирается статистика, чтобы множество записей состояло только из одной записи.

Защита системы от взлома. Перечисленные выше методы хакерской атаки на компьютерную систему являются наиболее типичными и описаны в общей форме. Самые распространенные из этих методов будут рассмотрены ниже более подробно, поскольку их применение в конкретных случаях имеет свои особенности, которые требуют применения дополнительных защитных мер. А пока для обобщенной модели взлома компьютерных систем можно сформулировать универсальные правила, которых следует придерживаться, чтобы свести риск к минимуму.

- Не отставайте от хакеров: будьте всегда в курсе последних разработок из области компьютерной безопасности. Регулярно просматривайте материалы, размещаемые на хакерских серверах Internet (например. astalavista.box.sk).
- Руководствуйтесь принципом разумной достаточности: не стремитесь построить абсолютно надежную защиту. Ведь чем мощнее защита, тем больше ресурсов компьютерной системы она потребляет и тем труднее использовать ее.
- Храните в секрете информацию о принципах действия защитных механизмов компьютерной системы.
- Постарайтесь максимально ограничить размеры защищаемой компьютерной сети и без крайней необходимости не допускайте ее подключения к Internet.

• Перед тем как вложить денежные средства в покупку нового программного обеспечения, поищите информацию о нем, имеющуюся на хакерских серверах Internet.

• Размещайте серверы в охраняемых помещениях. Не подключайте к ним клавиатуру и дисплеи, чтобы доступ к этим серверам осуществлялся только через сеть.

• Абсолютно все сообщения, передаваемые по незащищенным каналам связи, должны шифроваться и снабжаться цифровой подписью.

• Если защищаемая компьютерная сеть имеет соединение с незащищенной сетью, то все сообщения, отправляемые в эту сеть или принимаемые из нее, должны проходить через брандмауэр, а также шифроваться и снабжаться цифровой подписью.

• Не пренебрегайте возможностями, которые предоставляет аудит. Интервал между сеансами просмотра журнала аудита не должен превышать одних суток.

• Если окажется, что количество событий, помещенных в журнал аудита, необычайно велико, то изучите внимательно все новые записи, поскольку не исключено, что компьютерная система подверглась атаке хакера, который пытается замести следы своего нападения, зафиксированные в журнале аудита.

• Регулярно производите проверку целостности программного обеспечения компьютерной системы. Проверяйте ее на наличие программных закладок.

• Регистрируйте все изменения политики безопасности в обычном бумажном журнале. Регулярно сверяйте политику безопасности с зарегистрированной в этом журнале. Это поможет обнаружить присутствие программной закладки, если она была внедрена хакером в компьютерную систему.

• Создайте несколько ловушек для хакеров (например, заведите на диске файл с заманчивым именем, прочитать который невозможно с помощью обычных средств, и если будет зафиксировано успешное обращение к этому файлу, значит, в защищаемую компьютерную систему была внедрена программная закладка).

• Регулярно тестируйте компьютерную систему с помощью специальных программ, предназначенных для определения степени ее защищенности от хакерских атак.

В целом различают следующие виды вредоносных хакерских атак:

1) программные закладки;
2) троянские программы;
3) отказ в обслуживании *DoS-атака*;
4) атака Man-in-the-Middle "человек посередине";
5) атаки на уровне приложений;
6) внедрение SQL-кода (инъекция);
7) вирусные атаки.

8.2.1. Программные закладки

Закладкой (или программной закладкой) в информационной безопасности называют скрытно внедренную в защищенную систему программу либо намеренно измененный фрагмент программы, которая позволяет злоумышленнику осуществить несанкционированный доступ к ресурсам системы на основе изменения свойств системы защиты.

Часто программные закладки выполняют роль перехватчиков паролей, трафика, а также служат в качестве проводников для компьютерных вирусов. Программные закладки невозможно обнаружить при помощи стандартных антивирусных средств, их выявление возможно только специальными тестовыми программами.

Классифицируют закладки по методу внедрения и по назначению.

По методу внедрения в компьютерную систему программные закладки делятся:

– на программно-аппаратные закладки, которые ассоциированы с аппаратными средствами, их средой обитания является BIOS;

– загрузочные закладки, которые ассоциированы с программами начальной загрузки, располагающимися в загрузочных секторах жесткого диска;

– драйверные закладки, которые ассоциированы с драйверами периферийных устройств персонального компьютера;

– прикладные закладки, которые ассоциированы с прикладным программным обеспечением;

– исполняемые закладки, которые ассоциированы с программными модулями, содержащими код программной закладки;

– закладки-имитаторы, имитирующие интерфейс служебных программ, исполнение которых предполагает ввод конфиденциальной информации;

– замаскированные закладки, маскирующиеся под программы, позволяющие оптимизировать работу персонального компьютера, компьютерные игры и прочие развлекательные программы.

По назначению закладки делятся:

– на закладки, осуществляющие копирование конфиденциальной информации;

– закладки, осуществляющие изменение алгоритмов функционирования системных, прикладных и служебных программ;

– закладки, осуществляющие изменение режимов работы программного обеспечения.

Для того чтобы программная закладка начала функционировать, необходимо соблюдение некоторых условий, заставляющих процессор исполнять команды, входящие в код программной закладки:

– программная закладка должна попасть в оперативную память;

– должен быть выполнен ряд активизирующих условий, зависящих от типа программной закладки.

По условиям нахождения в оперативной памяти компьютера программные закладки делятся:

– на резидентные закладки, постоянно находящиеся в оперативной памяти до перезагрузки или завершения работы компьютера;

– нерезидентные закладки, выгружающиеся из оперативной памяти по истечении определенного времени либо при выполнении определенных условий.

Защита от программных закладок осуществляется в следующих вариантах:

– защита от внедрения закладки в систему;

– выявление внедренной закладки;

– удаление внедренной закладки.

Защита от внедрения программных закладок в большинстве случаев осуществляется путем создания изолированного персонального компьютера, защищенного от проникновения программных закладок извне. Для того чтобы считаться изолированным, компьютер должен удовлетворять следующим условиям:

– BIOS не должен содержать программных закладок;

– установленная операционная система должна быть проверена на наличие программных закладок;

– должна быть установлена неизменность BIOS и операционной системы;

– на персональном компьютере не должны были запускаться и не запускаются программы, которые не прошли проверку на наличие в них программных закладок;

– должен быть исключен запуск проверенных программ вне персонального компьютера.

Выявление внедренных программных закладок осуществляется путем обнаружения признаков их присутствия в системе, которые делятся:

– на качественные и визуальные;

– обнаруживаемые средствами диагностики.

К качественным и визуальным относят признаки, которые могут быть идентифицированы пользователем во время работы с системой. Это могут быть как отклонения от привычной работы системы, так и изменения в пользовательских и системных файлах. Наличие данных признаков свидетельствует о необходимости проведения проверки на наличие программных закладок в системе.

Признаки, обнаруживаемые средствами диагностики, идентифицируются специальным тестовым программным обеспечением, сигнализирующим о наличии вредоносного программного кода в системе.

Метод удаления внедренных программных закладок зависит от метода их внедрения в систему. При обнаружении программно-аппаратной закладки необходимо перепрограммировать ПЗУ компьютера. При обнаружении загрузочной, драйверной, прикладной, замаскированной закладки или закладки-имитатора необходимо произвести их замену на соответствующее программное обеспечение от доверенных источников. При обнаружении исполняемой закладки следует убрать текст закладки из исходного текста программного модуля и откомпилировать модуль заново.

8.2.2. Троянские программы

Троянской программой (троянцем, или троянским конем) называется вредоносная программа, которая маскируется под безвредные или полезные программы, чтобы пользователь запустил их на своем компьютере, распространяемая злоумышленниками. Название «троянские» восходит к эпизоду в Илиаде, рассказывающем о «Троянском коне» – дарёном деревянном коне, использованном для проникновения в Трою, что и стало причиной падения Трои. В коне, подаренном в знак лже-перемирия, прятались воины Одиссея, ночью выбравшиеся из коня и открывшие ворота антитроянской армии.

«Трояны» – самый простой вид вредоносных программ, сложность которых зависит исключительно от сложности истинной задачи и средств маскировки. Самые примитивные «трояны» (например, стирающие содержимое диска при запуске) могут иметь исходный код в несколько строк. Таким образом, троянская программа – это особая разновидность программной закладки.

Большинство троянских программ предназначено для сбора конфиденциальной информации. Их задача, чаще всего, состоит в выполнении действий, позволяющих получить доступ к паролям, сведениям о банковских счетах и т. д. Остальные троянцы создаются для причинения прямого ущерба компьютерной системе, приводя ее в неработоспособное состояние.

К последним можно отнести, например, троянскую программу PC CYBORG, которая завлекала ничего не подозревающих пользователей обещаниями предоставить им новейшую информацию о борьбе с вирусом. Проникнув в компьютерную систему, PC CYBORG отсчитывала 90 перезагрузок этой системы, а затем прятала все каталоги на ее жестком диске и шифровала находящиеся там файлы.

Существует классификация, где троянские программы разбиваются на категории, основанные на том, как они внедряются в систему и наносят ей вред:

- удалённый доступ,
- уничтожение данных,

- загрузчик,
- сервер.
- дезактиватор программ безопасности.

Обнаружить такие троянские программы трудно. Троянские программы обнаруживаются и удаляются антивирусным программным обеспечением точно так же, как и остальные вредоносные программы.

Злоумышленник, решивший запустить в компьютер троянца, обычно пытается сделать его частью системного файла. Такие файлы входят в дистрибутив операционной системы и их присутствие на любом компьютере, где эта операционная система установлена, не вызывает никаких подозрений. Однако любой системный файл имеет вполне определенную длину. Если данный атрибут будет каким-либо образом изменен, то это встревожит пользователя. Зная это, злоумышленник постарается достать исходный текст соответствующей программы и проанализирует его на предмет присутствия в нем избыточных элементов, которые могут быть удалены безо всякого ощутимого ущерба. Тогда вместо найденных избыточных элементов он вставит в программу своего троянца и перекомпилирует ее заново. Если размер полученного двоичного файла окажется меньше или больше размера исходного, то процедура повторяется. И так до тех пор, пока не будет получен файл, размер которого в наибольшей степени близок к оригиналу.

Распознать троянскую программу можно по дате модификации файла или по изменению его атрибутов.

Однако и контрольную сумму в общем случае оказывается не так уж трудно подделать. Поэтому для проверки целостности файловой системы компьютера используется особая разновидность алгоритма вычисления контрольной суммы, называемая *односторонним хэшированием.*

Функция хэширования называется односторонней, если задача отыскания двух аргументов, для которых ее значения совпадают, является трудно решаемой. Отсюда следует, что функция одностороннего хэширования может быть применена для того, чтобы отслеживать изменения, вносимые злоумышленником в файловую систему компьютера, поскольку попытка злоумышленника изменить какой-либо файл так, чтобы значение, полученное путем одностороннего хэширования этого файла, осталось неизменным, обречена на неудачу.

8.2.3. Отказ в обслуживании (DoS-атака)

DoS (от англ. *Denialof Service* – отказ в обслуживании) – атака, имеющая своей целью заставить сервер не отвечать на запросы, нанести вред системе.

Разновидностью такой атаки является DDoS-атака (от англ. *Distributed Denialof Service* – распределенная DoS), имеющая ту же цель, что и DoS, но производимая не с одного компьютера, а с нескольких компьютеров в сети. Для этого несколько компьютеров объединяются, и каждый производит DoS атаку на систему жертвы. DDoS используется там, где обычный DoS неэффективен.

Впервые DDoS-атаки стали известны в 1996 г., но их массовое проявление возникло в 1999 г., когда вследствие проведения данного типа атаки «легли» серверы таких огромных корпораций, как Yahoo, CNN, Amazon, eBay. В 2000 г. атака на эти сервера повторилась, системные администраторы ничего этому не смогли противопоставить.

DDoS-атаки могут использоваться и как средство политического воздействия. В этих случаях атакуются, как правило, серверы государственных учреждений или правительственных организаций. Опасность такого рода атак состоит еще и в том, что они могут носить провокационный характер: кибератака серверов одной страны может осуществляться с серверов другой, а управляться с территории третьего государства. Так было с Прибалтикой, когда переносили памятник солдату. Государство подверглось кибератаке и всю вину свалили на Россию, хотя, как выяснилось, потом атаки были с Китая и других стран.

Denialof Service (DoS), без сомнения, является наиболее известной формой хакерских атак. Против атак такого типа труднее всего создать стопроцентную защиту. Для организации такой атаки требуется минимум знаний и умений. Но именно простота реализации и огромные масштабы причиняемого вреда привлекают к DoS пристальное внимание администраторов, отвечающих за сетевую безопасность.

Наиболее известные разновидности DoS атак:

- Floods (Mailbombing);
- SYN flooding;
- Flood ping (ICMP flooding);
- Boink (Bonk, Teardrop, new Tear/Tear2);
- Ping Of Death (Ssping, IceNuke, Jolt);
- Land.

Floods (Mailbombing). Перевод с английского на русский – "затопление". Во время floods атак происходит посылка большого количества на атакуемую систему ICMP (чаще всего) либо UDP пакетов, которые не несут полезной информации (мусор). В результате происходит уменьшение полосы пропускания канала и загрузка компьютерной системы анализом пришедших бесполезных пакетов и генерацией на них ответов.

Считается самым старым методом атак, хотя суть его проста и примитивна: большое количество почтовых сообщений делает невозможным

работу с почтовыми ящиками, а иногда и с целыми почтовыми серверами. Для этой цели было разработано множество программ, и даже неопытный пользователь мог совершить атаку, указав всего лишь e-mail жертвы, текст сообщения, и количество необходимых сообщений. Многие такие программы позволяли прятать реальный IP-адрес отправителя, используя для рассылки анонимный почтовый сервер. Эту атаку сложно предотвратить, так как даже почтовые фильтры провайдеров не могут определить реального отправителя спама.

Провайдер может ограничить количество писем от одного отправителя, но адрес отправителя и тема зачастую генерируются случайным образом.

SYN flooding. Затопление SYN-пакетами – самый известный способ "забить" информационный канал. Вспомним, как работает TCP/IP в случае входящих соединений. Система отвечает на пришедший C-SYN-пакет S-SYN/CACK-пакетом, переводит сессию в состояние SYN_RECEIVED и заносит ее в очередь. Если в течение заданного времени от клиента не придет S-ACK, то соединение удаляется из очереди, в противном случае соединение переводится в состояние ESTABLISHED. По RFC, когда очередь входных соединений уже заполнена, а система получает SYN-пакет, приглашающий к установке соединения, он будет молча проигнорирован. Затопление SYN-пакетами основано на переполнении очереди сервера, после чего сервер перестает отвечать на запросы пользователей. В различных системах работа с очередью реализована по-разному.

Атака обычно направлена на определённую, конкретную службу, например telnet или ftp. Она заключается в передаче пакетов установления соединения на порт, соответствующий атакуемой службе. При получении запроса система выделяет ресурсы для нового соединения, после чего пытается ответить на запрос (послать "SYN-ACK") по недоступному адресу. По умолчанию NT версий 3.5 - 4.0 будет пытаться повторить подтверждение 5 раз – через 3, 6, 12, 24 и 48 с. После этого еще 96 с система может ожидать ответ, и только после этого освободит ресурсы, выделенные для будущего соединения. Общее время занятости ресурсов – 189 с.

После истечения некоторого времени (зависит от реализации) система удаляет запросы из очереди. Однако ничего не мешает хакеру послать новую порцию запросов. Таким образом, даже находясь на соединении 2400 bps, хакер может посылать каждые полторы минуты по 20-30 пакетов на сервер, поддерживая его в нерабочем состоянии.

Floodping (ICMP flooding). Перевод с английского на русский – "поток пингов". Во время этой атаки происходит посылка компьютерной системе жертвы большого количества запросов эха ICMP (пинг системы). В результате происходит уменьшение полосы пропускания канала и загрузка компьютерной системы анализом пришедших пакетов и генерацией на них ответов.

Примечание: В мирных целях пинг используется администраторами и пользователями для проверки работоспособности основных частей транспортной системы вычислительной сети, чтобы оценить работу сети при максимальной нагрузке. Программа посылает ICMP-пакет типа ECHO REQUEST, выставляя в нем время и его идентификатор. Ядро машины-получателя отвечает на подобный запрос пакетом ICMP ECHOREPLY. Получив его, ping выдает скорость прохождения пакета. При стандартном режиме работы пакеты высылаются через некоторые промежутки времени, практически не нагружая сеть.

Boink (Bonk, Teardrop, new Tear/Tear2). При передаче пакета данных протокола IP по сети может осуществляться деление этого пакета на несколько фрагментов. Впоследствии, при достижении адресата, пакет восстанавливается из этих фрагментов. Хакер может инициировать посылку большого числа фрагментов, что приводит к переполнению программных буферов на приемной стороне и, в ряде случаев, к аварийному завершению системы.

Количество реализаций этой атаки достаточно велико. На компьютер жертвы передается несколько фрагментированных IP пакетов, которые при сборке образуют один пакет размером более 64 КБ (максимальный размер IP пакета равен 64 КБ минус длина заголовка).

Данная атака была эффективна против компьютеров с ОС Windows. При получении такого пакета Windows NT, не имеющая специального патча icmp-fix, "зависает" или аварийно завершается. Другие варианты подобных атак используют неправильные смещения в IP фрагментах, что приводит к некорректному выделению памяти, переполнению буферов и в конечном итоге к сбоям в работе систем.

Ping Of Death (Ssping, IceNuke, Jolt). Сущность атаки в следующем: на машину жертвы посылается сильно фрагментированный ICMP пакет большого размера (64 КБ). Реакцией Windows-систем на получение такого пакета является безоговорочное повисание, включая мышь и клавиатуру.

Программа для атаки широко доступна в сети в виде исходника на C и в виде запускаемых файлов для некоторых версий Unix.

Жертвой такой атаки могут стать не только Windows машины, атаке подвержены Mac OS и некоторые версии Unix.

Преимущества такого способа атаки в том, что обычно firewall пропускает ICMP пакеты, а если firewall и настроен на фильтрацию адресов посылателей, то, используя нехитрые приемы spoofing, можно обмануть и такой firewall.

Недостаток PingOfDeath в том, что для одной атаки надо переслать более 64 КБ по сети, что делает вообще его говоря малоприменимым для широкомасштабных диверсий.

Land. Эта атака использует уязвимости реализаций стека TCP/IP в некоторых ОС. Она заключается в передаче на открытый порт компьютера-жертвы TCP-пакета с установленным флагом SYN, причем исходный

адрес и порт такого пакета соответственно равны адресу и порту атакуемого компьютера. Это приводит к тому, что компьютер-жертва пытается установить соединение сам с собой, в результате чего сильно возрастает загрузка процессора и может произойти "подвисание" или перезагрузка. Данная атака весьма эффективна на некоторых моделях маршрутизаторов фирмы CiscoSystems, причем успешное применение атаки к маршрутизатору может вывести из строя всю сеть организации.

Угроза атак типа DoS может быть снижена тремя способами:

1) Функции антиспуфинга. Правильная конфигурация функций антиспуфинга на маршрутизаторах и межсетевых экранах поможет снизить риск DoS. Эти функции как минимум должны включать фильтрацию RFC 2827. Если хакер не сможет замаскировать свою истинную личность, он вряд ли решится провести атаку.

2) Функции анти-DoS. Правильная конфигурация функций анти-DoS на маршрутизаторах и межсетевых экранах способна ограничить эффективность атак. Эти функции часто ограничивают число полуоткрытых каналов в любой момент времени.

3) Ограничение объема трафика (traffic rate limiting). Организация может попросить провайдера (ISP) ограничить объем трафика. Этот тип фильтрации позволяет ограничить объем некритического трафика, проходящего по вашей сети. Типичным примером является ограничение объемов трафика ICMP, который используется только для диагностических целей. Атаки (D)DoS часто используют ICMP.

8.2.4. Атака Man-in-the-Middle "человек посередине"

Атака Man-in-the-Middle "человек посередине" – вид атаки, когда злоумышленник перехватывает канал связи между двумя системами и получает доступ ко всей передаваемой информации. При получении доступа на таком уровне злоумышленник может модифицировать информацию нужным ему образом, чтобы достичь своих целей. Цель атаки man-in-the-middle (MITM) – кража или фальсифицирование передаваемой информации, или же получение доступа к ресурсам сети путём перехвата сообщения, передающегося между двумя системами. Такие атаки крайне сложно отследить, так как обычно злоумышленник находится внутри организации. Например, в стандартной HTTP-транзакции клиент и сервер общаются с помощью TCP-соединения. Используя различные методы, злоумышленник может разбить оригинальное TCP-соединение на два новых, одно между собой и клиентом, другое между собой и сервером.

После перехвата TCP-соединения, злоумышленник действует как прокси, при этом он может читать данные и даже изменять их. Это вполне реально. Довольно редко соединения между сервером и клиентом будут

прямыми, чаще всего они связаны через большое количество промежуточных серверов. На любом из этих серверов могут быть развернуты средства для перехвата трафика.

Атака MITM является довольно эффективной из-за природы HTTP-протокола и передаваемых данных, основанных на ASCII. Например, применяя man-in-the-middleattack, можно перехватить куки сессии пользователя, а также изменить структуру HTTP-заголовка.

Достаточно эффективная защита от этой атаки – шифрование передаваемого трафика. HTTPS – это обычный протокол HTTP, который поддерживает шифрование. Он может защитить передачу данных в виде обычного текста. HTTPS использует SSL или TLS для шифрования запросов и ответов веб-сервера, делая их непроницаемыми для сниферов и атак "человек посередине".

Однако, даже HTTPS-соединение не панацея. Атака "человек посередине" может быть осуществлена при использовании HTTPS-соединения. С единственной разницей в том, что нужно будет создать две независимых SSL-сессии, по одной на каждое TCP-соединение. Браузер устанавливает SSL-соединение с атакующим и он, в свою очередь, устанавливает такое же соединение с сервером. В таких случаях браузер обычно предупреждает пользователя о том, что используется невалидный цифровой сертификат, но рядовой юзер с легкостью игнорирует эти предупреждения, толком не осознавая, что делает. Хотя в некоторых случаях предупреждение может и не последовать, если, например, сертификат сервера скомпрометирован злоумышленником, или когда он сам имеет сертификат, подписанный доверенным центром сертификации.

Данный метод сложный, однако, хакер, вооруженный необходимым оборудованием и программным обеспечением, вполне может провести подобную атаку даже при зашифрованном соединении.

8.2.5. Атаки на уровне приложений

Атаки на уровне приложений могут проводиться несколькими способами. Самый распространенный из них – использование хорошо известных слабостей серверного программного обеспечения (sendmail, HTTP, FTP). Используя эти слабости, хакеры могут получить доступ к компьютеру от имени пользователя, работающего с приложением (обычно это бывает не простой пользователь, а привилегированный администратор с правами системного доступа). Сведения об атаках на уровне приложений широко публикуются, чтобы дать администраторам возможность исправить проблему с помощью коррекционных модулей (патчей). К сожалению, многие хакеры также имеют доступ к этим сведениям, что позволяет им совершенствоваться.

Главная проблема при атаках на уровне приложений заключается в том, что хакеры часто пользуются портами, которым разрешен проход через межсетевой экран. К примеру, хакер, эксплуатирующий известную слабость Web-сервера, часто использует в ходе атаки TCP порт 80. Поскольку web-сервер предоставляет пользователям Web-страницы, то межсетевой экран должен обеспечивать доступ к этому порту. С точки зрения межсетевого экрана атака рассматривается как стандартный трафик для порта 80.

Полностью исключить атаки на уровне приложений невозможно. Хакеры постоянно открывают и публикуют в Интернете новые уязвимые места прикладных программ. Самое главное здесь – хорошее системное администрирование.

Вот некоторые меры, которые можно предпринять, чтобы снизить уязвимость для атак этого типа:

• читайте лог-файлы операционных систем и сетевые лог-файлы и/или анализируйте их с помощью специальных аналитических приложений;

• подпишитесь на услуги по рассылке данных о слабых местах прикладных программ: Bugtrad (http://www.securityfocus.com) и CERT.

8.2.6. Внедрение SQL-кода (инъекция)

SQL-инъекция – атака, в ходе которой изменяются параметры SQL-запросов к базе данных. В результате запрос приобретает совершенно иной смысл, и в случае недостаточной фильтрации входных данных способен не только произвести вывод конфиденциальной информации, но и изменить/удалить данные. Очень часто такой вид атаки можно наблюдать на примере сайтов, которые используют параметры командной строки (в данном случае – переменные URL) для построения SQL-запросов к базам данных без соответствующей проверки.

PHP-инъекция – один из способов взлома веб-сайтов, работающих на PHP. Он заключается в том, чтобы внедрить специально сформированный злонамеренный сценарий в код веб-приложения на серверной стороне сайта, что приводит к выполнению произвольных команд. Известно, что во многих распространённых в интернете бесплатных движках и форумах, работающих на PHP (чаще всего это устаревшие версии), есть непродуманные модули или отдельные конструкции с уязвимостями. Крэкеры анализируют такие уязвимости, как неэкранированные переменные, получающие внешние значения.

8.2.7. IP-спуфинг

IP-спуфинг – тоже распространённый вид атаки в недостаточно защищённых сетях, когда злоумышленник выдаёт себя за санкционированного пользователя, находясь в самой организации или за её пределами. Для

этого крэкеру необходимо воспользоваться IP-адресом, разрешённым в системе безопасности сети. Такая атака возможна, если система безопасности позволяет идентификацию пользователя только по IP-адресу и не требует дополнительных подтверждений. Это можно сделать двумя способами: хакер может воспользоваться или IP-адресом, находящимся в пределах диапазона санкционированных IP-адресов, или авторизованным внешним адресом, которому разрешается доступ к определенным сетевым ресурсам. Атаки IP-спуфинга часто являются отправной точкой для прочих атак. Классический пример – атака DoS, которая начинается с чужого адреса, скрывающего истинную личность хакера.

Как правило, IP-спуфинг ограничивается вставкой ложной информации или вредоносных команд в обычный поток данных, передаваемых между клиентским и серверным приложением или по каналу связи между одноранговыми устройствами. Для двусторонней связи хакер должен изменить все таблицы маршрутизации, чтобы направить трафик на ложный IP-адрес. Некоторые хакеры, однако, даже не пытаются получить ответ от приложений – если главная задача заключается в получении от системы важного файла, то ответы приложений не имеют значения.

Если же хакеру удается поменять таблицы маршрутизации и направить трафик на ложный IP-адрес, то он получит все пакеты и сможет отвечать на них так, как будто является санкционированным пользователем.

Угрозу спуфинга можно ослабить (но не устранить) с помощью перечисленных ниже мер.

1) Контроль доступа. Самый простой способ предотвращения IP-спуфинга состоит в правильной настройке управления доступом. Чтобы снизить эффективность IP-спуфинга, настройте контроль доступа на отсечение любого трафика, поступающего из внешней сети с исходным адресом, который должен располагаться внутри вашей сети. Правда, это помогает бороться с IP-спуфингом, когда санкционированными являются только внутренние адреса; если же санкционированными являются и некоторые адреса внешней сети, то данный метод становится неэффективным.

2) Фильтрация RFC 2827. Вы можете пресечь попытки спуфинга чужих сетей пользователями вашей сети (и стать добропорядочным сетевым гражданином). Для этого необходимо отбраковывать любой исходящий трафик, исходный адрес которого не является одним из IP-адресов вашей организации. Данный тип фильтрации, известный под названием RFC 2827, может выполнять и ваш провайдер (ISP). В результате отбраковывается весь трафик, который не имеет исходного адреса, ожидаемого на определенном интерфейсе. К примеру, если ISP предоставляет соединение с IP-адресом 15.1.1.0/24, то он может настроить фильтр таким образом, чтобы с данного интерфейса на маршрутизатор ISP допускался только трафик, поступающий с адреса 15.1.1.0/24. Отметим, что до тех пор, пока

все провайдеры не внедрят этот тип фильтрации, его эффективность будет намного ниже возможной. Кроме того, чем дальше от фильтруемых устройств, тем труднее проводить точную фильтрацию. Например, фильтрация RFC 2827 на уровне маршрутизатора доступа требует пропуска всего трафика с главного сетевого адреса (10.0.0.0/8), тогда как на уровне распределения (в данной архитектуре) можно ограничить трафик более точно (адрес – 10.1.5.0/24).

Наиболее эффективный метод борьбы с IP-спуфингом – тот же, что и в случае со сниффингом пакетов: необходимо сделать атаку абсолютно неэффективной. IP-спуфинг может функционировать только при условии, что аутентификация происходит на базе IP-адресов, поэтому внедрение дополнительных методов аутентификации делает подобные атаки бесполезными. Лучшим видом дополнительной аутентификации является криптографическая. Если она невозможна, то хорошие результаты может дать двухфакторная аутентификация с использованием одноразовых паролей.

8.2.8. Злоупотребление доверием

Злоупотребление доверием представляет собой злонамеренное использование отношений доверия, существующих в сети. Классическим примером такого злоупотребления является ситуация в периферийной части корпоративной сети. В этом сегменте часто располагаются серверы DNS, SMTP и HTTP. Поскольку все они принадлежат к одному и тому же сегменту, взлом любого из них приводит к взлому всех остальных, так как эти серверы доверяют другим системам своей сети.

Другим примером является установленная с внешней стороны межсетевого экрана система, имеющая отношения доверия с системой, установленной с его внутренней стороны. В случае взлома внешней системы хакер может использовать отношения доверия для проникновения в систему, защищенную межсетевым экраном.

Риск злоупотребления доверием можно снизить за счет более жесткого контроля уровней доверия в пределах своей сети. Системы, расположенные с внешней стороны межсетевого экрана, ни при каких условиях не должны пользоваться абсолютным доверием со стороны защищенных экраном систем. Отношения доверия должны ограничиваться определенными протоколами и, по возможности, аутентифицироваться не только по IP-адресам, но и по другим параметрам.

8.2.9. Переадресация портов

Переадресация портов представляет собой разновидность злоупотребления доверием, когда взломанный хост используется для передачи через межсетевой экран трафика, который в противном случае был бы обязательно отбракован. Представим себе межсетевой экран с тремя интерфейсами, к каждому из которых подключен определенный хост. Внешний хост может подключаться к хосту общего доступа (DMZ), но не к тому, что установлен с внутренней стороны межсетевого экрана. Хост общего доступа может подключаться и к внутреннему, и к внешнему хосту. Если хакер захватит хост общего доступа, то он сможет установить на нем программное средство, перенаправляющее трафик с внешнего хоста прямо на внутренний. Хотя при этом не нарушается ни одно правило, действующее на экране, внешний хост в результате переадресации получает прямой доступ к защищенному хосту. Примером приложения, которое может предоставить такой доступ, является netcat. Более подробную информацию можно получить на сайте http://www.avian.org.

8.2.10. Использование ботнетов

Робот, он же бот (*bot*, англ.) – специальная программа для автоматизации рутинных задач, чаще всего используется в Интернете.

Ботнет (botnet, англ) – это сеть компьютеров, зараженных вредоносной программой поведения Backdoor. Backdoor’ы позволяют киберпреступникам удаленно управлять зараженными машинами (каждой в отдельности, частью компьютеров, входящих в сеть, или всей сетью целиком).

Ботнеты обладают мощными вычислительными ресурсами, являются грозным кибероружием и хорошим способом зарабатывания денег для злоумышленников. При этом зараженными машинами, входящими в сеть, хозяин ботнета может управлять откуда угодно: из другого города, страны или даже с другого континента, а организация Интернета позволяет делать это анонимно.

Изначально созданные как троянские программы, бэкдоры работали без разрешения или уведомления пользователя. Для управления зараженным компьютером злоумышленник должен был сам установить соединение с каждой инфицированной машиной. Первые бэкдоры работали в локальных сетях.

В самой идее ботнетов нет ничего ни нового, ни криминального, поскольку по большому счету ботнетом можно называть любую распределённую систему вычислений. Но вот когда с конца 1990-х гг. криминальные хакеры начали всё активнее использовать средства скрытного дистанционного управления машинами, работающие через «черные ходы», обес-

печиваемые троянцами и руткитами, ботнеты сетевых преступников стали большущей занозой. Особенно для банков и прочих платежно-финансовых сервисов в онлайне, коль скоро главная цель ботнетов – похищение информации о кредитных картах и других банковских реквизитах, требующихся для доступа к деньгам на счетах. В неменьшей степени страдают от краж и другие учреждения, оперирующие персональной информацией граждан, а также, разумеется, и миллионы людей, чьи данные похищаются в преступных целях.

Особую остроту этой проблеме придает то, что современный программный инструментарий для сборки и использования шпионского ботнета совсем не сложен в освоении и доступен злоумышленникам даже с минимальными компьютерными навыками. На подпольных онлайновых рынках такие инструментальные пакеты продаются по цене от нескольких сот до нескольких тысяч долларов, а самые жадные и целеустремленные искатели могут раздобыть их вообще бесплатно.

О появлении IRC-ботнетов стало известно довольно быстро. Как только о них появились публикации в хакерских журналах, появились и «угонщики» ботнетов – люди, которые обладали, возможно, теми же знаниями, что и владельцы ботнетов, но охотились за более легкой наживой. Они искали такие IRC-каналы, где было подозрительно много посетителей, заходили на них, изучали и «угоняли» ботнет: перехватывали управление сетью, перенаправляли боты на другие, защищенные паролем, IRC-каналы и в результате получали полный единоличный контроль над «чужой» сетью зараженных машин.

Следующим этапом развития ботнетов стало перемещение центров управления во всемирную паутину. Сначала хакеры разработали средства удаленного управления сервером, которые были основаны на скрипт – движках Perl и PHP, ASP, JSP и некоторых других.

Затем кто-то создал такое соединение компьютера в локальной сети с сервером в Интернете, которое позволяло откуда угодно управлять компьютером. Схема удаленного управления компьютером в локальной сети в обход таких средств защиты, как прокси и NAT, была опубликована в Интернете и быстро стала популярной в определенных кругах.

Полулегальные разработки средств удаленного управления, направленные на получение в обход защиты удаленного доступа к машинам в локальных сетях, дали толчок к созданию веб-ориентированных ботнетов.

Веб-ориентированные ботнеты оказались чрезвычайно удобным решением, которое популярно и сегодня. Множеством компьютеров можно управлять с любого устройства, имеющего доступ в Интернет, в том числе с мобильного телефона, а с веб-интерфейсом способен справиться даже школьник.

Управление компьютером, который заражен ботом, может быть прямым и опосредованным.

В случае прямого управления злоумышленник может установить связь с инфицированным компьютером и управлять им, используя встроенные в тело программы-бота команды.

В случае опосредованного управления бот сам соединяется с центром управления или другими машинами в сети, посылает запрос и выполняет полученную команду.

В любом случае хозяин зараженной машины, как правило, даже не подозревает о том, что она используется злоумышленниками, поэтому зараженные вредоносной программой-ботом компьютеры называют еще зомби-компьютерами, а сеть, в которую они входят, – зомби-сетью.

Ботнеты могут использоваться злоумышленниками для решения криминальных задач разного масштаба.

Рассылка спама. Это наиболее распространенный и один из самых простых вариантов эксплуатации ботнетов. По экспертным оценкам, в настоящее время более 80 % спама рассылается с зомби-машин. Спам с ботнетов не обязательно рассылается владельцами сети. За определенную плату спамеры могут взять ботнет в аренду.

Многотысячные ботнеты позволяют спамерам осуществлять с зараженных машин миллионные рассылки в течение короткого времени. Кроме обеспечения скорости и масштабности рассылок, ботнеты решают еще одну проблему спамеров. Адреса, с которых активно рассылается спам, зачастую попадают в черные списки почтовых серверов, и письма, приходящие с них, блокируются или автоматически помечаются как спам. Рассылка спама с сотен тысяч зомби-машин позволяет не использовать для рассылки одни и те же адреса.

Сбор адресов электронной почты на зараженных машинах – еще одна возможность использования ботнетов. Украденные адреса продаются спамерам либо используются при рассылке спама самими хозяевами ботнета. При этом растущий ботнет позволяет получать новые и новые адреса.

8.2.11. Социальная инженерия

Социальная инженерия (от англ. *Social Engineering*) – использование некомпетентности, непрофессионализма или небрежности персонала для получения доступа к информации. Социальная инженерия – это не технический, а психологический приём. Пользуясь данными, полученными при инвентаризации, взломщик может позвонить какому-либо пользователю (например, корпоративной сети) от имени администратора и попытаться узнать у него, например, пароль. Это становится возможным, когда в больших сетях, пользователи не знают всех работников, и тем более не

всегда могут точно узнать их по телефону. Кроме этого, используются сложные психологические приёмы, поэтому шанс на успех сильно возрастает. Этот метод обычно применяется без компьютера, с использованием обычного телефона, почтовой переписки либо кружечки пива. В ходе такой атаки злоумышленник устанавливает контакт с жертвой, и, вводя её в заблуждение либо войдя в доверие, пытается получить необходимые сведения, которые сложно получить другим путём, либо другие пути являются более рискованными. Как гласит старая поговорка, «*Самое слабое звено системы безопасности – Человек*».

9. ВИРУСНЫЕ АТАКИ И ИХ НЕЙТРАЛИЗАЦИЯ

Вирусные атаки осуществляются с помощью компьютерных вирусов (КВ). Компьютерными вирусами называются саморазмножающиеся программы, созданные для разрушения логической структуры ПК, уничтожения его программного обеспечения, создания помех или полной блокировки работы ПК, а также для несанкционированного съёма (воровства) информации.

Основными путями проникновения вирусов в ПК являются съемные диски, переносные жесткие диски, которые используются для переноса большого объема с ПК на другой лазерный диск и компьютерные сети.

Если вирус попал в ПК, то важно быстро его обнаружить (принцип медицины – чем раньше болезнь выявлена, тем легче лечить).

Наиболее ярко выраженные признаки наличия вируса следующие:

- частое зависание и сбои в работе ПК, до этого хорошо работавшего;
- неправильная работа хорошо работавших ранее программ;
- искажение содержание файлов или их исчезновение;
- изменение размеров файлов;
- вывод на экран непонятных изображений, сообщений;
- появление странных звуковых сигналов;
- уменьшение размера свободного места в оперативной памяти;
- невозможность загрузки оперативной системы.

9.1. Классификация вирусов и стратегия их распространения

Для того чтобы понять стратегию распространения, необходимо знать алгоритм их действия.

Различают вирусы по следующим признакам.

– по среде обитания (сетевые, файловые, загрузочные, файлово-загрузочные);

– способу заражения среды обитания (резидентные, нерезидентные);

– особенностям алгоритма (паразитические, почтовые вирусы – репликаторы или черви, невидимки или стелс-вирусы, мутанты, троянские, полиморфные);

– опасности воздействия (не опасные, опасные, очень опасные).

Кроме того, различают также:

– макрокомандные вирусы;
– вирусы в пакетных файлах ОС;
– вирусы в драйверах ОС;
– бестелесные вирусы;
– вирусы для пиринговых (файлообменных) сетей;
– комбинированные вирусы.

Сетевыми вирусами – называются вирусы, распространяющиеся по компьютерным сетям и попадающие на ПК по сети.

Файловые вирусы – это вирусы, записывающие свой код в тело программного файла или офисного документа. Эти вирусы заражают исполнительные файлы с расширением COM, EXE, а также вспомогательные программные файлы, загружаемые при выполнении других программ. Попав в другие типы файлов они не получают управления и теряют способности к размножению.

Заражая файл, вирус записывает свой код внутрь выполняемого файла и изменяет его таким образом, чтобы после запуска файла код вируса получил управление (рис. 14).

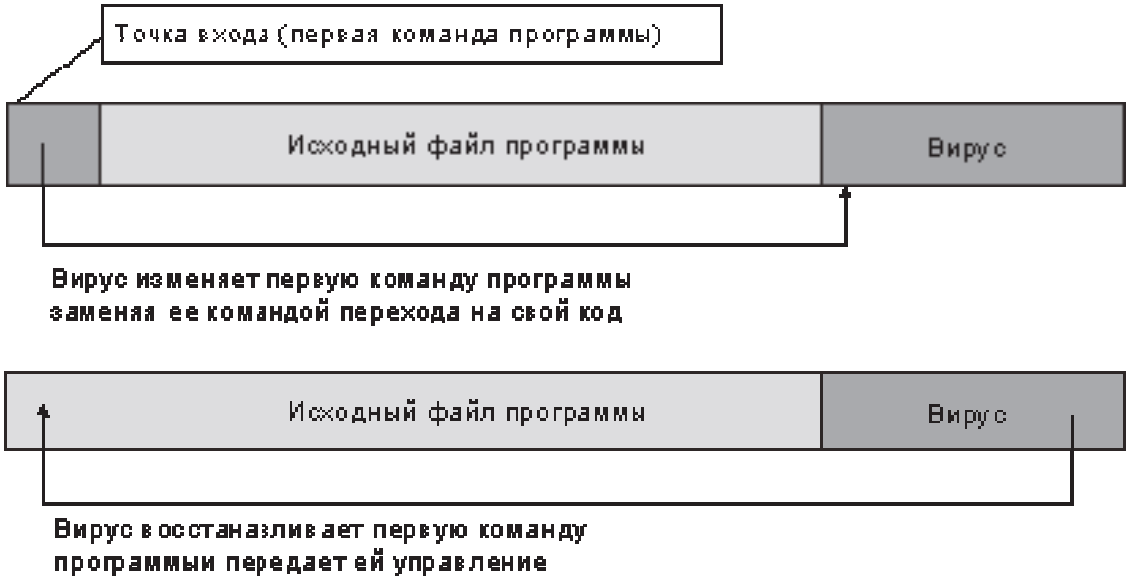


Рис. 14. Внедрение вируса в файл

Вирус может поместить свой код или несколько фрагментов своего кода в разных местах зараженной программы. После внедрения в файл вирус выполняет другие вредоносные действия: заражает другие файлы, устанавливает в памяти собственные резидентные модули и пр. Затем вирус, как правило, передает управление зараженной программе и далее она исполняется как обычно.

В качестве примера показаны на рис. 15 исходное содержимое программного файла mouse.com, а на рис. 16 – содержимое того же файла, но зараженного очень известным в прошлом опасным вирусом OneHalf.

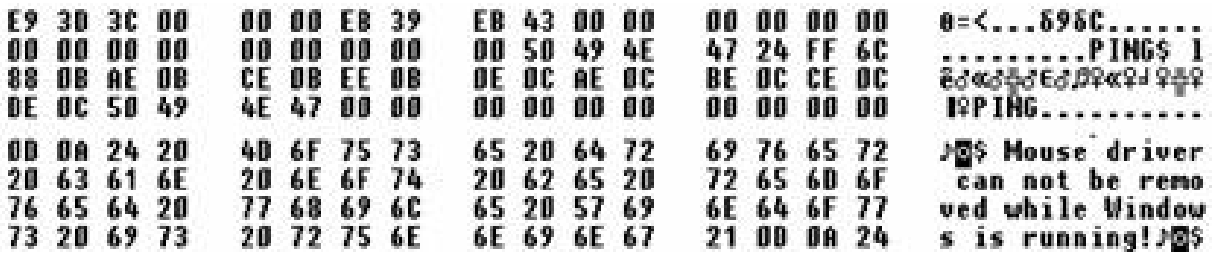


Рис. 15. Содержимое программного файла mouse.com

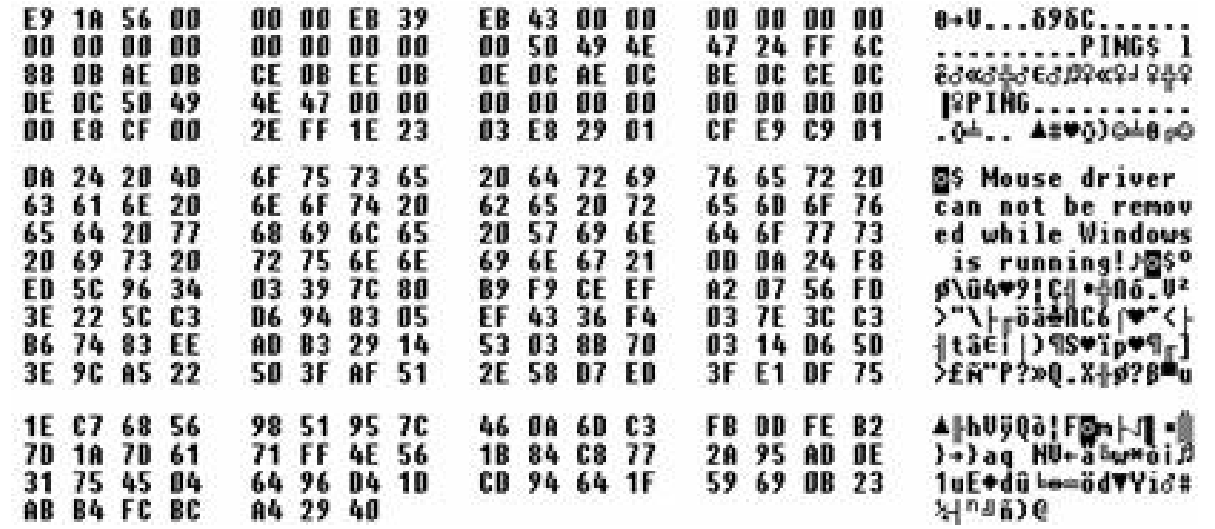


Рис. 16. Вирус OneHalf в файле mouse.com

Во время запуска программы (или загрузке офисного документа для редактирования) вирус получает управление. Получив управление, файловый вирус может записать свое тело в другие файлы, хранящиеся на диске компьютера.

Существует потенциальная возможность распространения компьютерных вирусов и с файлами графических изображений, если эти файлы содержат программный код.

Загрузочными вирусами называются вирусы, которые внедряются в загрузочный сектор диска (BOOT диска) или в начальный сектор жестких дисков. Процесс загрузки операционной системы (ОС) с диска или дискеты производится в несколько шагов. На первом шаге программа загрузки считывает содержимое специальных областей диска, называемых *загрузочными записями*. Загрузочные записи обычно расположены в самом начале диска (или дискеты) и содержат программный код, необходимый для выполнения следующих шагов загрузки ОС. Главная загрузочная запись, находящаяся на жестком диске, называется Master Boot Record (MBR). Аналогичная запись на дискете носит название Boot Record (BR). И вирус записывает свой код в главную загрузочную запись Master Boot Record диска или загрузочную запись Boot Record диска и дискет, активизируясь после загрузки компьютера и получая управление до программы загрузки ОС, в результате чего процедура управления выполняется под контролем вируса.

Эти вирусы всегда бывают резидентными и заражают вставляемые дискеты или компакт диски. При этом дискета может быть и не загрузочной, не системной, т. к. на любой дискете есть в наличии сектор загрузчик ОС. Но на системной дискете он находит файлы ОС, загружает их и передаёт им управление, а на несистемной – не находит. Поэтому если в дисководе А осталась заражённая дискета, то в момент загрузки вирус заразит жёсткий диск.

Файлово-загрузочные вирусы заражают как загрузочные сектора, так и файлы. Встречаются также вирусы командных файлов, которые формируют с помощью командных файлов исполнимый файл на диске, запускают его, он выполняет размножение вируса и вредящие действия. После чего этот файл стирается. Эти вирусы начинают свою работу при выполнении командного файла.

Резидентные компьютерные вирусы оставляют при заражении в оперативной памяти свою резидентную часть, которая потом перехватывает обращения ОС к объектам заражения (файлам, загрузочным секторам дисков и т.д.) и внедряется в них. Эти вирусы являются активными до выключения ПК или перегрузки. Не резидентные вирусы не заражают памяти ПК.

Паразитические вирусы изменяют содержание файлов диска и могут быть достаточно легко обнаружены и уничтожены.

Вирусы-репликаторы (иногда называют червями) или почтовые вирусы распространяются по компьютерным сетям, вычисляют адреса сетевых ПК и записывают по этим адресам свои копии. Заражение почтовым вирусом происходит в результате действий пользователей, просматривающих почту, а также из-за ошибок в почтовых программах и операционных системах. Известно, что вместе с электронным сообщением можно передать любые файлы. Такие файлы называются присоединенными или фай-

лами вложений (attachmentfile). Именно через них на компьютер может проникнуть вирус, червь, троянская или другая вредоносная программа. Кроме того, сообщение электронной почты может передаваться в виде документов HTML, которые обычно служат основой для создания Web-сайтов Интернета. Сообщение может содержать ссылку на вредоносный компонент, размещенный где-либо в Интернете, а также вредоносный программный код, активизирующийся при просмотре сообщения.

Попав на компьютер пользователя, почтовый вирус может разослать свой код по адресам, извлеченным из книги электронных адресов почтовой программы, установленной на компьютере. Это позволяет почтовому вирусу быстро распространяться по Интернету.

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

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

– прямое подключение к SMTP-серверу, используя встроенную в код червя почтовую библиотеку;

– использование сервисов MS Outlook;

– использование функций Windows MAPI.

Почтовые черви для поиска почтовых адресов используют следующие методы:

– рассылают себя по всем адресам, обнаруженным в адресной книге MS Outlook;

– считывают адреса из адресной базы WAB;

– сканируют «подходящие» файлы на диске и выделяют в них строки, являющиеся адресами электронной почты;

– отсылают себя по всем адресам, обнаруженным в письмах в почтовом ящике (при этом некоторые почтовые черви «отвечают» на обнаруженные в ящике письма).

Многие черви используют сразу несколько из перечисленных методов. Встречаются и другие способы поиска адресов электронной почты. Существуют также прочие способы заражения удаленных компьютеров, например:

– копирование червя на сетевые ресурсы;

– проникновение червя на компьютер через уязвимости в операционных системах и приложениях;

– проникновение в сетевые ресурсы публичного использования;

– паразитирование на других вредоносных программах.

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

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

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

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

Современные антивирусы нейтрализуют почтовые вирусы непосредственно на почтовых серверах, а также на рабочих станциях (персональных компьютерах) до того, как сообщения попадут в почтовую программу.

Вирус-невидимка (стелс-вирус) – это вирус, оставляющий в памяти компьютера модули, перехватывающие обращение программ к дискам. Стелс-вирус перехватывает обращения операционной системы к пораженным файлам и подставляет вместо своего тела незараженные участки диска, почему их очень трудно обезвредить. Такие вирусы умеют «прятаться» от антивирусных программ. С этой целью вирусы перехватывают вызовы некоторых функций ОС. Благодаря такому перехвату антивирус, читая зараженный файл или загрузочную запись, фактически получает незараженные данные, тем самым вводится в заблуждение.

Вирусы-мутанты, или шифрующиеся вирусы, содержат алгоритм шифровки-расшифровки цепочек байтов тела своей программы, благодаря которым копии одного и того же вируса не имеют ни одной повторяющейся цепочки байтов. Вирус при заражении новых файлов и системных областей диска шифрует собственный код, пользуясь для этого случайными паролями (ключами). Когда вирус получает управление, он расшифровывает свой собственный код и передает ему управление. Очень опасны.

Современные антивирусы умеют расшифровывать код вируса, поэтому шифрующиеся вирусы могут быть эффективно обнаружены и уничтожены.

Троянские – маскируются под программу и разрушают файловую структуру дисков. Троянские программы различаются между собой по тем действиям, которые они производят на зараженном компьютере. Например, следующие.

Backdoor – троянские утилиты удаленного администрирования. Троянские программы этого класса являются утилитами удаленного администрирования компьютеров в сети. По своей функциональности они во многом напоминают различные системы администрирования, разрабатываемые и распространяемые фирмами-производителями программных продуктов. При запуске «троянец» устанавливает себя в системе и затем следит за ней, при этом пользователю не выдается никаких сообщений о действиях троянца в системе. Более того, ссылка на «троянца» может отсутствовать в списке активных приложений. «Пользователь» этой троянской программы может и не знать о ее присутствии в системе, в то время как его компьютер открыт для удаленного управления. В результате эти троянцы могут быть использованы для обнаружения и передачи конфиденциальной информации, для запуска вирусов, уничтожения данных и т. п. Троянские программы данного типа являются одним из самых опасных видов вредоносного программного обеспечения, поскольку в них заложена возможность самых разнообразных злоумышленных действий, присущих другим видам троянских программ.

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

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

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

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

Trojan-Clicker – интернет-кликеры. Семейство троянских программ, основная функция которых – организация несанкционированных обращений к интернет-ресурсам (обычно к веб-страницам). Достигается это либо посылкой соответствующих команд браузеру, либо заменой системных файлов, в которых указаны «стандартные» адреса интернет-ресурсов (например, файл hosts в MS Windows). У злоумышленника могут быть следующие цели для подобных действий:

– увеличение посещаемости каких-либо сайтов с целью увеличения показов рекламы;

– организация DoS-атаки (Denialof Service) на какой-либо сервер;

– привлечение потенциальных жертв для заражения вирусами или троянскими программами.

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

Trojan-Proxy – троянские прокси-сервера. Семейство троянских программ, скрытно осуществляющих анонимный доступ к различным интернет-ресурсам. Обычно используются для рассылки спама.

Trojan-Spy – шпионские программы. Данные троянцы осуществляют электронный шпионаж за пользователем зараженного компьютера: вводимая с клавиатуры информация, снимки экрана, список активных приложений и действия пользователя с ними сохраняются в какой-либо файл на диске и периодически отправляются злоумышленнику. Троянские программы этого типа часто используются для кражи информации пользователей различных систем онлайновых платежей и банковских систем.

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

сервис удаленному злоумышленнику. Rootkit – сокрытие присутствия в операционной системе. Понятие rootkit пришло к нам из UNIX. Первоначально это понятие использовалось для обозначения набора инструментов, применяемых для получения прав root. Rootkit – программный код или техника, направленная на сокрытие присутствия в системе заданных объектов (процессов, файлов, ключей реестра и т.д.).

ArcBomb — «бомбы» в архивах. Представляют собой архивы, специально оформленные таким образом, чтобы вызывать нештатное поведение архиваторов при попытке разархивировать данные – зависание или существенное замедление работы компьютера или заполнение диска большим количеством «пустых» данных. Особенно опасны «архивные бомбы» для файловых и почтовых серверов, если на сервере используется какая-либо система автоматической обработки входящей информации – «архивная бомба» может просто остановить работу сервера. Встречаются три типа подобных «бомб»: некорректный заголовок архива, повторяющиеся данные и одинаковые файлы в архиве.

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

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

Огромное количество одинаковых файлов в архиве также практически не сказывается на размере архива при использовании специальных методов (например, существуют приемы упаковки 10100 одинаковых файлов в 30 КБ RAR или 230 КБ ZIP-архив).

Trojan-Notifier – оповещение об успешной атаке. Троянцы данного типа предназначены для сообщения своему «хозяину» о зараженном компьютере. При этом на адрес «хозяина» отправляется информация о компьютере, например, IP-адрес компьютера, номер открытого порта, адрес электронной почты и т. п. Отсылка осуществляется различными способами: электронным письмом, специально оформленным обращением к веб-странице «хозяина», ICQ-сообщением. Данные троянские программы используются в многокомпонентных троянских наборах для извещения своего «хозяина» об успешной инсталляции троянских компонент в атакуемую систему.

Полиморфные вирусы – вирусы, постоянно изменяющие (модифицирующие) свое тело для укрытия от обнаружения. В теле этих вирусов не имеется ни одной постоянной цепочки байтов, по которой можно было бы идентифицировать вирус. В частности, они меняют или шифруют свой код при создании каждой копии. Кроме того, они изменяют свою стартовую часть, которая служит для раскодировки остальных команд вируса. Некоторые вирусы подобного типа имеют очень сложный механизм самомоди-

фикации. В них каждая значащая команда передается одним из сотен тысяч возможных вариантов. При этом для шифрования вирус пользуется случайными паролями (ключами), а также различными методами шифрования, что исключает возможность опознания вируса по сигнатурам вирусов. Полиморфные вирусы намного труднее обнаружить, чем обычные, так как экземпляры таких вирусов отличаются друг от друга. Однако для их поиска и нейтрализации были разработаны новые методики. Современные антивирусные программы справляются с полиморфными вирусами, несмотря на все ухищрения, предпринятые их разработчиками.

Макрокомандные вирусы – это вирусы, атакующие не программные файлы, а файлы документов пакета программ Microsoft Office.

Современные текстовые и табличные процессоры, такие как Microsoft Word и Excel, записывают в файлы документов не только текстовую, числовую и графическую информацию, но и программные объекты – так называемые макрокоманды. С 1995 г. появились вирусы, поражающие файлы офисных документовWord. Ранее они не могли поражаться, т.к. они не содержали исполнительных программ. Однако программисты фирмы MICROSOFT встроили в документы Word для WINDOWS мощный язык макрокоманд Word Basic. При этом команды не видны при редактировании документа, поэтому стало возможным их заражение. Эти вирусы получили название макрокомандных вирусов. Макрокомандный вирус прикрепляется к файлам офисных документов и распространяется вместе с ними. Файл, зараженный макрокомандным вирусом, можно открыть как обычный файл документа. Его можно редактировать и сохранить изменения на диске. Единственное, что нельзя с ним сделать, так это сохранить файл в другом формате, например в формате документа или в формате RTF. Таким образом, компьютерные вирусы могут внедряться в документы типов *.doc, *.xls, а также другие офисные документы, создаваемые пакетом Microsoft Office и содержащие макрокоманды.

Макрокомандный вирус размножается, изменяя код стандартных макрокоманд, предназначенных, например, для открытия и сохранения файла. Вместе с выполнением полезных функций измененные макрокоманды будут сохранять тело вируса в других документах Microsoft Office.

Фактически макрокомандные вирусы можно создать для документов, создаваемых любыми приложениями, если помимо данных внутри документов хранятся макрокоманды, а язык макрокоманд допускает не только чтение, но и запись файлов.

В целом все компьютерные программы можно разделить на исполняемые и интерпретируемые программы. Исполняемые программы содержат код, который предназначен для непосредственного выполнения центральным процессором компьютера. Что же касается интерпретируемых программ, то они представляют собой текстовые файлы (или фрагменты

текста, встроенные в офисные документы), которые исполняются, а точнее говоря, интерпретируются при помощи специальной программы. Такая программа называется интерпретатором.

Интерпретируемые программы составляются на таких языках программирования, как Basic, Java, JavaScript, VBScript, Visual Basic for Application и др. Кроме того, пакетные файлы, содержащие команды ОС, также можно рассматривать как интерпретируемые программы.

Если интерпретируемая программа записана в файле, то этот файл может стать объектом атаки компьютерного вируса или вредоносной программы другого типа.

Вирус может записать свой код внутрь такого файла, в результате чего он получит управление при запуске интерпретируемой программы.

Компьютерный вирус может распространяться через файлы интерпретируемых программ, в том числе через командные файлы ОС.

Пользователь обычно сам запускает интерпретируемые программы явным или неявным образом. Неявный запуск макрокоманд происходит при загрузке для редактирования офисных документов. Макрокоманды документов Microsoft Office есть ни что иное, как интерпретируемые программы на языке Microsoft Visual Basic for Application.

Распространение макрокомандных вирусов происходит в процессе обмена зараженными офисными документами. При этом файлы документов могут передаваться с использованием дискет, компакт-дисков, флеш-дисков или любых других аналогичных устройств внешней памяти, через интрасеть или Интернет.

Заражение макрокомандным вирусом может произойти после того, как пользователь откроет офисный документ, содержащий макрокомандный вирус, для просмотра в соответствующем офисном приложении.

Кроме того, макрокомандные вирусы могут оставить в системе вирусы или вредоносные объекты любых других типов.

Современные антивирусы обнаруживают макрокомандные вирусы, сканируя содержимое документов.

Вирусы в пакетных файлах ОС. Почти в любой операционной системе (ОС) имеется такое средство автоматизации выполнения процедур, как пакетные файлы.

Пакетные файлы содержат программы на специальном командном языке, который зависит от ОС. С помощью этого языка можно запускать произвольные программы, выдавать команды ОС, создавать файлы и каталоги, словом, делать практически все что угодно с ОС и содержимым диска.

Возможности пакетных файлов используют специально созданные вирусы, называемые *вирусами пакетных файлов*. Пакетный вирус, вирус пакетных файлов – это вирус, который записывает свое тело внутрь пакетного файла операционной системы (ОС), маскируя исполнимый код под строки комментариев.

Следует отметить, что вирусы этого типа встречаются крайне редко, тем не менее они могут быть созданы для любой распространенной ОС.

Вирусы в драйверах ОС. Эти вирусы внедряются в файлы драйверов операционных систем (программы управления устройствами), перечисленные в файле CONFIQ.SYS при начальной загрузке ПК. Иногда драйверы используются как этап в стратегии распространения вируса. При запуске заражаются драйверы, а при запуске драйвера вирус становится резидентным и заражает файлы на дисках.

Драйверы представляют собой системные программы, с помощью которых ОС взаимодействует с периферийными устройствами компьютера, такими как диск, клавиатура, принтер и т.д. Так как драйверы расположены в программных файлах, то вирусы, заражающие драйверы, можно отнести к файловым вирусам.

Бестелесные вирусы. Вирусы, заражающие не файлы или загрузочные области дисков, а оперативную память компьютера. Эти вирусы называются бестелесными. Бестелесный вирус заражает только оперативную память компьютера, не попадая в файлы или служебные области дисков.

Такие вирусы не могут быть обнаружены антивирусными программами, которые ограничивают проверки сканированием файлов, расположенных на дисках компьютера. Хотя бестелесные вирусы существует только до тех пор, пока работает операционная система, время их существования может быть достаточно велико. Это произойдет, например, если они попали в память сервера, работающего круглосуточно.

Вирусы для пиринговых сетей. В современном Интернете имеется большое количество сетей, предназначенных для обмена файлами без применения централизованного сервера. Эти сети позволяют пользователям Интернета свободно обмениваться музыкальными файлами, программами и другой информацией.

Эти сети часто называются файлообменными или пиринговыми. Последнее из этих названий происходит от названия применяемого в таких сетях способа обмена данными узел-узел (Peer-To-Peer).

Для пиринговых сетей разработчиками вредоносных программ были созданы специальные вирусы, называемые вирусами для пиринговых сетей. Вирус пиринговых сетей – это вредоносная программа, специально предназначенная для систем обмена файлами между компьютерами пользователей Интернета, такими как Kazaa, Windows Messenger, ICQ и т.д.

Чтобы такой вирус попал на компьютер пользователя пиринговой сети, пользователю требуется выполнить какое-либо действие, например, загрузить и запустить на выполнение файл.

9.2. Антивирусная защита

Для нейтрализации вирусных атак применяют специальные антивирусные программы. Антивирусными программами называются программы, осуществляющие обнаружение и защиту от вирусов. Применяемые средства антивирусной защиты должны быть сертифицированы согласно п. 20.6 приказу ФСТЭК от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

Рынок сертифицированных средств антивирусной защиты представлен такими компаниями, как «Лаборатория Касперского», ESET, Доктор Веб, Security Studio End point Protection и др.

Все эти компании отличаются качественными и комплексными продуктами, обеспечивающими должный уровень антивирусной защиты. Главной особенностью Security Studio Endpoint Protection, выделяющей его среди конкурентов, является наличие сертификатов ФСТЭК на встроенную систему обнаружения вторжений (СОВ), что позволяет объединить статьи расходов на покупку антивирусного ПО и системы обнаружения вторжений.

Выбор в пользу того или иного средства основывался на таких факторах, как эффективность работы; обширность вирусной базы; регулярное обновление; возможность блокировки неизвестных угроз; простой для понимания интерфейс; легкость в настройке параметров программы; доступная цена, пониженная ресурсоемкость.

При выборе необходимо помнить, что использование на компьютере антивируса, как правило, увеличивает время загрузки операционной системы. Чем больше системных ресурсов потребляет приложение, тем меньше их остается для других приложений. В состоянии покоя антивирусы способны потреблять сотни мегабайт оперативной памяти. Это является нежелательным эффектом для пользователя, но зачастую с этим приходиться мириться.

Различают:

1) программы-детекторы;
2) программы-доктора, или фаги;
3) программы-ревизоры;
4) программы-фильтры (сторожа);
5) программы-вакцины, или иммунизаторы.

Программы-детекторы осуществляют поиск характерной для данного вируса цепочки последовательности байтов (сигнатуры вируса) в оперативной памяти в файлах и при обнаружении выдают соответствующее сообщение. Недостаток – их могут находить только те вирусы, которые известны разработчикам.

Программы-доктора, или фаги, не только находят файлы, зараженные вирусами, но и «лечат» их, т.е. удаляют из файла тело программы вируса, возвращая файлы в исходное состояние. Часто такие программы создаются для поиска и уничтожения большого числа типов вирусов. Наиболее известны: Aidstest, Scan, Norton Antivirus. Эти программы также нуждаются в обновлении их версий, так как появляются новые КВ.

Программы-ревизоры – это программы, которые запоминают исходное состояние программ, каталогов и загрузочных областей диска тогда, когда ПК не заражен и периодически сравнивают их состояние с исходным. Обнаруженные различия выводятся на экран. Сравнение проводится сразу после загрузки ОС. При этом проверяются длина файла, дата и время модификации и т.д. Это наиболее надежные программы, которые обнаруживают стелс-КВ.

Программы-фильтры, или «сторожа», – это небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе ПК, характерных для вирусов. Такими действиями могут быть:

а) попытка корректировки файлов с расширением COM и EXE;

б) изменение атрибутов файлов;

в) запись в загрузочные сектора;

г) загрузка резидентной программы.

При попытке программ произвести указанные действия «сторож» посылает пользователю сообщение об этом и предлагает запретить или разрешить эти действия. «Фильтры» хороши тем, что обнаруживают вирус на самой ранней стадии его появления. Недостаток – не лечат и порой назойливы. Применяются редко.

По организации своей работы антивирусы делятся на две группы: сканеры и мониторы. Антивирусные сканеры проверяют систему только тогда, когда Вы их запускаете: анализируют содержимое оперативной памяти, прочёсывают диск, отыскивая заразу. Найдя оную, – лечат или стирают. Проработав, отключаются. Антивирусные мониторы (сторожа) работают постоянно (это называется «резидентно»), проверяя на лету всю информацию, которую программы собираются писать на диск или просто держат в памяти.

По принципу своей работы антивирусы делятся также на две группы:

1) работающие по использованию сигнатурного анализа;

2) работающие по использованию эвристического анализа.

В первом случае антивирусные программы имеют базу данных, в которую заносятся образцы сигнатуры каждого вируса. Эта база постоянно обновляется. При проверке антивирусная программа просматривает сигнатуру (всю цепочку байтов) каждого проверяемого файла. И если находит в её составе сигнатуру вируса, то считает, что файл зараженный. При лечении эта вредоносная сигнатура вырезается. Метод очень надежный, но с одним существенным недостатком - пока образца вируса в базе данных нет, защиты от такого вируса невозможна.

Эвристический анализ (эвристическое сканирование) – это совокупность функций антивируса, нацеленных на обнаружение неизвестных вирусным базам вредоносных программ.

Практически все современные антивирусные средства применяют технологию эвристического анализа программного кода. Методика эвристического анализа позволяет обнаруживать ранее неизвестные инфекции, однако, лечение в таких случаях практически всегда оказывается невозможным. В таком случае, как правило, требуется дополнительное обновление антивирусных баз для получения последних сигнатур и алгоритмов лечения, которые, возможно, содержат информацию о ранее неизвестном вирусе. В противном случае, файл передается для исследования антивирусным аналитикам или авторам антивирусных программ.

В процессе эвристического анализа производится проверка эмулируемой программы анализатором кода. К примеру, программа инфицирована полиморфным вирусом, состоящим из зашифрованного тела и расшифровщика. Эмулятор кода считывает инструкции в буфер антивируса, разбирает их на инструкции и производит их исполнение по одной инструкции, после этого анализатор кода подсчитывает контрольную сумму и сверяет её с той, которая хранится в базе. Эмуляция будет продолжаться до тех пор, пока необходимая для подсчета контрольной суммы часть вируса не будет расшифрована. Если сигнатура совпала, то программа определена.

Недостатки эвристического сканирования – чрезмерная подозрительность эвристического анализатора может вызывать ложные срабатывания при наличии в программе фрагментов кода, выполняющего действия и/или последовательности, в том числе и свойственные некоторым вирусам.

Наличие простых методик обмана эвристического анализатора. Как правило, прежде чем распространять вредоносную программу (вирус), её разработчики исследуют существующие распространенные антивирусные продукты, различными методами избегая её детектирование при эвристическом сканировании. К примеру, видоизменяя код, используя элементы, выполнение которых не поддерживается эмулятором кода данных антивирусов, используя шифрование части кода и др.

Несмотря на заявления и рекламные проспекты разработчиков антивирусных средств относительно совершенствования эвристических меха-

низмов, эффективность эвристического сканирования на данный момент далека от ожидаемой.

На сегодня на рынке антивирусных средств существует немало предложений. Наиболее известны следующие.

Антивирус Касперского. Среди достоинств можно выделить то, что антивирусная база Касперского очень большая, что позволяет ему оперативно реагировать на новые угрозы и отражать их от компьютера. В интернете существует очень много фишинговых сайтов, созданных для кражи паролей. Антивирус сразу уведомит пользователя о переходе по вредоносной ссылке и заблокирует доступ к ним. Одним из главных для пользователя преимуществ является простой интерфейс программы, который без проблем освоит даже начинающий пользователь. Для обычного пользователя программа работает по принципу, как говорится, «поставил и забыл». Имеется также функция безопасного запуска приложений, при которой вредоносное ПО отслеживается еще до момента полной загрузки операционной системы. При проверке системы антивирусом выдается список уязвимостей в приложениях. Программы из данного списка могут быть подвержены вирусным атакам больше всего. Также хакеры используют специальное вредоносное ПО, которое также обнаруживается рассматриваемым нами антивирусом. Вся информация о вирусах и вредоносных программах передается разработчику для усовершенствования в дальнейшем защитной программы. Но многие, несмотря на все преимущества, критикуют данный антивирус. На «слабых» компьютерах он заметно тормозит систему. Те, кто не может себе позволить купить более мощный компьютер, зачастую вынуждены попросту ставить новый антивирус.

В антивирус Касперского встроен брандмауэр, предназначенный для улучшения защиты компьютера. Доступно несколько степеней защиты. Можно выбрать максимальную, чтобы на компьютер могло попасть наименьшее число вредоносных объектов, но тогда это может вызвать неудобства при работе на компьютере – антивирус потребует больше ресурсов и может тормозить систему, поэтому многие советуют выбирать среднюю степень защиты и время от времени проводить антивирусную проверку. Купить продление лицензии Касперского вы можете на сайте разработчика.

AVAST. Достоинства:

– интуитивно понятный, приятный интерфейс;

– богатый арсенал (песочница, виртуализация, брандмауэр);

– сканирование при загрузке, позволяющее убивать вирусы в системных папках;

– низкие требования к ресурсам системы.

Недостатки:

– не гарантирует 100 % защиты (но её не обеспечивает никто);

– мало обращает внимания на трояны и шпионы;

– бесплатная версия (Avast Free Antivirus) работает медленнее платной Avast Internet Security.

Dr. Web – мощный антивирус, с очень частым обновлением антивирусных баз и способен создать мощную защиту от любых угроз.

Одним из наиболее важных достоинств будет компактность, это дает возможность быстро обновить Dr. Web даже при медленном интернете.

Dr. Web проверяет всю память ПК, что не дает шанса вирусам спрятаться в отдаленных уголках памяти. Вирусные базы могут обновляться в автоматическом режиме, что значительно упрощает использование приложения.

Этот антивирус способен выявлять практически любые вирусы и зараженные файлы, а также вылечивать их. Есть также особенность, которой нет у большинства других программ, это возможность проверять на вирусы почтовый трафик. Для этого в Dr. Web вмонтирован специальный фильтр для почтового ящика. Скорость реакции Dr. Web также хорошая, что только увеличивает степень защиты.

Dr. Web забирает минимум ресурсов компьютера, поэтому он, как никто другой, подходит для слабых машин, практически не влияя на производительность во время выполнения других задач, таких, как игры или работа с другими мощными программами.

В отличие от большинства конкурирующих решений, программные продукты Dr. Web имеют сертификаты соответствия ФСТЭК России и ФСБ России. Это позволяет использовать их в организациях с повышенными требованиями к уровню безопасности.

Dr. Web сертифицирован Министерством обороны Российской Федерации. Dr. Web соответствует требованиям Федерального закона «О персональных данных» № 152-ФЗ от 27.07.2006, предъявляемым как к антивирусным подсистемам локальной сети компании, так и к подсистемам защиты от несанкционированного доступа и может применяться в сетях, соответствующих максимально возможному уровню защищенности, включая сети, защищенные по классу К1.

Dr. Web определяет:

– почтовые вирусы;
– сетевые вирусы;
– файловые вирусы;
– троянские программы;
– стелс-вирусы;
– полиморфные вирусы;
– бестелесные вирусы;
– макровирусы;
– вирусы, поражающие документы MS Office;

– скрипт-вирусы;
– шпионское ПО (Spyware);
– программы-похитители паролей;
– клавиатурные шпионы;
– программы-дозвонщики;
– рекламное ПО (Adware);
– потенциально опасное ПО;
– хакерские утилиты;
– программы-люки;
– программы-шутки;
– вредоносные скрипты;
– другие нежелательные коды.

Ключевые функции Dr. Web:

– сканер – качественные детектирование и нейтрализация вирусов и вредоносных объектов на жестких дисках, сменных носителях и в оперативной памяти;

– защита от вирусов, использующих rootkit-технологии;

– обнаружение и нейтрализация вирусов, существующих в оперативной памяти и никогда не встречающихся в виде отдельных файлов (бестелесные черви);

– определение вирусов в архивах любой степени вложенности и в упакованных объектах;

– проверка файлов, сжатых упаковщиками, в том числе, не известными;

– проверка входящей и исходящей корреспонденции на вирусы по протоколам SMTP/POP3/NNTP/IMAP;

– защита от массовых рассылок с компьютера сообщений почтовыми червями;

– защита от несанкционированного доступа извне, предотвращение утечек важных данных по сети, блокировка подозрительных соединений на уровне пакетов и приложений;

– сканирования по требованию и индивидуальные графики проверок ПК;

– автоматический прием обновлений вирусной базы Dr. Web с любой нужной периодичностью;

– автоматические уведомления об обнаруженных инфицированных, неизлечимых или подозрительных объектах;

– напоминания о необходимости проведения обновлений вирусных баз;

– централизованное управление настройками всех компонентов;

– прозрачность работы – подробные отчеты о работе каждого модуля.

Эту программу уже очень многие оценили по достоинству и постоянно используют на своих ПК.

Для того чтобы не допустить проникновения на свой компьютер вирусов и других вредоносных объектов, необходимо приобретение лицензионных копий программ на компакт-дисках непосредственно у компании-разработчика и ее партнеров. Тем не менее известны случаи, когда по чьей-то ошибке в продажу попали лицензионные компакт-диски с зараженными файлами.

Нелицензионные программы потенциально опасны, т.к. файлы этих программ могут содержать компьютерные вирусы и другие вредоносные объекты.

10. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ

Криптографические методы защиты информации – это специальные методы шифрования, кодирования или иного преобразования информации, в результате которых ее содержание становится недоступным без предъявления ключа криптограммы и обратного преобразования (рис. 17).

Криптографический метод защиты, безусловно, самый надежный метод защиты, так как охраняется непосредственно сама информация, а не доступ к ней (например, зашифрованный файл нельзя прочесть даже в случае кражи носителя). Данный метод защиты реализуется в виде программ или пакетов программ.

Шифрование – преобразовательный процесс: исходный текст, который носит также название открытого текста, заменяется шифрованным текстом.

Дешифрование – обратный шифрованию процесс. На основе ключа шифрованный текст преобразуется в исходный.

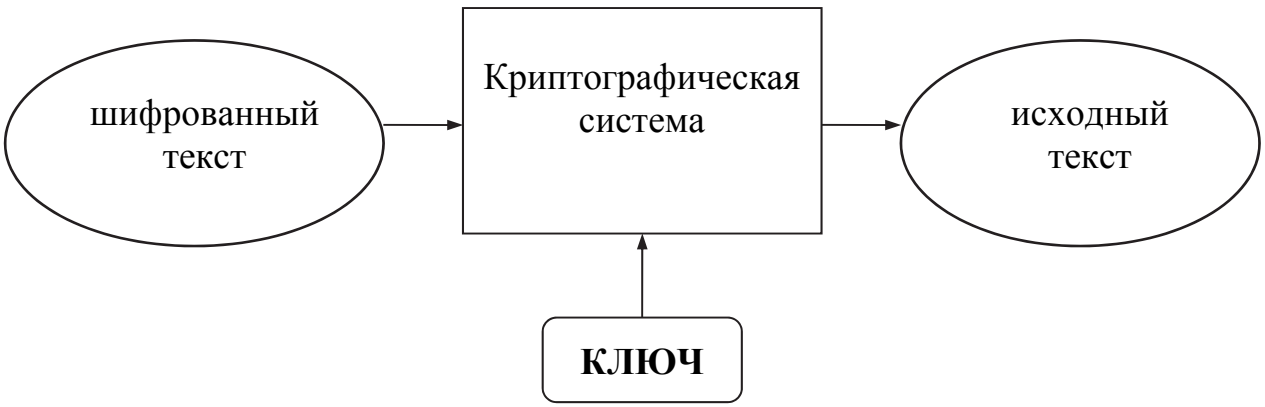


Рис. 17. Ключ криптограммы

Ключ – информация, необходимая для беспрепятственного шифрования и дешифрования текстов.

Шифрование данных может осуществляться в режимах On-line (в темпе поступления информации) и Off-line (автономном).

При автономном наиболее распространены два алгоритма.

Стандарт шифрования данных DES (Data Encryption Standart) был разработан фирмой IBM в начале 70-х гг. и в настоящее время является правительственным стандартом для шифрования цифровой информации. Он рекомендован Ассоциацией Американских Банкиров. Сложный алгоритм DES использует ключ длиной 56 бит и 8 битов проверки на четность и требует от злоумышленника перебора 72 квадрилионов возможных ключевых комбинаций, обеспечивая высокую степень защиты при небольших расходах. При частой смене ключей алгоритм удовлетворительно решает проблему превращения конфиденциальной информации в недоступную.

Алгоритм RSA был изобретен Ривестом, Шамиром и Альдеманом в 1976 г. и представляет собой значительный шаг в криптографии.

Если ключи DES можно сгенерировать за микросекунды, то примерное время генерации ключа RSA – десятки секунд, поэтому открытые ключи RSA предпочитают разработчики программных средств, а секретные ключи DES – разработчики аппаратуры.

Основные направления использования криптографических методов – передача конфиденциальной информации по каналам связи (например, электронная почта), установление подлинности передаваемых сообщений, хранение информации (документов, баз данных) на носителях в зашифрованном виде.

Современная криптография включает в себя четыре крупных раздела:

1) симметричные криптосистемы;
2) криптосистемы с открытым ключом;
3) электронная подпись;
4) управление ключами.

10.1. Симметричные криптосистемы

В симметричных криптосистемах и для шифрования, и для дешифрования используется один и тот же ключ. На основе ключа шифрованный текст преобразуется в исходный и наоборот исходный текст заменяется шифрованным текстом.

Все многообразие существующих криптографических методов в симметричных криптосистемах можно свести к следующим четырем классам преобразований:

1) **многоалфавитная подстановка** – символы шифруемого текста заменяются символами того же или другого алфавита в соответствии с заранее определенным правилом. Для обеспечения высокой криптостойкости требуется использование больших ключей.

2) **перестановка** – символы шифруемого текста переставляются по некоторому правилу в пределах заданного блока передаваемого текста;

3) **аналитическое преобразование** – шифруемый текст преобразуется по некоторому аналитическому правилу, например гаммирование – заключается в наложении на исходный текст некоторой псевдослучайной последовательности, генерируемой на основе ключа;

4) **комбинированное преобразование или блочные шифры** – представляют собой последовательность (с возможным повторением и чередованием) основных методов преобразования, применяемую к блоку (части) шифруемого текста. Блочные шифры на практике встречаются чаще, чем "чистые" преобразования того или иного класса в силу их более высокой криптостойкости. Российский и американский стандарты шифрования основаны именно на этом классе.

10.2. Криптосистемы с открытым ключом

В системах с открытым ключом используются два ключа – открытый и закрытый, которые математически связаны друг с другом.

Информация шифруется с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения (ключ – информация, необходимая для беспрепятственного шифрования и дешифрования текстов.)

Как бы ни были сложны и надежны криптографические системы, их слабое место при практической реализации – проблема распределения ключей. Для того чтобы был возможен обмен конфиденциальной информацией между двумя субъектами ИС, ключ должен быть сгенерирован одним из них, а затем каким-то образом опять же в конфиденциальном порядке передан другому, т.е. в общем случае для передачи ключа опять же требуется использование какой-то криптосистемы.

Для решения этой проблемы на основе результатов, полученных классической и современной алгеброй, были предложены системы с открытым ключом.

Суть их состоит в том, что каждым адресатом ИС генерируются два ключа, связанные между собой по определенному правилу. Один ключ объявляется открытым, а другой закрытым. Открытый ключ публикуется и доступен любому, кто желает послать сообщение адресату. Секретный ключ сохраняется в тайне. Исходный текст шифруется открытым ключом адресата и передается ему. Зашифрованный текст в принципе не может быть расшифрован тем же открытым ключом. Дешифрование сообщения возможно только с использованием закрытого ключа, который известен только самому адресату.

10.3. Электронная подпись

Системой электронной подписи называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим **пользователем проверить авторство и подлинность сообщения.**

В чем состоит проблема аутентификации данных? В конце обычного письма или документа исполнитель или ответственное лицо обычно ставит свою подпись. Подобное действие обычно преследует две цели. Во-первых, получатель имеет возможность убедиться в истинности письма, сличив подпись с имеющимся у него образцом. Во-вторых, личная подпись является юридическим гарантом авторства документа. Последний аспект особенно важен при заключении разного рода торговых сделок, составлении доверенностей, обязательств и т.д. Если подделать подпись человека на бумаге весьма непросто, а установить авторство подписи современными криминалистическими методами – техническая деталь, то с подписью электронной дело обстоит иначе. Подделать цепочку битов, просто ее скопировав, или незаметно внести нелегальные исправления в документ сможет любой пользователь. С широким распространением в современном мире электронных форм документов (в том числе и конфиденциальных) и средств их обработки особо актуальной стала проблема установления подлинности и авторства безбумажной документации.

10.4. Управление ключами

Управление ключами – это процесс составления и распределения ключей между пользователями. Как бы ни была сложна и надежна сама криптосистема, она основана на использовании ключей. Если для обеспечения конфиденциального обмена информацией между двумя пользователями процесс обмена ключами тривиален, количество пользователей составляет десятки и сотни, то управление ключами – серьезная проблема. Если не обеспечено достаточно надежное управление ключами, то завладев ею, злоумышленник получает неограниченный доступ ко всей информации. Управление ключами – информационный процесс, включающий в себя три элемента:

1) генерацию ключей,
2) накопление ключей,
3) распределение ключей.

Генерация ключей. В серьезных информационных системах используются специальные аппаратные и программные методы генерации случайных ключей.

Идеальными генераторами являются устройства на основе "натуральных" случайных процессов. Например, случайным математическим объектом являются десятичные знаки иррациональных чисел, которые вычисляются с помощью стандартных математических методов.

Накопление ключей. Под накоплением ключей понимается организация их хранения, учета и удаления.

Секретные ключи никогда не должны записываться в явном виде на носителе, который может быть считан или скопирован. В достаточно сложной ИС один пользователь может работать с большим объемом ключевой информации, и иногда даже возникает необходимость организации минибаз данных по ключевой информации. Такие базы данных отвечают за принятие, хранение, учет и удаление используемых ключей. Итак, каждая информация об используемых ключах должна храниться в зашифрованном виде.

Ключи, зашифровывающие ключевую информацию, называются мастер-ключами. Желательно, чтобы мастер-ключи каждый пользователь знал наизусть и не хранил их вообще на каких-либо материальных носителях.

Очень важным условием безопасности информации является периодическое обновление ключевой информации в ИС. При этом переназначаться должны как обычные ключи, так и мастер-ключи. В особо ответственных ИС обновление ключевой информации желательно делать ежедневно. Вопрос обновления ключевой информации связан и с третьим элементом управления ключами - распределением ключей.

Распределение ключей. Распределение ключей – самый ответственный процесс в управлении ключами. К нему предъявляются два требования:

1) оперативность и точность распределения;
2) скрытность распределяемых ключей.

Распределение ключей между пользователями реализуются двумя разными подходами:

1) путем создания одного или нескольких центров распределения ключей. Недостаток такого подхода состоит в том, что в центре распределения известно, кому и какие ключи назначены, и это позволяет читать все сообщения, циркулирующие в ИС;

2) прямой обмен ключами между пользователями информационной системы. В этом случае проблема состоит в том, чтобы надежно удостоверить подлинность субъектов. Для обмена ключами можно использовать криптосистемы с открытым ключом, используя тот же алгоритм RSA.

В целом задача управления ключами сводится к поиску такого протокола распределения ключей, который обеспечивал бы:

- возможность отказа от центра распределения ключей;
- взаимное подтверждение подлинности участников сеанса;

– подтверждение достоверности сеанса механизмом запроса-ответа, использование для этого программных или аппаратных средств;

– использование при обмене ключами минимального числа сообщений.

Реализация криптографических методов

Проблема реализации методов защиты информации имеет два аспекта:

1) разработка средств, реализующих криптографические алгоритмы;
2) методика использования этих средств.

Каждый из рассмотренных криптографических методов может быть реализован либо программным, либо аппаратным способом.

Возможность программной реализации обуславливается тем, что все методы криптографического преобразования формальны и могут быть представлены в виде конечной алгоритмической процедуры.

При аппаратной реализации все процедуры шифрования и дешифрования выполняются специальными электронными схемами. Наибольшее распространение получили модули, реализующие комбинированные методы.

Основным достоинством программных методов реализации защиты является их гибкость, т.е. возможность быстрого изменения алгоритмов шифрования. Основным же недостатком программной реализации является существенно меньшее быстродействие по сравнению с аппаратными средствами (примерно в 10 раз). В последнее время стали появляться комбинированные средства шифрования, так называемые программно-аппаратные средства. В этом случае в компьютере используется своеобразный "криптографический сопроцессор" – вычислительное устройство, ориентированное на выполнение криптографических операций (сложение по модулю, сдвиг и т.д.). Меняя программное обеспечения для такого устройства, можно выбирать тот или иной метод шифрования. Такой метод объединяет в себе достоинства программных и аппаратных методов.

Таким образом, выбор типа реализации криптозащиты для конкретной ИС в существенной мере зависит от ее особенностей и должен опираться на всесторонний анализ требований, предъявляемых к системе защиты информации.

10.5. Проверка подлинности сообщения информации (идентификация и аутентификация)

Проверка подлинности сообщения информации – это идентификация и аутентификация.

Методы, применяемые в открытых сетях для подтверждения и проверки подлинности сообщения, следующие:

– субъект демонстрирует знание секретного ключа, при этом ключ либо вообще не передается по сети, либо передается в зашифрованном виде;

– субъект демонстрирует обладание программным или аппаратным средством генерации одноразовых паролей или средством, работающим в режиме "запрос-ответ". Нетрудно заметить, что перехват и последующее воспроизведение одноразового пароля или ответа на запрос ничего не дает злоумышленнику;

– субъект демонстрирует подлинность своего местоположения, при этом используется система навигационных спутников.

Методы, применяемые в открытых сетях для подтверждения и проверки подлинности сообщения, должны быть устойчивы к пассивному и активному прослушиванию сети.

Для исключения неавторизованного проникновения в компьютерную сеть используется комбинированный подход – пароль + идентификация пользователя по персональному "ключу". "Ключ" представляет собой пластиковую карту (магнитная или со встроенной микросхемой - смарт-карта) или различные устройства для идентификации личности по биометрической информации – по радужной оболочке глаза, отпечаткам пальцев, размерам кисти руки и т.д. Серверы и сетевые рабочие станции, оснащенные устройствами чтения смарт-карт и специальным программным обеспечением, значительно повышают степень защиты от несанкционированного доступа.

Смарт-карты управления доступом позволяют реализовать такие функции, как контроль входа, доступ к устройствам ПК, к программам, файлам и командам.

11. ПРОГРАММНО-АППАРАТНАЯ ЗАЩИТА СЕТЕЙ

Работа с сетью налагает свои особенности программной безопасности, поскольку именно через коммуникации сетей происходит наибольшее число вирусных хакерских атак.

Для начала необходимо привести краткую справку, которая может понадобиться для понимания данного материала тем, кто не знаком с сетевыми технологиями. Те, кто знаком с ними, могут пропустить эту часть, потому что всё дано только в базовых понятиях без технических деталей.

Вся информация в сети передаётся пакетами, т.е. "порциями". У пакета есть адрес отправителя, получателя, порт отправителя и порт получателя, а также некоторые другие служебные данные. Пакеты могут быть фрагментированы, т.е. один пакет может быть разбит на несколько фрагментов и отправлен в таком виде. Информация о фрагментации добавляется к служебной, поэтому компьютер-получатель знает, как правильно собрать фрагменты в один пакет. Для понимания материала укажем три типа пакета:

1) TCP – самый надёжный пакет, потому что компьютер должен послать уведомление, что пакет получен, если уведомления нет, то пакет посылается повторно, поэтому потеря информации исключена. Но есть недостаток: из-за посылки уведомления о получении каждого пакета снижается скорость;

2) UDP – схож с TCP, но уведомление о получении не посылается, поэтому возможна потеря информации в том случае, если пакет не достигает получателя. Но этот вид пакетов быстрее, нежели TCP;

3) ICMP – не используются для передачи информации. Пакеты, скорее, служебного плана, например, для диагностики сети или для пинга.

Связь между двумя компьютерами в модели клиент-сервер: клиент посылает серверу на открытый порт SYN-пакет (т.е. пакет, у которого установлен флаг SYN), на что сервер отвечает SYN/ACK-пакетом (в том случае, если он готов установить соединение), после этого клиент посылает ACK-пакет, и связь считается установленной. Это элементарная модель, которая может понадобиться для понятия некоторых атак, за более подробной информацией нужно обратиться к справочнику по сетевым технологиям.

IP адрес – сетевой адрес компьютера вида XXX.XXX.XXX.XXX, где XXX могут быть от 0 до 255.

MAC адрес – уникальный адрес, вшитый в сетевую карту. Имеет вид: XX:XX:XX:XX:XX:XX, где XX могут быть от 00 до ff.

Адреса имеют некоторые ограничения, и некоторые не могут существовать (т.е. принадлежать компьютеру в сети), например IP адрес 0.0.0.0 или 255.255.255.255. Некоторые IP адреса не могут принадлежать машине, напрямую подключённой к Интернет, т.к. некоторые группы (т.е. диапазоны) IP адресов зарезервированы. За более подробной информацией нужно также обратиться к специальному справочнику.

TCP/IP протокол служит для передачи данных в Интернете и в большинстве сетей.

ARP протокол служит для сопоставления IP адресов MAC адресам.

ARP сервер – сервер, который отвечает за хранение сопоставленных записей вида IP адрес – MAC адрес.

DNS сервер – компьютер, который по DNS запросу клиента (например, Вашему запросу, когда Вы вводите адрес в строке адреса в Internet Explorer) переводит буквенные Интернет адреса (например: yandex.ru) в соответствующие им IP адреса (например: 23.145.14.155).

Коммутатор и концентратор – предназначение у этих устройств одинаково: подключить к одному каналу (например, Интернета) несколько компьютеров, но принцип действия различается. Концентратор принимает пакет, а потом пересылает его каждому компьютеру, а дальше компьютеры проверяют, для них ли был предназначен этот пакет. Коммутатор точно

знает, какой пакет какому компьютеру предназначается, и он посылает его конкретному компьютеру, а не всем сразу. Коммутаторы более дорогие устройства, но и более быстрые и безопасные.

Сегмент сети – группа компьютеров, подключённая к одному концентратору или коммутатору.

11.1. Защита проводных сетей

В целом защиту информации на сетевом уровне можно разделить на централизованную, глобальную, внешнюю и распределенную, локальную, внутрисетевую. Возможна также комбинированная защита, сочетающая оба этих случая.

Защита на локальном, внутрисетевом уровне осуществляется администратором с помощью специальных программ, имеющихся как в системе управляющего сервера, так и в отдельных аппаратных устройствах, например в концентраторах.

В некоторых концентраторах имеются специальные программы, которые контролируют подключенные к нему рабочие станции таким образом, что каждый подключенный к концентратору компьютер получает свой адрес, зарегистрированный программой концентратора. Если подключился другой компьютер, адрес которого не зарегистрирован в программе концентратора, то этот порт автоматически отключается с подачей тревожного сигнала администратору сети.

Концентратор позволяет также локализовать потоки информации в сети, а также контролировать эти потоки и управлять ими, с помощью применения пользовательских фильтров.

Защита на глобальном, внешнем уровне сводится к контролю информационных потоков и сообщений от внешней сети к локальной.

Наиболее эффективным средством защиты сетей на внешнем уровне является межсетевой экран – программное или аппаратное устройство, которое располагается между защищаемой (внутренней) сетью и внешней средой (внешними сетями или другими сегментами корпоративной сети) и контролирует все информационные потоки как во внутреннюю сеть, так и из нее. Согласно нормативным документам Государственной технической комиссии при Президенте РФ, межсетевой экран (он же брандмауэр (от немецкого – *brandmauer*), он же файрвол (от английского – *firewall*), он же FW, МСЭ или МЭ) представляет собой локальное (однокомпонентное) или функционально распределенное средство (комплекс), реализующее контроль за информацией, которая поступает в автоматизированную систему (АС) и/или выходит из нее, и обеспечивающее защиту автоматизированной системы посредством фильтрации информации, то есть ее анализа по совокупности критериев и принятия решения о ее распространении в (из) АС.

Контроль информационных потоков состоит в их фильтрации, то есть в выборочном пропускании через экран, возможно, с выполнением некоторых преобразований и извещением отправителя о том, что его данным в пропуске отказано. Фильтрация осуществляется на основе набора правил, предварительно загруженных в экран и являющихся выражением сетевых аспектов политики безопасности организации.

Какими функциями должен обладать корпоративный межсетевой экран? Перечень базовых функций отличается в зависимости от модели аппаратной платформы, версии ПО и фирмы-производителя МЭ, однако типовыми функциями можно назвать следующие:

- поддержка основных сетевых протоколов (согласно RFC);
- наличие пользовательского интерфейса для управления и формирования сетевых политик безопасности;
- поддержка общепризнанных сетевых технологий, таких как: VPN, NAT, PAT, VLA^RUNK, SNMPv.3, syslog и пр.;
- возможность построения отказоустойчивого (многоуровневого) и/или кластерного решения;
- журналирование событий и наличие инструментов для навигации по журналу регистрации;
- интеграция с присутствующими в инфраструктуре компании системами и средствами аутентификации пользователей (Active Directory, RADIUS, E-Directory и пр.);
- наличие масштабируемой аппаратной платформы (по количеству физических интерфейсов, CPU, HDD, оперативной памяти и пр.);
- наличие в России технической поддержки по выбранному решению.

Какие критерии необходимо определить для себя при выборе корпоративного МЭ? В настоящее время рынок МЭ в России представлен более чем двумя десятками различных как отечественных, так и иностранных производителей. Для компании, ранее не использовавшей МЭ, выбрать подходящий (формулируя для себя набор критериев) в условиях маркетинговых войн между дистрибьюторами будет достаточно непросто. Для одних руководителей критерии качества – это минимальная общая стоимость МЭ, количество успешных внедрений в России за истекший период, отзывы об эффективности работы МЭ, представленные доверенными экспертами. Для других – это формальное количество реализованных в решении требований и условий, которые были озвучены представителями заказчика до начала выборных процедур или удачно проведенное в ходе деловой встречи сравнение предлагаемого МЭ с продуктами конкурентов. Оба подхода, использующие метод анализа "черного ящика", не являются на 100 % эффективными, поскольку не могут в полной мере гарантировать применимость предлагаемого решения в конкретном случае. Именно поэтому чаще всего применяется метод построения стенда (пилотный про-

ект), который призван продемонстрировать особенности того или иного МЭ при его развертывании в инфраструктуре компании. В рамках пилотного проекта совместно с представителями разработчика (интегратора) формируется комплексная методика испытаний решения, по результатам исполнения которой принимается взвешенное решение об эффективности и, как следствие, о внедрении того или иного МЭ в конкретную среду.

Данные в сети, будь то локальная сеть или Интернет, передаются небольшими пакетами. Каждый пакет несёт в себе признак используемого протокола, адреса источника и приёмника, а также номера соответствующих портов. Последние – это числа, по которым операционная система распознаёт, какое приложение получит конкретный пакет данных. Например, при загрузке страницы с сервера http://ya.ru/ интернет-браузер получает данные с веб-сайта по протоколу HTTP. При этом обмен данными между компьютером и сервером происходит по более низкоуровнему протоколу TCP/IP, а пересылаемые от сервера к компьютеру пакеты данных имеют номер порта приёмника, скажем, 1121, а номер порта источника – всегда 80. Конечно, в реальной сети идёт постоянный обмен данными, и взаимодействие компьютеров всегда намного сложнее, однако этот простой пример показывает, что человек искушённый извлечёт из него немало информации. По этой причине *нельзя позволять пакетам, курсирующим в локальной сети, попадать в Интернет*. Также нельзя разрешать некоторым пакетам из Интернета попадать в локальную сеть предприятия.

На каждом предприятии доступ компьютеров в Интернет по локальной сети обеспечивается с помощью отдельно стоящего компьютера (его ещё называют сервером доступа). Иногда это специализированный компьютер, но чаще всего обычный, расположенный близко к устройству, обеспечивающему выход в Глобальную сеть. К сожалению, стандартные средства операционных систем не позволяют вести гибкую настройку маршрутизации и фильтрования пакетов, поэтому на таком компьютере следует разместить специализированное оборудование, например фирмы Cisco. Подобные аппаратные маршрутизаторы отличаются большей надёжностью.

Настройка ПО гораздо проще конфигурирования специализированного оборудования и может быть выполнена системным администратором средней квалификации. При этом следует запретить трансляцию пакетов, содержащих адрес приёмника в диапазоне адресов локальной сети предприятия. Также следует запретить трансляцию пакетов, не содержащих адреса локальной сети предприятия, из Интернета в локальную сеть. Это позволит оградить сеть предприятия от прослушивания извне, а также минимизировать возможности для передачи в локальную сеть враждебных пакетов. Время работы маршрутизатора, когда осуществляется трансляция пакетов, следует выбрать равным времени работы организации плюс не-

большой временной резерв для задерживающихся в офисе или пришедших раньше времени сотрудников.

Настройка firewall потребует более серьёзного подхода: следует разрешить обмен данными с Интернетом только по тем протоколам, которые реально используются на предприятии. Например, это могут быть протоколы HTTP, HTTPS, SMTP, POP3, DNS, ICQ и т.д. Попытка обмена данными по неразрешённым протоколам должна блокироваться firewall и записываться им в журнал.

Один из способов защиты сетевых каталогов с программами от проникновения компьютерных вирусов является установка прав доступа и режима «Только чтение». Это можно сделать средствами файловой системы NTFS (если сервер работает в среде ОС Microsoft Windows) или средствами файловых систем других ОС, таких как Novell Net Ware, FreeBSD, Linux и других Unix-подобных ОС.

Заметим, что подобная защита не будет работать, если вирус получит права доступа, эквивалентные правам системного администратора.

Необходимо помнить, что внедрение МЭ не может решить все проблемы безопасности. Несмотря на то, что многие производители МЭ в настоящее время позиционируют свои решения на рынке, как "всеобъемлющие продукты по обеспечению информационной безопасности корпоративного бизнеса", необходимо, отбросив "маркетинговую вуаль", понимать, что любой МЭ – это прежде всего инструмент для фильтрации проходящего трафика и контроля установления соединения. Очевидно, что, помимо сетевых угроз для объекта защиты, существует множество других, защита от которых выходит за рамки возможностей межсетевого экранирования. Это и угрозы утечки конфиденциальной информации с АРМ через съемные носители, и угрозы нарушения доступности и/или работоспособности ресурсов внутри защищаемой МЭ сети компании, и многие другие. Необходимо понимать, что МЭ – это только один (далеко не единственный) компонент системы защиты информации в компании. Решение проблем обеспечения информационной безопасности – это сложная наукоемкая задача, требующая комплексного подхода.

Необходимо также заметить, что бороться с угрозами, присущими сетевой среде, средствами универсальных операционных систем не представляется возможным. Универсальная ОС – это огромная программа, наверняка содержащая, помимо явных ошибок, некоторые особенности, которые могут быть использованы для получения нелегальных привилегий. Современная технология программирования не позволяет сделать столь большие программы безопасными.

Недавно на рынке появились МЭ нового поколения. Обычные МЭ, как правило, идентифицируют приложение по используемому TCP-порту. Так, например, FTP-клиент обычно работает через порт TCP/21, MySQL –

TCP/3306 и т.д. Пользователи идентифицируются исходя из IP-адреса источника. Однако современные приложения уже давно не используют одни и те же статические порты, более того, некоторые программы динамически меняют номера портов во время коммуникационной сессии. За пользователями сегодня вовсе не обязательно закреплен один и тот же IP-адрес. Учитывая данную специфику, компанией Palo Alto Networks был разработан с нуля МЭ нового поколения, в основе которого идентификация приложений, пользователей и угроз. Их особенность – сначала всегда идентифицируется приложение, а затем трафик пропускается только в том случае, если он разрешен политикой безопасности. И только если данный трафик разрешен политикой ИБ, на него накладываются дополнительные проверки I PS/Ant ivirus/etc.

11.2. Защита беспроводных сетей Wi-Fi

Большинство современных компьютеров поддерживают беспроводной доступ в сеть – технология Wi-Fi – сокращение от Wireless Fidelity. Wi-Fi – это логотип, который компания WECA использует для обозначения совместимости конкретного изделия с беспроводными сетями (WLAN). Термин введен Wi-Fi Alliance. Все изделия проходят сложные тесты, и тем устройствам, которые отвечают требуемым стандартам взаимодействия (802.11), присваивается сертификат с правом на логотип Wi-Fi (Wi-Fi Certified). Другими словами, компьютеры могут подключаться к интернету (и к другим устройствам, поддерживающим беспроводную связь) без сетевого кабеля. Главное преимущество беспроводных соединений – возможность работать с интернетом в любой точке дома или офиса (если позволяет расстояние между компьютером и устройством беспроводного доступа в сеть). Устройства беспроводной связи работают на базе стандартов 802.11a,802.11b, 802.11g, 802.11n, 802.16d, 802.16e, 802.16m и продвигаются на рынок сетевого оборудования очень интенсивно. Принцип беспроводной передачи данных заключает себе потенциальную возможность несанкционированных подключений к точкам доступа. При разработке корпоративной сети администраторы в первую очередь заботятся о покрытии всей территории офисов, забывая, что хакеры могут подключиться к сети прямо из автомобиля, припаркованного на улице. Бывают ситуации, когда просто нереально заблокировать саму возможность "слышать" передаваемый трафик. Несанкционированное подключение точек доступа к ЛВС может выполняться и самими работниками предприятия.

Как и любая сеть, сети Wi-Fi также подвержены опасности взлома. Существуют следующие методы взлома этих сетей.

Анализ сетевого трафика снифером Ethereal. Сбор информации об атакуемом объекте – это необходимый этап при подготовке атаки. К сожалению администраторов и владельцев беспроводной сети, пассивное прослушивание и анализ передаваемой информации может предоставить сторонним наблюдателям достаточно данных для успешного проникновения в сеть. Для сбора информации достаточно войти в зону покрытия сети, и, воспользовавшись рабочей станцией с беспроводным сетевым интерфейсом, подключить программный анализатор сетевого трафика (например, Kismet или Ethereal). Если WEP-кодирование не включено (обычная заводская настройка оборудования), то наблюдатель видит в открытом виде все данные, передаваемые в сети. Если WEP-кодирование все-таки включено, то кодируются только данные, передаваемые в сетевом пакете, а заголовок пакета передается в открытом виде. Из анализа заголовка можно извлечь информацию об идентификаторе сети, аппаратных адресах узлов доступа и клиентов сети, а также значение вектора инициализации, используемое получателем для дешифровки полученных данных. Прослушивание и анализ перехваченных сетевых пакетов делает попытки сокрытия беспроводной сети несостоятельными за счет отключения широковещательной передачи узлами доступа «маячковых» сигналов.

Подделка аппаратного адреса (MAC spoofing). Использование механизма идентификации клиентов по аппаратным адресам сетевых интерфейсов для доступа к сетевым ресурсам – не самая лучшая идея. Перехватив и проанализировав сетевой трафик, можно за короткое время получить список аппаратных адресов всех активных клиентов. Задача же изменения аппаратного адреса своего сетевого интерфейса давно решена. Под «линуксоподобными» операционными системами достаточно воспользоваться стандартной сетевой утилитой ifconfig, а для Windows-систем надо трудиться несколько больше, переставляя драйвер сетевого интерфейса или устанавливая дополнительную утилиту.

Взлом криптозащиты. Дьявол прячется в деталях. Стандарт 802.11 предусматривает две длины ключей – 40 бит и 104 бита. При длине ключа в 104 бита декодирование данных прямым перебором становится довольно утомительным занятием даже при работе новейшей вычислительной техники. На первый взгляд, реализованный в WEP-механизм криптозащиты должен быть устойчив ко взлому, но обе стороны (отправитель и получатель) должны обладать секретным ключом, используемым вместе с вектором инициализации для кодирования и декодирования информации. А в стандарте 802.11b не оговорен механизм обмена ключей между сторонами. В результате при интенсивном обмене данными, реальна ситуация повторного использования значений векторов инициализации с одним и тем же секретным ключом. Особенность реализованного алгоритма криптозащиты приводит к тому, что, имея два сетевых пакета, зашифрованных одним ко-

дирующим ключом, можно не только расшифровать данные, но и вычислить секретный ключ. Это позволяет декодировать всю перехваченную информацию.

Посредник (Man-In-The-Middle). Данный вид атаки использует функцию роуминга клиентов в беспроводных сетях. Злоумышленник на своей рабочей станции имитирует узел доступа с более мощным сигналом, чем реальный узел доступа. Клиент беспроводной сети автоматически переключается на новый узел доступа, передавая на него весь свой трафик. В свою очередь, злоумышленник передает этот трафик реальному узлу доступа под видом клиентской рабочей станции. Таким образом, система злоумышленника включается в обмен данными между клиентом и узлом доступа как посредник, что и дало название данному виду атаки – Man-In-The-Middle (пер. с англ. – посредник). Эта атака опасна тем, что позволяет взламывать защищенные соединения (VPN), устанавливаемые по беспроводной сети, вызывая принудительную реавторизацию VPN-клиента. В результате злоумышленник получает авторизационные данные скомпрометированного им клиента.

Отказ в обслуживании. Сама среда передачи данных предоставляет возможность силовой атаки на беспроводные сети. Цель подобного нападения – снижение производительности сети или ухудшение качества сетевого обслуживания вплоть до полного паралича сети. Атаки подобного вида уже рассматривались ранее. Злоумышленник может избирательно атаковать как отдельную рабочую станцию или точку доступа, так и всех клиентов сети. DoS-атака может быть и непреднамеренной. Например, вызванная включением радиопередающего оборудования, работающего на той же частоте, что и беспроводная сеть.

С учетом того, что нельзя избирательно ограничивать доступ к физической среде передачи данных в беспроводных сетях, радиоволнам, вероятно, придется смириться с существованием еще одной ахиллесовой пяты данной технологии.

Обеспечить безопасность устройства беспроводного доступа и, соответственно, свести к минимуму связанный с этим видом доступа риск можно с помощью следующих несложных шагов:

– Измените пароль администратора в своем беспроводном устройстве. Хакеру легко выяснить, какой пароль устанавливается по умолчанию производителем устройства, и использовать этот пароль для доступа в вашу беспроводную сеть. Избегайте паролей, которые легко подобрать или угадать (см. указания в разделе, посвященном выбору паролей).

– Отключите трансляцию идентификатора сети (SSID broadcasting; SSID – Service Set Identifier, идентификатор сети), чтобы ваше беспроводное устройство не транслировало в эфир информацию о том, что оно включено.

– Включите шифрование трафика: лучше всего использовать протокол WPA, если ваше устройство его поддерживает (если нет, то используйте WEP-шифр).

– Смените идентификатор сети (SSID) вашего устройства. Если оставить идентификатор, установленный по умолчанию производителем устройства, то злоумышленник, узнав этот идентификатор, сможет легко "засечь" вашу беспроводную сеть. Не используйте имена, которые легко угадать (см. указания в разделе, посвященном выбору паролей).

12. КОМПЛЕКСНОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Исторически развитие средств и методов защиты информации условно можно разделить на три этапа.

Первый из этих подходов условно может быть назван примитивным. Он характерен для начального периода развития работ по защите информации. Отличительными особенностями этого подхода являются попытки решения проблемы защиты путем разового включения в состав системы на этапе ее создания несложных механизмов защиты. Основное внимание уделялось обеспечению ее физической целостности. Проблемы защиты от несанкционированного получения информации в большинстве случаев не возникало. Это объяснялось автономностью работы ЭВМ первых поколений, индивидуальностью алгоритмической реализации процедур обработки, представление информации в памяти ЭВМ и на машинных носителях в закодированном виде, простота организационного контроля всего процесса обработки информации.

По мере роста масштабов использования автоматизированной обработки информации уязвимость информации со стороны злоумышленников стала усиливаться. Ущерб от подобных действий нередко принимал внушительные размеры и приводил к весьма серьезным последствиям. О распространенности данного вида незаконных действий достаточно убедительно говорит хотя бы такой факт: как утверждают зарубежные специалисты, на каждую копию программы, полученную законным путем, существует не менее десяти копий, полученных незаконным путем.

Кроме того, опасной формой угроз безопасности информации оказалось заражение систем и сетей компьютерными вирусами, поэтому на рубеже 70-80-х гг. на смену примитивному пришел полусистемный подход, который характеризуется существенным расширением используемых средств защиты, особенно организационных – назначением специального профессионально подготовленного лица, ответственного за защиту. В американских публикациях это лицо именовалось офицером безопасности.

Наконец, в последние годы на смену полусистемному приходит комплексный подход к организации защиты информации. Для этого подхода характерен взгляд на защиту информации как на непрерывный процесс, осуществляемый на всех этапах жизненного цикла автоматизированных систем с помощью использования всех имеющихся средств защиты, причем все используемые средства и методы объединены в единую систему, одной из основ функционирования которой является созданная на этом этапе нормативно-правовая база защиты информации. К указанным средствам относятся законы, стандарты и другие нормативно-правовые акты, регламентирующие правила обращения с защищаемой информацией и являющиеся обязательными для соблюдения. Расширяется типизация и стандартизация проектных решений, стремление к аппаратной реализации функций защиты, переход на поточно-индустриальные принципы производства и использования.

Отчетливо просматривается тенденция выработки и реализации концепции защиты, направленной на решение трех классов задач – задач анализа, синтеза и управления.

Задача анализа заключается в объективной оценке потенциальных угроз информации и возможного ущерба от их проявления.

Задачи синтеза – определение наиболее эффективных форм и способов организации механизмов защиты.

Задачей управления является обеспечение рационального использования созданных механизмов защиты в процессе обработки защищаемой информации.

12.1. Принцип комплексного подхода к обеспечению информационной безопасности

Принцип комплексного подхода к обеспечению информационной безопасности на сегодня – безопасность информации предусматривается уже на этапе проектирования, внедрения и поддержки.

Наиболее перспективной основой для построения систем информационной безопасности – это рациональное сочетание различных организационных и программно-технических мер и средств с учетом требований действующих нормативно-правовых и нормативно-технических документов.

При создании комплексной системы необходимо защищать информацию во всех фазах ее существования – как электронной (содержащейся и обрабатываемой в автоматизированных системах или на машинных носителях), так и документальной (бумажные документы). В комплексной системе защищать информацию необходимо не только от несанкционированного доступа к ней, но и от несанкционированного вмешательства в процесс ее обработки, хранения и передачи, попыток нарушения работоспособности программно-технических средств и т.п.

В основе реализации комплексного подхода к обеспечению информационной безопасности сегодня лежат еще два принципа.

Первый принцип состоит в том, что абсолютно надежную, «непробиваемую» защиту создать практически невозможно, поскольку необходимо разумное соотношение затрат на защиту информации и возможных финансовых потерь от нарушения информационной безопасности. Естественно, первое напрямую зависит от финансовых возможностей предприятия.

Важно также и то, какие затраты должен понести злоумышленник, чтобы «вскрыть» систему, и как они соотносятся с ценностью и актуальностью хранимой в ней информации. Правильно построенные системы должны требовать от злоумышленника таких затрат времени или денег на «вскрытие», чтобы эта операция оказывалась бессмысленной с практической точки зрения.

Второй принцип предполагает, что система должна быть гибкой и легко адаптироваться к изменяющимся внешним условиям. Поскольку угрозы информационной безопасности постоянно становятся все изощреннее, в системе должен быть заложен определенный запас прочности как в части программно-технических средств, так и части организационных мер безопасности.

Комплексный подход при создании систем информационной безопасности предполагает, наряду с применением технических средств защиты, решение вопросов упорядочивания и управления ИБ на базе единой интегрированной архитектуры системы информационной безопасности, которая реализует следующие принципы:

- соответствие существующим положениям по информационной безопасности;
- интегрирование всех необходимых подсистем, комплексов и технических средств;
- универсальность, гибкость и масштабируемость архитектуры, ее полная управляемость;
- возможность варьировать состав и наполнение комплексов и подсистем;
- обеспечение минимальной совокупной стоимости всей защиты.

В целом комплексный подход предполагает защиту всей информационной инфраструктуры предприятия от любых несанкционированных действий, поэтому очень важно, как с методической точки зрения будет организована разработка такой системы.

К настоящему времени сложилась вполне определенная последовательность разработки комплексных систем обеспечения информационной безопасности, которая включает в себя несколько рассмотренных ниже этапов. Наиболее важные этапы в области комплексной информационной безопасности:

• проектирование, внедрение и сопровождение систем информационной безопасности, обеспечивающих безопасность функционирования ИТ-ресурсов компании;

• комплексное диагностическое обследование, оценка и аудит систем информационной безопасности, в том числе на соответствие существующим стандартам.

12.2. Основные направления и этапы работ по созданию комплексной системы безопасности

В общем случае создание комплексной системы безопасности проводится в рамках трех направлений работ – методологическом, организационном и техническом.

Основной задачей методологического направления является разработка концепции (политики) безопасности предприятия. Концепция безопасности представляет собой документ, который, в частности, определяет:

• состав и особенности информационных потоков организации;

• виды представления информации для каждого информационного потока (например, бумажный документ, электронный документ, запись в базе данных и др.);

• категории конфиденциальной информации в организации и классификацию информации по категориям конфиденциальности;

• возможные пути разглашения конфиденциальной информации (модель угроз);

• модель нарушителя для каждой угрозы, в т.ч. профессиональный круг лиц, к которому может принадлежать нарушитель, мотивацию и цели действий нарушителя, предполагаемая квалификация нарушителя и характер его возможных действий;

• вероятности реализации каждого вида угроз и усредненные вероятные величины убытков (риски).

В рамках организационного направления работ создается совокупность правил, регламентирующих деятельность сотрудников при обращении с информацией независимо от форм ее представления. Эта совокупность правил отражается в руководящих документах, составляющих регламент обеспечения безопасности.

Регламент обеспечения безопасности, в частности, определяет правила обращения с конфиденциальной информацией в зависимости от фазы ее обработки и категории конфиденциальности:

• порядок допуска сотрудников к конфиденциальной информации;

• обязанности и ограничения, накладываемые на сотрудников, допущенных к конфиденциальной информации;

• порядок изменения категории конфиденциальности работ и информации;

• требования к помещениям, в которых проводятся конфиденциальные работы и обрабатывается конфиденциальная информация в соответствии с ее категориями;

• требования к конфиденциальному делопроизводству;

• требования к учету, хранению и обращению с конфиденциальными документами;

• меры по контролю за обеспечением конфиденциальности работ и информации;

• порядок действий, предпринимаемых при обнаружении разглашения информации с целью пресечения процесса разглашения/утечки (план мероприятий по противодействию атаке на конфиденциальную информацию);

• порядок действий, предпринимаемых после пресечения процесса разглашения/утечки информации (план мероприятий по восстановлению конфиденциальности информации);

• меры ответственности за разглашение конфиденциальной информации.

В состав регламента безопасности могут входить как собственно концепция безопасности, так и целый ряд дополнительных документов, например, инструкции по пропускному и внутриобъектовому режиму, инструкции по системе разграничения доступа, инструкции по работе с кадрами и др. Эти документы должны определять порядок функционирования комплексной системы информационной безопасности как в штатном режиме, так и в аварийных ситуациях.

В рамках технического направления реализуется комплекс программно-технических средств комплексной системы обеспечения информационной безопасности. Здесь возможны два основных варианта — разработка всей информационной системы «с нуля» с учетом требований информационной безопасности или встраивание элементов защиты в уже существующую информационную систему.

Хронологически процесс разработки комплексной системы информационной безопасности включает несколько этапов, которые включают предпроектную стадию, стадию проектирования и разработки системы, стадию внедрения (опытная эксплуатация, приемо-сдаточные испытания и аттестация системы по установленным правилам), а также стадию эксплуатации и модернизации системы.

Функционально процесс разработки системы безопасности можно представить последовательностью этапов информационного обследования, разработки организационно-распорядительных документов, приобретения, установки и настройки программно-технических средств защиты, ввода системы в эксплуатацию. В ходе эксплуатации системы, как правило, проводится ее модернизация в соответствии с изменяющимися внешними условиями.

Основными этапами создания комплексной системы защиты информации должны быть:

– *обследование организации* – выполнение работ по аудиту информационной безопасности может быть как внутренними силами, так и с привлечением сторонней организации;

– *проектирование системы защиты информации* – выполняется по результатам проведенного аудита информационной безопасности;

– *внедрение системы защиты информации* – осуществляется, как правило, силами сторонней организации при участии сотрудников отдела информационной безопасности для обеспечения контроля качества;

– *сопровождение системы информационной безопасности* – осуществляется силами сторонней организации, а эксплуатация и администрирование безопасности силами отдела ИБ;

– *обучение специалистов по защите информации* – проводится в плановом порядке по графику, утвержденному руководством.

12.3. Основные подсистемы программно-технической реализации комплексной защиты информации

Техническая составляющая должна включать следующие подсистемы:

– подсистему антивирусной защиты;

– подсистему резервного копирования и архивирования;

– подсистему защиты электронной почты;

– подсистемы обнаружения атак;

– подсистемы управления информационной безопасности, централизованного мониторинга и аудита событий ИБ;

– подсистемы защиты каналов передачи данных;

– подсистемы управления доступом (идентификации и аутентификации пользователей);

– подсистему регистрации и учета;

– подсистему обеспечения целостности;

– подсистему защиты информации в ЛВС филиалов и дочерних обществ.

Подсистема антивирусной защиты

Эта подсистема должна соответствовать следующим требованиям:

– должен быть организован мониторинг антивирусной активности;

– желательно организовать двухуровневую антивирусную защиту с применением антивирусного ПО различных производителей;

– должна быть обеспечена антивирусная защита серверного оборудования.

Подсистема резервного копирования и архивирования

Эта подсистема должна соответствовать следующим требованиям:

– необходимо создать соответствующие документы и инструкции, регламентирующие процесс резервного копирования и архивирования и связанные с производственной необходимостью;

– организовать резервное копирование для всех серверов, указанных в регламентах резервного копирования;

– разработать процедуры и регулярно проводить тестирование резервных копий.

Подсистема защиты электронной почты

Эта подсистема должна соответствовать следующим требованиям:

– должны быть задействованы механизмы защищенного почтового обмена внутри ЛВС, должна быть обеспечена аутентификация пользователей при отправке почты;

– почтовый сервер для приема внешней электронной почты должен быть выделен в демилитаризованную зону.

Подсистема обнаружения атак

В целях контроля и оперативного реагирования на выполнение несанкционированных операций в сегменте сопряжения и серверных сегментах ЛВС рекомендуется внедрить систему IDS\IPS. Подсистема обнаружения атак (ПОА) предназначена для своевременного обнаружения атак на узлы сети.

В состав подсистемы входят:

– сервер управления подсистемой;

– сетевой и серверные сенсоры обнаружения атак;

– телекоммуникационное оборудование.

Сервер управления подсистемой выполняет следующие функции:

– централизованное управление сенсорами обнаружения атак;

– централизованное обновление баз данных сигнатур;

– централизованное получение данных с сенсоров обнаружения атак;

– хранение зафиксированных событий за определенный промежуток времени.

Сенсоры обнаружения атак выполняют следующие функции:

– обнаружение враждебной деятельности и распознавание атак на узлы сети;

– обработка сетевого трафика на основе заданной политики и имеющейся базы данных сигнатур атак;

– захват сетевого трафика.

Телекоммуникационное оборудование выполняет роль «агента», который передает необходимый сетевой трафик на сенсор. При этом исполь-

зуется технология SPAN (Switch Port Analyzer), которая позволяет передать на сенсор копию сетевого трафика необходимого сегмента сети.

Подсистема управления информационной безопасностью, централизованного мониторинга и аудита событий

Для организации мониторинга, определения и своевременного реагирования на угрозы ИБ рекомендуется внедрение подсистемы управления ИБ, централизованного мониторинга и аудита событий ИБ.

В состав подсистемы входят:

1) ПАК мониторинга и аудита выполняет функцию сбора событий безопасности с сетевых устройств и агентов (с помощью технологии NetFlow);

2) ПАК управления подсистемой мониторинга и аудита выполняет следующие функции:

– управления ПАК мониторинга и аудита;

– интеграции собранных с ПАК мониторинга и аудита данных о событиях безопасности;

– оперативного оповещения об инцидентах безопасности;

– генерации сводных отчётов с рекомендациями по управлению ИБ.

Подсистема защиты каналов передачи данных

В целях обеспечения защиты передаваемых данных рекомендуется организовать соединения VPN, что позволит значительно увеличить безопасность существующих внешних информационных потоков для внешних организаций. В дальнейшем подсистема может также послужить основой для организации защищенного мобильного доступа сотрудников.

В состав подсистемы входят:

1) маршрутизатор с функциями шлюза VPN, который выполняет следующие основные функции:

– поддержку межсетевого взаимодействия с удалёнными подразделениями;

– защиту транзитного трафика между удалёнными пользователями и узлами сети;

– защиту трафика самого маршрутизатора;

– пакетную фильтрацию трафика.

2) программные агенты VPN, установленные на АРМ удалённых пользователей, которые выполняют следующие функции:

– защиту транзитного трафика между удалёнными пользователями и узлами сети;

– пакетную фильтрацию трафика.

Подсистема идентификации и аутентификации пользователей

Для централизации управления аутентификационной информацией, а также для обеспечения соответствия АС требованиям нормативных доку-

ментов РФ, рекомендуется внедрять подсистему идентификации и аутентификации пользователей.

Подсистема обеспечивает:

– индивидуальную идентификацию и аутентификацию пользователей при доступе к информационным ресурсам;

– поддержку различных методов аутентификации, в т. ч. предлагаемый метод с использованием сертификатов открытых ключей;

– возможность использования различных электронных ключевых носителей (eToken), в т. ч. предлагаемых на пластиковых смарт-картах;

– использование компонент подсистемы для организации подсистемы защищённой электронной почты;

– возможность оперативного контроля за процессом предоставления доступа ко всем важным приложениям и ресурсам организации;

– эффективное управление правами доступа и идентификацией пользователей информационных систем;

– применение пользователями одного пароля для идентификации для многих приложений и ресурсов;

– ведение статистики использования информационных ресурсов, подготовка отчетов, проведение аудитов.

Подсистема регистрации и учета

Должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС.

Должна осуществляться регистрация выдачи печатных (графических) документов на "твердую" копию.

Должна осуществляться регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов.

Должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам.

Должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей.

Должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку).

Учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема).

Должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется однократной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов).

Подсистема обеспечения целостности

Должна быть обеспечена целостность программных средств СЗИ НСД, а также неизменность программной среды.

Должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая контроль доступа в помещения АС посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АС и хранилище носителей информации, особенно в нерабочее время.

Должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест-программ, имитирующих попытки НСД.

Должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности.

Подсистема защиты информации в ЛВС филиалов и дочерних обществ

Учитывая то, что ЛВС филиалов и дочерних обществ газотранспортного предприятия в большинстве случаев подключены к РСПД предприятия, необходимо определить общие требования к системе ИБ филиала:

– ЛВС филиала должна подключаться к РСПД через систему межсетевого экранирования;

– системы защиты информации прикладных информационных систем, функционирующих в филиале, должны работать под управлением единого сервера безопасности филиала;

– элементы АСУ ТП, функционирующие в филиале для обеспечения надежной передачи технологической информации должны иметь несколько резервных каналов связи;

– система ЗИ от НСД филиала должна соответствовать требования по классу защищенности 1Г в соответствии с методическими документами Гостехкомиссии России.

На стадии проектирования и создания объекта информатизации и СЗИ в его составе на основе предъявляемых требований и заданных заказчиком ограничений на финансовые, материальные, трудовые и временные ресурсы осуществляются:

– разработка раздела технического проекта на объект информатизации в части защиты информации;

– строительно-монтажные работы в соответствии с проектной документацией, размещением и монтажом технических средств и систем;

– разработка организационно-технических мероприятий по защите информации в соответствии с предъявляемыми требованиями;

– закупка сертифицированных образцов и серийно выпускаемых в защищенном исполнении технических средств обработки, передачи и хранения информации, либо их сертификация;

– закупка сертифицированных технических, программных и программно-технических (в т.ч. криптографических) средств защиты информации и их установка;

– разработка (доработка) или закупка и последующая сертификация по требованиям безопасности информации программных средств защиты информации в случае, когда на рынке отсутствуют требуемые сертифицированные программные средства;

– организация охраны и физической защиты помещений объекта информатизации, исключающих несанкционированный доступ к техническим средствам обработки, хранения и передачи информации, их хищение и нарушение работоспособности, хищение носителей информации;

– разработка и реализация разрешительной системы доступа пользователей и эксплуатационного персонала к обрабатываемой (обсуждаемой) на объекте информатизации информации;

– определение заказчиком подразделений и лиц, ответственных за эксплуатацию средств и мер защиты информации, обучение назначенных лиц специфике работ по защите информации на стадии эксплуатации объекта информатизации;

– выполнение генерации пакета прикладных программ в комплексе с программными средствами защиты информации;

– разработка эксплуатационной документации на объект информатизации и средства защиты информации, а также организационно-распорядительной документации по защите информации (приказов, инструкций и других документов);

– выполнение других мероприятий, специфичных для конкретных объектов информатизации и направлений защиты информации.

На стадии ввода в действие объекта информатизации осуществляются:

– опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе объекта информатизации и отработки технологического процесса обработки (передачи) информации;

– аттестация объекта информатизации по требованиям безопасности информации.

На этой стадии оформляются:

– акты внедрения средств защиты информации по результатам их испытаний;

– предъявительский акт к проведению аттестационных испытаний;

– заключение по результатам аттестационных испытаний.

С целью своевременного выявления и предотвращения утечки информации по техническим каналам, исключения или существенного затруднения несанкционированного доступа и предотвращения специальных программно-технических воздействий, вызывающих нарушение целостности информации или работоспособность технических средств в учреждении (на предприятии), проводится периодический (не реже одного раза в год) контроль состояния защиты информации.

Контроль осуществляется службой безопасности (предприятия).

При необходимости по решению руководителя предприятия в местах размещения средств обработки информации могут проводиться работы по обнаружению и изъятию «закладок», предназначенных для скрытого перехвата защищаемой информации.

Такие работы могут проводиться организациями, имеющими соответствующие лицензии ФСТЭК России на данный вид деятельности.

Протоколирование и аудит

Под протоколированием понимается сбор и накопление информации о событиях, происходящих в информационной системе предприятия. У каждого сервиса свой набор возможных событий, но в любом случае их можно подразделить на внешние – вызванные действиями других сервисов, внутренние – вызванные действиями самого сервиса, и клиентские – вызванные действиями пользователей и администраторов.

Аудит – это анализ накопленной информации, проводимый оперативно, почти в реальном времени, или периодически.

Реализация протоколирования и аудита преследует следующие главные цели:

– обеспечение подотчетности пользователей и администраторов;

– обеспечение возможности реконструкции последовательности событий;

– обнаружение попыток нарушений информационной безопасности;

– предоставление информации для выявления и анализа проблем.

Обеспечение подотчетности важно в первую очередь как средство сдерживания. Если пользователи и администраторы знают, что все их действия фиксируются, они, возможно, воздержатся от незаконных операций. Если есть основания подозревать какого-либо пользователя в нечестности, то можно регистрировать его действия особенно детально, вплоть до каждого нажатия клавиши. При этом обеспечивается не только возможность

расследования случаев нарушения режима безопасности, но и откат некорректных изменений. Тем самым обеспечивается целостность информации.

Реконструкция последовательности событий позволяет выявить слабости в защите сервисов, найти виновника вторжения, оценить масштабы причиненного ущерба и вернуться к нормальной работе.

Выявление и анализ проблем позволяют помочь улучшить такой параметр безопасности, как доступность. Обнаружив узкие места, можно попытаться переконфигурировать или перенастроить систему, снова измерить производительность и т.д.

ЗАКЛЮЧЕНИЕ

Острота проблемы защиты информационных технологий в современных условиях определяется следующими факторами:

– высокими темпами роста парка средств вычислительной техники и связи, расширением областей использования ЭВМ, многообразием и повсеместным распространением информационно-управляющих систем, подлежащих защите;

– вовлечением в процесс информационного взаимодействия все большего числа людей и организаций, резким возрастанием их информационных потребностей;

– повышением уровня доверия к автоматизированным системам управления и обработки информации, использованием их в критических технологиях;

– отношением к информации, как к товару, переходом к рыночным отношениям, с присущей им конкуренцией и промышленным шпионажем, в области создания и сбыта (предоставления) информационных услуг;

– концентрацией больших объемов информации различного назначения и принадлежности на электронных носителях;

– наличием интенсивного обмена информацией между участниками этого процесса;

– количественным и качественным совершенствованием способов доступа пользователей к информационным ресурсам;

– обострением противоречий между объективно существующими потребностями общества в расширении свободного обмена информацией и чрезмерными или наоборот недостаточными ограничениями на ее распространение и использование;

– дифференциацией уровней потерь (ущерба) от уничтожения, фальсификации, разглашения или незаконного тиражирования информации (уязвимости различных затрагиваемых субъектов);

– многообразием видов угроз и возможных каналов несанкционированного доступа к информации;

– ростом числа квалифицированных пользователей вычислительной техники и возможностей по созданию ими программно-математических воздействий на систему;

– развитием рыночных отношений (в области разработки, поставки, обслуживания вычислительной техники, разработки программных средств, в том числе средств защиты).

Естественно, в такой ситуации возникает потребность в защите вычислительных систем и информации от несанкционированного доступа, кражи, уничтожения и других преступных и нежелательных действий.

Наблюдается большая разнородность целей и задач защиты – от обеспечения государственной безопасности до защиты интересов отдельных организаций, предприятий и частных лиц, дифференциация самой информации по степени ее уязвимости.

Общеизвестно, что создать абсолютно надежную систему защиты невозможно. При достаточном количестве времени и средств можно преодолеть любую защиту, поэтому можно говорить только о некотором достаточном уровне безопасности, обеспечении такого уровня защиты, когда стоимость ее преодоления становится больше стоимости получаемой при этом информации (достигаемого эффекта), или когда за время получения информации она обесценивается настолько, что усилия по ее получению теряют смысл.

НОРМАТИВНО-ПРАВОВЫЕ ДОКУМЕНТЫ

Законы РФ

1. Конституция Российской Федерации (1993 г.).

2. О безопасности: Закон РФ от 05.03.1992 г. № 2446-1.

3. О государственной тайне: Закон РФ от 21.07.1993 г. № 5485-1 (с изм. и доп., вступившими в силу с 15.12.2007).

4. Об информации, информационных технологиях и о защите информации: ФЗ РФ от 27.07.2006 г. № 149-ФЗ.

5. О коммерческой тайне: ФЗ РФ от 29 июля 2004 г. № 98-ФЗ.

6. О персональных данных: ФЗ РФ от 27 июля 2006 г. № 152-ФЗ.

7. Об электронной цифровой подписи: ФЗ РФ от 10 января 2002 г. № 1-ФЗ.

8. О правовой охране программ для ЭВМ и баз данных: ФЗ РФ от 23 сентября 1992 г. № 3523-1.

9. О федеральных органах правительственной связи и информации: ФЗ РФ от 19 февраля 1993 г. № 4524-1.

10. Об органах Федеральной Службы Безопасности в Российской Федерации: ФЗ РФ от 03.04.95 № 40-ФЗ (СЗ № 15-95 г. ст. 1269).

11. О лицензировании отдельных видов деятельности": ФЗ РФ от 8 августа 2001 г., № 128-ФЗ.

12. О техническом регулировании: ФЗ РФ от 27 декабря 2002 г. № 184-ФЗ.

13. О сертификации продукции и услуг: ФЗ РФ от 10 июня 1993 г. № 5151-1.

14. О техническом регулировании: ФЗ РФ от 27 декабря 2002 г. № 184-ФЗ.

15. О внесении изменений в Федеральный закон "О персональных данных": ФЗ РФ от 25 июля 2011 г. № 261-ФЗ.

16. О внесении изменений в ст. 25 ФЗ "О персональных данных": от 23 декабря 2010 г. № 359-ФЗ.

17. Об участии в международном информационном обмене: ФЗ РФ № 86-ФЗ от 30.06.2003.

18. О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных: ФЗ РФ от 19 декабря 2005 г. № 160-ФЗ.

19. О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона "Об электронной подписи": ФЗ от 06.04.2011 № 65-ФЗ.

20. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (в ред. Федерального закона от 5 апреля 2013 № 59-ФЗ).

21. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ (ред. Федерального закона от 5 апреля 2013 г. № 33-ФЗ).

22. Трудовой кодекс Российской Федерации от 30 декабря 2001 г. № 197-ФЗ (в ред. Федерального закона от 5 апреля 2013 г. № 60-ФЗ и от 5 апреля 2013 г. № 58-ФЗ).

23. Гражданский кодекс Российской Федерации (Ч. 1) от 30 ноября 1994 № 51-ФЗ (в ред. от 11 февраля 2013 г.) – ст. 150, 151, 152.

Правовые акты Президента РФ

1. Об основах государственной политики в сфере информатизации: Указ Президента РФ № 170 от 20.01.94 г.

2. Вопросы Межведомственной комиссии по защите государственной тайны: Указ Президента РФ от 6 октября 2004 г. № 1286.

3. О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена: Указ Президента РФ от 17 марта 2008 г. № 351.

4. Об утверждении перечня сведений конфиденциального характера: Указ Президента РФ от 6 марта 1997 г. № 188.

5. Концепция национальной безопасности Российской Федерации: Указ Президента РФ от 17 декабря 1997 г. № 1300 в редакции Указа Президента РФ от 10 января 2000 г. № 24.

6. Об утверждении перечня сведений, отнесенных к государственной тайне: Указ Президента РФ от 30 ноября 1995 г. № 1203.

7. Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела: Указ Президента РФ от 30 мая 2005 г. № 609.

8. О Концепции правовой информатизации России: Указ Президента РФ от 28 июня 1993 г. № 966.

9. Об основах государственной политики в сфере информатизации: Указ Президента РФ от 20 января 1994 г. № 170.

10. О дополнительных гарантиях прав граждан на информацию: Указ Президента РФ от 31 декабря 1993 г. № 2334.

Постановления Правительства РФ

1. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: Постановление Правительства РФ от 01 ноября 2012 № 1119 // СЗ РФ. – 2012. – № 45. – Ст. 6257.

2. Об утверждении Положения о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам: Постановление Совета Министров – Правительства РФ от 15.09.1993 № 912-51.

3. 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: Постановление Правительства РФ от 15 апреля 1995 г. № 333.

4. Положение о сертификации средств защиты информации: Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 (с изменениями и дополнениями от 23 апреля 1996 г. № 509; от 29 марта 1999 г. № 342; от 17 декабря 2004 г. № 808).

5. Об организации лицензирования отдельных видов деятельности: Постановление Правительства РФ от 26.01.2006г. № 45.

6. Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти: Постановление Правительства РФ от 3 ноября 1994 г. № 1233.

7. О лицензировании деятельности по технической защите конфиденциальной информации: Постановление Правительства РФ от 15.08.06 № 504.

8. Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных: Постановление Правительства РФ от 17.11.2007 № 781.

9. Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами: Постановление Правительства Российской Федерации от 29 декабря 2007 г. № 957.

Основные национальные стандарты в области защиты информации

1. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.
2. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью.
3. ГОСТ Р ИСО 7498-2-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель.
4. ГОСТ Р 51241-2008. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний.
5. ГОСТ Р 50.1.053-2005. Информационные технологии. Основные термины и определения в области технической защиты информации.
6. ГОСТ Р 51188-98. Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство.
7. ГОСТ Р 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
8. ГОСТ Р ИСО/МЭК 15408-1-2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 1. Введение и общая модель.
9. ГОСТ Р ИСО/МЭК 15408-2-2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 2. Функциональные требования безопасности.
10. ГОСТ Р ИСО/МЭК 15408-3-2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 3. Требования доверия к безопасности.
11. ГОСТ Р ИСО/МЭК 15408. Общие критерии оценки безопасности информационных технологий.
12. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.
13. ГОСТ Р 51898-2002. Аспекты безопасности. Правила включения в стандарты.

Международные стандарты

1. BS 7799-1:2005 – Британский стандарт BS 7799. Ч. 1. BS 7799 Part 1 – Code of Practice for Information Security Management.
2. BS 7799-2:2005 – Британский стандарт BS 7799. Ч. 2. BS 7799 Part 2 – Information Security management – specification for information security

management systems (Спецификация системы управления информационной безопасностью).

3. BS 7799-3:2006 – Британский стандарт BS 7799. Ч. 3. Новый стандарт в области управления рисками информационной безопасности.

4. ISO/IEC 17799:2005. Информационные технологии – Технологии безопасности – Практические правила менеджмента информационной безопасности.

5. ISO/IEC 27000. Словарь и определения.

6. ISO/IEC 27001:2005. Информационные технологии – Методы обеспечения безопасности – Системы управления информационной безопасностью – Требования.

7. ISO/IEC 17799:2006.

8. BS 7799-3:2006. Руководство по менеджменту рисков ИБ.

9. German Information Security Agency. IT Baseline Protection Manual – Standard security safeguards (Руководство по базовому уровню защиты информационных технологий).

ЛИТЕРАТУРА

1. Основы информационной безопасности : учеб. пособие / В. А. Челухин. – Комсомольск-на-Амуре : ГОУВПО «КнАГТУ», 2010. – 185 с.

2. Войтик, А. И. Экономика информационной безопасности : учеб. пособие / А. И. Войтик, В. Г. Прожерин. – СПб. : НИУ ИТМО, 2012. – 120 с.

3. Петров, И. С. Локализация и ослабление побочных электромагнитных излучений от средств вычислительной техники путем экранирования электромагнитных волн / И. С. Петров // Вестник ЮУрГУ. Серия «Компьютерные технологии, управление, радиоэлектроника». – 2012. – № 23. – С. 189-191.

4. Малюк, А. А. Теория защиты информации / А. А. Малюк. – М. : Горячая линия-Телеком, 2012. – 184 с.

5. Комплексная защита информации в корпоративных системах : учеб. пособие / В. Ф Шаньгин. – М. : ИД «ФОРУМ» : ИНФРА-М, 2010. – 592 с.

6. Родичев, Ю. Информационная безопасность: нормативно-правовые аспекты / Ю. Родичев. – СПб. : Питер, 2008. – 272 с.

7. Щербаков, А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты / А. Ю. Щербаков. – М. : Книжный мир, 2009. – 352 с.

8. Грязнов, Е. С. Безопасность локальных сетей / Е. С. Грязнов, С. А. Панасенко. – М. : Вузовский учебник, 2006. – 525 с.

9. Силаенков, А. Н. Проектирование системы информационной безопасности : учеб. пособие / А. Н Силаенков. – Омск : Изд-во ОмГТУ, 2009. – 128 с.

10. Попов, К. И. Правовые основы противодействия преступлениям в сфере компьютерной информации в сети Интернет / К. И. Попов, В. Майорова // Вестник УрФО. Безопасность в информационной сфере. – № 3(9). – 2013. – С. 38.

11. Косенко, М. Ю. Сбор информации при проведении тестирования на проникновение / М. Ю. Косенко // Вестник УрФО. Безопасность в информационной сфере. – № 3(9).– 2013. – С. 11.

12. Косенко, М. Ю. Злонамеренное использование облачных технологий / М. Ю. Косенко // Труды Первой Международной конференции «Информационные технологии и системы». – 2012. – С. 67–69.

13. Информационные технологии в юридической деятельности : учебник для бакалавров / под общ. ред. проф. П. У. Кузнецова. – М. : Юрайт, 2011. – С. 73.

Дополнительная литература

1. Тедеев, А. А. Информационное право : учебник / А. А Тедеев. – М. : Эксмо, 2005, С. 75.

2. Швецова, Н. Д. Системы технической безопасности: актуальные реалии / Н. Д. Швецова. – СПб. : Питер, 2004. – 340 с.

3. Соколов, Д. Н. Защита от компьютерного терроризма / Д. Н. Соколов, А. Д. Степанюк. – М. : БХВ-Петербург, Арлит, 2002. – 456 с.

4. Сыч, О. С. Комплексная антивирусная защита локальной сети / О. С. Сыч. – М. : Финансы и статистика, 2006. – 736 с.

5. Козлачков, П. С. Основные направления развития систем информационной безопасности / П. С. Козлачков. – М. : Финансы и статистика, 2004. – 736 с.

6. Скиба, В. Ю. Руководство по защите от внутренних угроз информационной безопасности / В. Ю. Скиба, В. А. Курбатов. – СПб. : Питер, 2008. – 320 с.

7. Галатенко, В. А. Стандарты информационной безопасности / В. А. Галатенко. – М. : Интернет-университет информационных технологий, 2006. – 264 с.

8. Леваков, Г. Н. Анатомия информационной безопасности / Г. Н. Леваков. – М. : ТК Велби, Проспект, 2004. – 256 с.

9. Бузов, Г. А. Защита от утечки информации по техническим каналам / Г. А. Бузов, С. В. Калинин, А. В. Кондратьев. – М. : Горячая линия-Телеком, 2005. – 416 с.

Иностранная литература

1. Thomas Wilhelm. “Professional Penetration Testing: Creating and Operating a Formal Hacking Lab”.Syngress, 2009.

2. Pete Herzog. “Open-Source Security Testing Methodology Manual”. ISECOM, 2006.

3. Karen Scarfone, Murugiah Souppaya, Amanda Cody, Angela Orebaugh. “Technical Guid toInformation Security Testing and Assessment”. NIST Special Publication 800-115.

4. M. Allman, V. Paxson, and J. Terrell. “A brief history of scanning”. In IMC ‘07: Proceedings of the 7th ACM SIGCOMM conference on Internet measurement, New York, 2007, pp 77–82.

5. Richard J Barnett, Barry Irwin. “Towards a Taxonomy of Network Scanning Techniques”. In SAICSIT, 2008.

6. Douglas E. Comer, David L. Stevens. “Internetworking with TCP/IP. Vol III. Client-Server Programming and Applications Linux/POSIX Socket Version”. Addison-Wesley, 2000.

7. Gordon Lyon. “Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning”. Nmap Project, 2009.

8. James Messer. “Secrets of Network Cartography: A Comprehensive Guide to Nmap”.

9. Chris McNab. “Network Security Assessment”. O’Reilly Media, Second Edition, 2007.

10. “Penetration Testing: Procedures & Methodologies”. EC-Council, 2010.

Электронные ресурсы

1. Искусство кибервойны: НАТО выпустила руководство для хакеров // Интернет-портал ТВ-новости. URL: http://russian.rt.com/article/5929 (дата обращения: 15.09.2013 г.).

2. Лаборатория Касперского. URL: http://www.Kaspersky.ru, Kaspersky Internet Security, Kaspersky Anti-Virus.

3. Журнал «Information Security». URL: http://www.itsec.ru/articles2/allpubliks.

4. Книга «Обеспечение информационной безопасности бизнеса». URL: http://www.proklondike.com/books/defence/andrianov_infobez_biz_2011.html.

5. Книга «Комплексная система защиты информации на предприятии». URL: http://www.proklondike.com/books/defence/gribunin_komplex_zaschita_na_predpriatiy_2009.html.

6. Журнал «Информационная безопасность банков». URL: http://www.journal.ib-bank.ru

7. Журнал «Защита информации». URL: http://www.inside-zi.ru.

8. Документы по информационной безопасности. URL: http://www.trinosoft.com/index.php?page=is.

9. U.S. National Security Strategy 2010 // National Strategy Forum. URL: http://www.nationalstrategy.com/NSFReview/Winter2009Vol19No1USNSS2010.aspx (дата обращения: 15.09.2013 г.).

Учебное издание

Челухин Владимир Алексеевич

КОМПЛЕКСНОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Учебное пособие

Научный редактор – кандидат технических наук,
доцент И. А. Трещев

Редактор Е. В. Безолукова

Подписано в печать 31.10.2014.
Формат 60 × 84 1/16. Бумага 65 г/м^2. Ризограф EZ570E.
Усл. печ. л. 12,32. Уч.-изд. л. 12,00. Тираж 100 экз. Заказ 26561.

Редакционно-издательский отдел
Федерального государственного бюджетного образовательного
учреждения высшего профессионального образования
«Комсомольский-на-Амуре государственный технический университет»
681013, Комсомольск-на-Амуре, пр. Ленина, 27.

Полиграфическая лаборатория
Федерального государственного бюджетного образовательного
учреждения высшего профессионального образования
«Комсомольский-на-Амуре государственный технический университет»
681013, Комсомольск-на-Амуре, пр. Ленина, 27.