Министерство образования и науки Российской Федерации
ФГАОУ ВПО «Российский государственный
профессионально-педагогический университет»
Учреждение Российской академии образования
«Уральское отделение»

А. А. Шайдуров

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Учебное пособие

Допущено Научно-методическим советом по информатике, вычислительной технике и компьютерным технологиям Учебно-методического объединения по профессионально-педагогическому образованию в качестве учебного пособия для студентов высших учебных заведений, обучающихся по специальности 050501.06 Профессиональное обучение (информатика, вычислительная техника и компьютерные технологии)

Екатеринбург
РГППУ
2010

УДК 316.776(075.8)
ББК С 843в61я73-1
Ш 17

Шайдуров А. А. Информационная безопасность и защита информации [Текст]: учеб. пособие / А. А. Шайдуров. Екатеринбург: Изд-во Рос. гос. проф.-пед. ун-та, 2010. 130 с.
ISBN 978-5-8050-0391-3

В пособии рассмотрены основные теоретические и практические моменты дисциплины «Информационная безопасность и защита информации», приемы обеспечения безопасности хранения документов на электронных носителях и методы сохранения конфиденциальности, целостности и доступности информации.

Учебное пособие адресовано студентам специальности 050501.06 Профессиональное обучение (информатика, вычислительная техника и компьютерные технологии).

Рецензенты: доктор педагогических наук, профессор Т. А. Матвеева (ГОУ ВПО «Уральский государственный технический университет – УПИ имени первого Президента России Б. Н. Ельцина»); кандидат педагогических наук, доцент Е. В. Чубаркова (ФГАОУ ВПО «Российский государственный профессионально-педагогический университет»)

ISBN 978-5-8050-0391-3

Содержание

Введение

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

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

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

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

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

Поэтому современному документоведу и специалисту антикризисного управления важно знать безопасные приемы труда в информационном пространстве. И это пособие призвано помочь студентам освоить приемы обеспечения безопасности хранения документов на электронных носителях и методы сохранения конфиденциальности, целостности и доступности информации.

В пособии рассмотрены нормативно-правовые основы обеспечения информационной безопасности, существенное внимание уделено основополагающим нормативным документам, определяющим порядок использования различной информации, а также ответственность за соответст-

вующие нарушения. Кроме этого, проанализированы основные угрозы информационной безопасности в контексте ее составляющих. Рассмотрена проблема защиты автоматизированных информационных систем от программных вирусов. В соответствии с приведенной классификацией компьютерных вирусов и вирусоподобных программ изложены основные способы противодействия их проникновению в компьютеры пользователей.

Описаны наиболее частые угрозы конфиденциальности и целостности информации в локальных вычислительных сетях, а в территориально распределенных сетях – угрозы нарушения доступности информации.

Раскрыты наиболее значимые механизмы защиты вычислительных систем от несанкционированных действий как преднамеренного, так и непреднамеренного характера.

Для повышения качества контроля знаний в конце каждой главы пособия приводятся вопросы и задания для самоконтроля.

Учебное пособие соответствует государственному образовательному стандарту по подготовке студентов высших профессионально-педагогических учебных заведений.

Глава 1. ИНФОРМАЦИОННЫЕ РЕСУРСЫ

1.1. Понятие информации

1.2. Информационные ресурсы: определение, классификация и характеристика их основных свойств; информационные ресурсы в условиях рыночных отношений

1.3. Документы как один из классов информационных ресурсов. Обобщенная модель документа. Основные барьеры доступа к документальным информационным ресурсам

1.1. Понятие информации

Существует три основные интерпретации понятия «информация».

Научная интерпретация. Информация – исходная общенаучная категория, отражающая структуру материи и способы ее познания, несводимая к другим, более простым понятиям.

Абстрактная интерпретация. Информация – некоторая последовательность символов, которые несут как вместе, так в отдельности некоторую смысловую нагрузку для исполнителя.

Конкретная интерпретация. В данной плоскости рассматриваются конкретные исполнители с учетом специфики их систем команд и семантики языка. Так, например, для машины информация – нули и единицы; для человека – звуки, образы.

Существуют несколько концепций (теорий) информации.

Первая концепция (концепция К. Шеннона), отражая количественно-информационный подход, определяет информацию как меру неопределенности (энтропию) события. Количество информации в том или ином случае зависит от вероятности его получения: *чем более вероятным является сообщение, тем меньше информации содержится в нем.*

Вторая концепция рассматривает информацию как свойство (атрибут) материи. Ее появление связано с развитием кибернетики и основано на утверждении, что *информацию содержат любые сообщения, воспринимаемые человеком или приборами.* Наиболее ярко и образно эта концепция информации выражена академиком В. М. Глушковым.

Третья концепция основана на логико-семантическом (семантика – изучение текста с точки зрения смысла) подходе, при котором информация трактуу-

ется как знание, причем не любое знание, а та его часть, которая используется для ориентировки, для активного действия, для управления и самоуправления. Иными словами, *информация – это действующая, полезная, «работающая» часть знаний.* Представителем этой концепции является В. Г. Афанасьев.

В настоящее время термин «информация» имеет глубокий и многогранный смысл. Во многом оставаясь интуитивным, он получает разные смысловые наполнения в разных отраслях человеческой деятельности:

- в житейском аспекте под информацией понимают сведения об окружающем мире и протекающих в нем процессах, воспринимаемые человеком или специальными устройствами;
- в технике под информацией понимают сообщения, передаваемые в форме знаков или сигналов;
- в теории информации (по К. Шеннону) важны не любые сведения, а лишь те, которые снимают полностью или уменьшают существующую неопределенность;
- в кибернетике, по определению Н. Винера, информация – эта та часть знаний, которая используется для ориентирования, активного действия, управления, т. е. в целях сохранения, совершенствования, развития системы;
- в семантической теории (смысл сообщения) – это сведения, обладающие новизной, и т. д.

Такое разнообразие подходов не случайность, а следствие того, что выявилась необходимость осознанной организации процессов движения и обработки того, что имеет общее название – информация.

По способу восприятия информацию разделяют на следующие виды: *визуальная, аудиальная, вкусовая, обонятельная* и *тактильная*. Такое деление основывается на органах чувств, с помощью которых информация воспринимается человеком: это зрение, слух, вкус, обоняние и осязание соответственно. Научные исследования показывают, что свыше 90 % информации, получаемой человеком из внешнего мира, приходится на зрение и слух, около 10 % – на вкус, обоняние и осязание.

При качественной оценке получаемой информации говорят о следующих ее свойствах:

- *полезность,* или *релевантность* (соответствие запросам потребителя);
- *достоверность.* Данные возникают в момент регистрации сигналов, но не все сигналы являются «полезными» – всегда присутствует какой-то уровень посторонних сигналов, в результате чего полезные данные

сопровождаются определенным уровнем «информационного шума». Если полезный сигнал зарегистрирован более четко, чем посторонние сигналы, достоверность информации может быть более высокой;

• *полнота* определяет достаточность данных для принятия решений или для создания новых данных на основе имеющихся;

• *актуальность,* или *своевременность* – это степень соответствия информации текущему моменту времени;

• *доступность* – мера возможности получить ту или иную информацию. На степень доступности информации влияют одновременно как доступность данных, так и доступность адекватных методов для их интерпретации.

• *защищенность* (невозможность несанкционированного использования или изменения);

• *эргономичность* (удобство формы или объема с точки зрения данного потребителя);

• *объективность* и *субъективность* информации. Понятие объективности информации является относительным. Это понятно, если учесть, что методы являются субъективными. Более объективной принято считать ту информацию, в которую методы вносят меньший субъективный элемент. Так, например, принято считать, что в результате наблюдения фотоснимка природного объекта или явления образуется более объективная информация, чем в результате наблюдения рисунка того же объекта, выполненного человеком;

• *понятность* (способность и возможность объекта воспринимать, понимать и воспроизводить информацию).

1.2. Информационные ресурсы: определение, классификация и характеристика их основных свойств; информационные ресурсы в условиях рыночных отношений

Информационные ресурсы – это вся накопленная информация об окружающей нас действительности, зафиксированная на материальных носителях и в любой другой форме, обеспечивающей ее передачу во времени и пространстве между различными потребителями для решения научных, производственных, управленческих и других задач.

Каждый новый тип носителя информации порождает свой класс информационных ресурсов, характеризуемый своим множеством свойств,

связанных с фиксацией, воспроизводством, доступом, восприятием и процессами обработки зафиксированной на носителе информации, а также реализацией процессов передачи информации во времени.

Свойства носителя существенным образом влияют на место каждого класса информационных ресурсов в процессах материальной и духовной деятельности отдельных людей и общества в целом.

В зависимости от носителей информации информационные ресурсы предлагается делить на следующие основные классы:

- документы всех видов, на любых видах носителей (в том числе все виды машиночитаемых носителей, используемых в вычислительной технике и технике средств связи);
- персонал (память людей), обладающий знаниями и квалификацией в различных областях науки и техники;
- организационные единицы – научные, производственные, управленческие и другие организации, располагающие кадровыми, техническими, производственными, финансовыми и прочими возможностями для решения определенного круга проблем и задач;
- промышленные образцы (любые материальные объекты, созданные в процессе производства), рецептуры и технологии, программные продукты, которые являются овеществленным результатом научной и производственной деятельности людей;
- научный инструментарий (в том числе автоматизированные системы научных исследований, автоматизированные рабочие места научных работников и проектировщиков, экспертные системы и базы знаний).

В федеральном законе понятие информационных ресурсов включает только документы: информационные ресурсы – отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, банках данных, других видах информационных систем) (Федеральный закон от 04.07.1996 г. № 85-ФЗ «Об участии в международном информационном обмене». Ст. 2). Это же определение используется в Законе «Об информации, информатизации и защите информации» [1].

Для обоснования принятого подхода к определению информационного ресурса покажем ограниченность и неполноту определения, используемого в законодательных документах [Там же].

1. Одна и та же информация, относящаяся к той или иной проблеме, может быть зафиксирована на различных носителях, и/или различные информа-

ционные фрагменты одной и той же проблемы могут быть зафиксированы таким образом, что правильное восприятие информации становится невозможным, если отсутствует доступ ко всем информационным фрагментам, представленным на различных носителях. Поэтому целостность информационных ресурсов обеспечивается в том и только том случае, если потребитель (пользователь) имеет доступ ко всем классам носителей, на которых зафиксирована информация, необходимая для решения стоящих перед ним задач.

2. Сужение понятия информационных ресурсов до класса документов исключает из рассмотрения значительные объемы информации, зафиксированные на иных классах носителей. Но каждый класс информационных ресурсов – это еще и иные способы взаимодействия с информационными ресурсами, способы их создания, регистрации, сбора, сохранения, взаимодействия с ними и, следовательно, иные способы управления информационными технологиями, а также иная правовая база, определяющая их использование.

3. Разрыв информационных связей между выделенными классами информационных ресурсов порождает разрывы в информационных процессах и технологиях. Это, в свою очередь, ведет к потере целостности восприятия окружающей действительности, резкому снижению качества информации и результативности при принятии информационных решений.

4. Создаются предпосылки к безвозвратной утрате важнейшей информации, которая не может быть содержательно осмыслена только на основе документальных информационных ресурсов. Учет только документальных информационных ресурсов может привести к полной утрате конкретной проблемной информации.

5. Нарушение целостности понимания информационных ресурсов создает предпосылки к нарушению информационной безопасности.

Учитывая, что предлагаемый подход к определению информационных ресурсов существенно отличается от определения, принятого в законодательстве, приведем перечень прецедентов, свидетельствующих о неполноте законодательного определения.

Перечень прецедентов является достаточным для иллюстрации неполноты подхода, при котором информационные ресурсы сводятся к документальным информационным ресурсам.

В уголовной практике:

1. Дело сопровождается «вещдоками», без них нет дела (орудия взлома, орудие убийства и/или его элементы: гильзы, пули, веревки и пр.). Вещдоки (или часть их) сохраняются «при деле».

2. Формируются специальные коллекции из орудий, участвовавших в преступлении:

• создание коллекций оружия для отождествления типа оружия по боеприпасу;

• коллекции гильз («гильзотеки») и использованных пуль для прослеживания движения «стволов» по преступлениям.

В государственном делопроизводстве в архивы сдавались печати (определенным образом «погашенные»).

В экспертизе, метрологии, сельском хозяйстве:

• эталонные образцы, реактивы и пр.;

• реперные объекты (например, Кронштадтский футшток («уровень моря»); Гринвичский и Пулковский меридианы, системы мегалитических памятников как материализованная фиксация астрономических знаний древности (скрытые и «раскрытые»), геодезические знаки опорной геодезической сети (по классам точности);

• «линии производителей», элитный семенной материал и пр.;

• мощнейший инструментальный комплекс «эталонного времени», сеть сейсмических и метеорологических станций, контрольно-измерительные полигонные комплексы (данный пример может быть примером класса «организационная единица» в чистом виде).

Американская система патентования требовала в качестве дополнения к патенту действующее устройство и/или модель.

Отчетные материалы геологоразведки состоят из двух частей: собственно описательных и аналитических материалов и образцов. К этому классу относятся метеоритные коллекции и пробы грунта, полученные в результате планетарных исследований.

Утрата образцов резко снижает ценность отчетов. Результаты разных партий, проводящих исследования, могут стать несопоставимыми. «Документальная ценность» образцов неисчерпаема (с появлением новых методов исследований происходит новое раскрытие информационного содержания). Например:

• многократные переоценки экспедиционных материалов по Тунгусскому метеориту;

• новые оценки гипотезы «жизни на Марсе» по результатам анализа метеоритного материала.

В медицине и биологии: коллекции живых штаммов, чистые ряды подопытных животных и насекомых (белые мыши, муха дрозофила).

Палеонтологические реконструкции. Сюда можно включить и результаты реконструкций по методу Герасимова в археологии и криминалистике.

«Персонал» для выполнения специфических работ:

• специальные группы экспертов для проведения органолептических оценок (виноделие, производство парфюмерных изделий и др.). Это класс информационных ресурсов «персонал» в чистом виде;

• специфические профессиональные группы: испытатель (всех категорий), проводник, лоцман, «колодезник», следопыт, некоторые специалисты таможенных профессий и др.;

• «язык», свидетель (утрата свидетеля в ряде случаев ведет к «развалу» дела), «пленный»;

• оперативные работники, резидентура, специалисты по опознанию;

• особо доверенные лица («хранители тайн»): в древности – особо посвященные члены религиозных групп, вожди племен; хранители утерянных тайн (греческий огонь, сокровища инков, целые системы знаний древних и пр.); в современной истории – три специалиста, сохраняющие рецепт кока-колы; хранители тайн ценностей и местонахождения документохранилищ Германского рейха (по решениям совещания 1944 г.); полная группа хранителей кодовых комбинаций (ключей) «особых кладовых»; «старшие призыва» (в германской армии) и другие подобные персоны и группы;

• группы «трофейных специалистов»: группа Брауна, Гелен, Гесс, Паулюс на Нюрнбергском процессе и др.;

• «законсервированная» резидентура.

1.3. Документы как один из классов информационных ресурсов. Обобщенная модель документа. Основные барьеры доступа к документальным информационным ресурсам

Документированная информация (документ) – зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать (Федеральный закон от 04.07.1996 г. № 85-ФЗ «Об участии в международном информационном обмене». Ст. 2).

Документ – главное средство закрепления различным способом на специальном материале (носителе) информации, получаемой в процессе развития науки и практической деятельности людей. В них закрепляется

и концентрируется информация о фактах, событиях, явлениях объективной действительности и мыслительной деятельности человека. Основная функция документа – обеспечение передачи информации в пространстве и времени между различными пользователями.

Данный класс информационных ресурсов является наиболее исследованным. Фактически все работы по созданию и развитию информационных систем направлены на формирование документальных информационных ресурсов и обеспечение доступа пользователей к ведомственным, национальным и международным документальным ресурсам.

Основной тенденцией развития документальных ресурсов является перенос все большей их части на машиночитаемые носители, что принципиально изменяет условия доступа к документальным информационным ресурсам.

С одной стороны, создаются условия прямого доступа к неограниченным массивам информации и автоматизированной их обработки, а с другой – возможность полного закрытия неконтролируемого доступа к этим массивам, а также возможность жестко контролируемого информирования и дезинформирования (т. е. выдачи той и только той информации, которую держатель информационных ресурсов считает нужным предоставить конкретному пользователю).

Перенос информационных ресурсов на машиночитаемые носители приводит к существенным изменениям во всех процессах, связанных с накоплением, обменом и обработкой информации и процессов доступа к ресурсам.

Задачи обеспечения документальными информационными ресурсами осложняются и тем, что все большая часть машиночитаемых информационных ресурсов не имеет своего аналога на традиционных носителях.

Формирование машиночитаемых информационных ресурсов создает ситуацию, при которой пользователь, не обладающий необходимыми техническими и программными средствами переработки машиночитаемых информационных ресурсов, фактически исключается из сферы эффективного применения наиболее ценных информационных ресурсов на всех уровнях: персональном, групповом, ведомственном, национальном, региональном и международном.

Между информацией, зафиксированной в документе, и пользователем появляется система барьеров (технических, программных, технологи-

ческих и других), которые существенно ограничивают и/или полностью исключают возможность доступа к информации.

Более полно определить факторы, влияющие на создание барьеров между информацией, зафиксированной в документе, и пользователем, можно на основании приведенной ниже обобщенной модели документа.

Обобщенная модель документа. Как показывает анализ существующих определений, каждый тип документа является функцией следующих документообразующих признаков:

- содержание информации, отражаемой в документе (проблемная область информации, описательная информация о документе);
- носитель информации (бумажный носитель, магнитные и магнитооптические носители, микрофильмовые носители и кинофотоматериалы, устройства отображения, сообщения по линиям связи);
- алфавит представления информации (цифры, буквы, символы иероглифических систем письменности, знаки и т. д.);
- метод (способ) фиксации информации, представленной в документе (тексты, формульная информация, табличная информация, графика, представление пространственных данных, аудиовизуальная информация, цифровая и аналоговая информация и т. д.);
- устройство (техническое средство), обеспечивающее как воспроизводство документа в форме, пригодной для восприятия человеком, так и регистрацию (фиксацию), сбор, передачу, хранение и обработку, ввод-вывод документов (средства ручной обработки, оргтехника, микрофильмовая техника, элекронно-вычислительная техника);
- правила (способы, методы, алгоритмы, программы) преобразования документов (информации (данных)) при изменении носителя информации, устройств воспроизведения, фиксации, сбора, передачи, хранения, обработки, ввода-вывода документов;
- метаинформация о документе (структура документа, система кодирования, включаемая в документ, операции, разрешенные над информацией, включаемой в документ, технические средства, необходимые для обработки документов и информации и т. д.).

Каждый документ характеризуется своим набором признаков. С другой стороны, один и тот же по содержанию документ может иметь различную форму представления в зависимости от того, в какой информационной структуре он функционирует.

Общее количество видов и форм документов, используемых в качестве источников информации, неизвестно. Только по признакам, входящим в группу «Содержание информации», различные исследователи состава фондов крупнейших библиотек и информационных центров выявили около 110–130 видов документов (широкого распространения и непубликуемых).

Классификация видов документов. Применительно к фондам научно-технических документов, как правило, выделяют шесть классификационных групп:

1) библиографию литературных источников (планы издательств, проспекты информационных изданий, справочный аппарат государственных библиотек и т. д.);

2) библиографию неопубликованных источников (бюллетени регистрации, отраслевые сборники рефератов НИР и ОКР, тезисы докладов на конференциях и семинарах и т. д.);

3) фактографическую информацию (прейскуранты оптовых цен, каталоги изделий внутриведомственной кооперации, документация по ценообразованию и т. д.);

4) нормативную документацию (государственные и республиканские стандарты, отраслевые нормативы трудоемкости, стандарты предприятий на унифицированные узлы и компоненты и т. д.);

5) патентную информацию (патентные зарубежные журналы, выдержки из патентных заявок, описания отечественных изобретений и т. д.);

6) основную первичную информацию (книги, периодика, отечественные и зарубежные научно-технические сборники и труды НИИ, конструкторская и технологическая документация и т. д.).

Расширяющееся многообразие документообразующих признаков ведет к сверхизбыточному нарастанию несовместимых форм представления информации в документах, что существенным образом увеличивает число барьеров между информацией, зафиксированной в документе, и пользователем, желающим получить доступ к этой информации.

Если при использовании документов на традиционных носителях основным барьером при условии получения документа был «языковой барьер» и уровень профессиональной подготовки пользователя, то переход к машиночитаемым носителям количество барьеров резко увеличивает.

Основные барьеры доступа к документальным информационным ресурсам. В зависимости от различных документообразующих признаков они могут быть заданы следующим перечнем.

1. Барьеры, возникающие при использовании микрофильмовых носителей (микрофильмы, микрофитиши):

- кратность уменьшения;
- цветочувствительность;
- цветопередача;
- разрешающая способность;
- адаптивность оборудования к типу носителя и его размерным параметрам;
- возможность автоматизированного поиска по имеющимся на носителе идентификационным кодам: степень доступности кодовых признаков, возможность декодирования аппаратными средствами, совместимость техническая;
- возможность выборочного и сплошного копирования и получения полноразмерных копий.

2. Магнитные и магнитооптические (CB КОМ) носители (магнитная лента, магнитные диски, дискеты, жесткие диски (винчестеры), CB КОМ, оперативная память):

- размерные характеристики носителя (длина, ширина, толщина, диаметр, количество поверхностей, с которых происходит чтение-запись информации);
- конструктивные характеристики, связанные с возможностью установки на конкретные устройства ввода-вывода информации;
- тип записи (плотность, число дорожек, ширина межблочных промежутков и т. п.);
- организация файлов;
- методы кодирования информации (используемый алфавит и методы кодирования символов алфавита, стандарты представления видеоинформации, графики пространственной информации, звука, аналоговой информации и т. д.);
- используемые методы защиты информации (криптография, электронные ключи, другие аппаратные методы защиты).

3. Алфавит представления информации:

- несовместимость символьного набора;

• несовместимость системы кодирования;

• несовместимые системы правил лексикографического упорядочения;

• несовместимость используемых символьных множеств с языками представления информации и типами представляемой информации;

• неразличимость «синонимии» символов (начертательной и кодовой);

• несовместимость правил транслитерирования.

4. Устройство (техническое средство):

• техническая несовместимость (общая, частичная);

• несогласованность конфигурации с требованиями к процессам обработки (объемы памяти, типы мониторов, видеокарты и пр.); невозможность использования требуемых программных продуктов.

5. Правила несовместимости (способы, методы, алгоритмы, программы) преобразования документов (информации, данных):

6. Метаинформация о документе (информация, описывающая документ):

• несовместимые методы и схемы описания (по содержанию, набору параметров);

• закрытость параметров и схем описания.

Исходя из изложенного, можно сделать следующие выводы.

1. Современный уровень развития информационных технологий с документальными ресурсами и тенденции их развития встраивают между носителем информации и пользователем информации, зафиксированной на носителе, сложнейшую техногенную среду (техническую, алгоритмическую, программную, технологическую), без участия которой пользователь не способен получить доступ к информации и воспринимать ее.

2. Несовместимость техногенной среды создает значительные трудности для восприятия информации, зафиксированной на машиночитаемых носителях, и во многих случаях ведет к ее безвозвратной утрате.

3. Использование машиночитаемых ресурсов возможно в том и только в том случае, если они используются в согласованной (нормализованной, стандартизованной) техногенной среде. Требуемый уровень согласования для различных типов машиночитаемых документов различен. Соответственно, каждая техногенная среда позволяет осуществлять работу с различными (свойственными только для нее) типами машиночитаемых ресурсов. Более того, различные модификации (версии) одной и той же техносферы могут порождать несовместимые машиночитаемые информационные ресурсы. К этой категории барьеров относятся ситуации, связан-

ные с использованием несовместимых текстовых редакторов, драйверов, видеокарт, системные требования к конфигурации и пр.

4. Современный уровень развития техносферы визуализации и использования информации, зафиксированной на машиночитаемых носителях, порождает формирование информационных ресурсов с высокой степенью «нерегулируемой (скрытой) криптографичности», определяемой несогласованностью инструментальных средств, находящихся в распоряжении конкретных пользователей. «Нерегулируемая (скрытая) криптографичность» информационных ресурсов, в свою очередь, порождает неадекватное воспроизводство информации, содержащейся на носителе, что исключает ее использование.

В каждый момент времени конкретная информационная система находится в состоянии информационной, технической, программной и технологической совместимости. Но система непрерывно развивается (модернизируется, модифицируется): изменяется состав технических, программных и технологических средств. Развиваются и внешние информационные системы.

Собственное развитие осуществляется, как правило, с учетом принятых ранее технических и программных решений (не исключаются случаи преобразований от «чистого листа», когда происходят принципиальные изменения, коренная ломка структуры технических и программных средств).

Каждая внешняя система, осуществляя аналогичный процесс развития, принимает иные проектные решения, обеспечивающие свои цели.

В результате в системах накапливаются документальные информационные ресурсы, несовместимые на уровне технических средств, различающиеся по структуре, форматам представления данных, методам кодирования, правилам содержательного описания и т. д. Взаимодействие пользователя с такими ресурсами невозможно без разработки системы комплексных программных средств, обеспечивающих приведение информационных массивов к виду, при котором могут осуществляться информационные технологии, образованные «новой конфигурацией» программно-технического комплекса системы на новый текущий момент времени. Создается ситуация, при которой «ретроспективные» массивы, даже приведенные к формальным условиям совместимости с массивами «на данный момент времени», являются неадекватной формой представления ранее накопленной информации. Степень этой «неадекватности» различна, она,

как правило, соответствует той степени «правильности», которую удалось обеспечить при конвертировании в новую форму представления.

При этом нужно учитывать, что преобразование информационных массивов не всегда имеет место. Это положение относится и к собственным массивам системы, и особенно к массивам внешних систем.

Например, несмотря на разработку мощных современных текстовых процессоров и баз данных далеко не всегда между ними возможен взаимный экспорт (импорт) файлов.

Многократное конвертирование в конечном счете может создать условия абсолютной утраты достоверности информации.

Ситуация осложняется тем, что:

- преобразуются значительные по объему массивы машиночитаемых ресурсов (гига- и терабайты, миллионы документов (записей));
- преобразования проводятся по системе алгоритмических процедур, реализованных в каждой системе различным образом. Алгоритмы, их ограничения, требования к процедурам и алгоритмам, определяющим конвертирование массивов, как правило, неизвестны (заданы по умолчанию, в явном виде пользователю неизвестны). К пользователю могут поступать одни и те же массивы, прошедшие через различные множества конверторов, что порождает эффект, аналогичный «множественному» переводу в традиционных информационных технологиях;
- пользователь, применяющий информацию, не знает, подвергался ли предоставленный ему массив конвертированию, какие процедуры при конвертировании проводились, с помощью каких конверторов и какое число конвертаций данного массива проводилось;
- возможна ситуация, при которой различные части информационного массива конвертировались по различным системам конверторов;
- в организации взаимодействия по межсистемному обмену документальными информационными ресурсами на машиночитаемых носителях возникают значительные трудности, преодоление которых требует значительных ресурсных затрат, связанных с необходимостью конвертирования информационных массивов.

Вопросы и задания для самоконтроля

1. Дайте определение понятию информации.
2. Охарактеризуйте основные теории информации.

3. Перечислите свойства информации.

4. Что такое информационный ресурс?

5. Что понимают под документом?

6. Охарактеризуйте обобщенную модель документа.

7. Какие барьеры доступа к документальным информационным ресурсам вы знаете?

8. С какими моментами связана утрата достоверности информации?

Глава 2. НАДЕЖНОСТЬ (ДОСТОВЕРНОСТЬ) ИНФОРМАЦИИ И ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

2.1. Надежность информации и способы несанкционированного доступа: инициативное сотрудничество, хищение, уничтожение, копирование, негласное ознакомление и др.

2.2. Технические средства несанкционированного доступа к информации. Защита от разных способов несанкционированного доступа

2.1. Надежность информации и способы несанкционированного доступа: инициативное сотрудничество, хищение, уничтожение, копирование, негласное ознакомление и др.

Под способом вообще понимается порядок и приемы действий, приводящие к достижению какой-либо цели. Можно определить способ несанкционированного доступа как совокупность приемов, позволяющих злоумышленнику получить охраняемые сведения конфиденциального характера.

Способами несанкционированного доступа являются [2]:

1. Инициативное сотрудничество.
2. Склонение к сотрудничеству.
3. Выведывание, выпытывание.
4. Подслушивание.
5. Наблюдение.
6. Хищение.
7. Копирование.
8. Подделка (модификация).
9. Уничтожение.
10. Незаконное подключение.
11. Перехват.
12. Негласное ознакомление.
13. Фотографирование и видеосъемка.
14. Сбор и аналитическая обработка информации.

Инициативное сотрудничество проявляется в определенных действиях лиц, чем-то не удовлетворенных или остро нуждающихся в средствах к существованию, из числа работающих на предприятии или просто алчных и жадных, готовых ради наживы на любые противоправные действия. Финансовые затруднения, политическое или научное инакомыслие, недовольство продвижением по службе, обиды от начальства и властей, недовольство своим статусом и многое другое толкают обладателей конфиденциальной информации на открытие несанкционированного доступа к информации. Наличие такого человека в сфере производства и управления предприятия позволяет злоумышленникам получать необходимые сведения о предприятии, так как осведомитель экономит их время и средства на внедрение своего агента, представляет свежую и достоверную информацию, которую обычным путем было бы сложно получить.

Склонение к сотрудничеству – это, как правило, насильственное действие со стороны злоумышленников. Склонение или вербовка может осуществляться путем подкупа, запугивания, шантажа. Склонение к сотрудничеству реализуется в виде реальных угроз, преследования и других действий, выражающихся в преследовании, оскорблении, надругательстве и т. д. Шантаж с целью получения средств к существованию, льгот, политических выгод в борьбе за власть практикуется с легкостью и завидным постоянством. Некоторые конкуренты не гнушаются и рэкетом, который особо был распространен в конце XX в. По интенсивности насилия это один из наиболее агрессивных видов деятельности, где за внешне мирными визитами и переговорами кроется готовность действовать намеренно жестоко с целью устрашения. Весьма близко к склонению лежит и переманивание специалистов фирмы конкурента на свою фирму с целью последующего обладания его знаниями.

Выведывание, выпытывание – это стремление под видом наивных вопросов получить определенные сведения. Выпытывать информацию можно и ложными трудоустройствами, и созданием ложных предприятий, и другими действиями.

Подслушивание – способ ведения разведки и промышленного шпионажа, применяемый агентами, наблюдателями, информаторами, специальными постами подслушивания. В интересах подслушивания злоумышленники идут на самые различные ухищрения, используют для этого специальных людей, сотрудников, современную технику, различные приемы ее

применения. Подслушивание может осуществляться непосредственным прямым восприятием речевой информации либо с помощью технических средств.

Наблюдение – способ ведения разведки о состоянии и деятельности противника. Ведется визуально и с помощью оптических приборов. Процесс наблюдения довольно сложен, так как требует значительных затрат сил и средств. Поэтому наблюдение, как правило, осуществляется целенаправленно, в определенное время и в нужном месте специально подготовленными людьми, ведется скрытно. К техническим средствам относятся оптические приборы (бинокли, трубы, перископы), телевизионные системы (для обычной освещенности и низкоуровневые), приборы наблюдения ночью и при ограниченной видимости. Очень часто результаты наблюдения фиксируются фото- и видеосъемкой для дальнейшего их использования.

Хищение – умышленное противоправное завладение чужим имуществом, средствами, документами, материалами, информацией. Похищают все: документы, продукцию, электронные носители информации, ключи, коды, пароли и шифры.

Копирование. В практике криминальных действий копируют документы, содержащие интересующие злоумышленника сведения; информацию, обрабатываемую в автоматизированных системах обработки данных; продукцию. Достаточно сложно определить, что информация была скопирована, так как копия не оставляет следов.

Подделка (модификация, фальсификация) в условиях беззастенчивой конкуренции приобрела большие масштабы. Подделывают доверительные документы, позволяющие получить определенную информацию, письма, счета, бухгалтерскую и финансовую документацию, ключи, пропуска, пароли, подписи и т. д.

Уничтожение. В части информации особую опасность представляет ее уничтожение с технических носителей, на которых содержатся огромные объемы сведений различного характера, причем многие из них весьма трудно изготовить в виде немашинных аналогов. Уничтожаются и люди, и документы, и средства обработки информации, и продукция.

Незаконное подключение. Под незаконным подключением будем понимать контактное или бесконтактное подключение к различным линиям связи с целью несанкционированного доступа к информации. Незаконное подключение как способ тайного получения информации известен

давно. Подключение возможно как к проводным линиям телефонной и телеграфной связи, так и к линиям связи иного информационного назначения: линиям передачи данных, соединительным линиям периферийных устройств, линиям диспетчерской связи, конференц-связи, питания, заземления и др.

Перехват. В практике радиоэлектронной разведки под перехватом понимают получение разведывательной информации за счет приема сигналов электромагнитной энергии пассивными средствами приема, расположенными, как правило, на достаточном расстоянии от источника конфиденциальной информации. Перехвату подвержены переговоры любых систем радиосвязи, переговоры, ведущиеся с подвижных средств телефонной связи (радиотелефон), переговоры внутри помещения посредством бесшнуровых систем учрежденческой связи и др.

Негласное ознакомление – способ получения информации, к которой субъект не допущен, но при определенных условиях может получить возможность кое-что узнать (открытый документ на столе во время беседы с посетителем, наблюдение за экраном компьютера со значительного расстояния в момент работы с закрытой информацией и т. д.). К негласному ознакомлению относится и перлюстрация почтовых отправлений, учрежденческой и личной переписки.

Фотографирование – способ получения видимого изображения объектов на фотоматериале. Особенность этого способа – документальность, позволяющая при дешифровании фотоснимков по элементам и демаскирующим признакам получить весьма ценные, детальные сведения об объекте наблюдения.

Сбор и аналитическая обработка являются завершающим этапом изучения и обобщения добытой информации с целью получения достоверных и объемлющих сведений по интересующему аспекту деятельности объекта и его интересов. Полный объем сведений о деятельности не может быть получен каким-нибудь одним способом. Чем большими информационными возможностями обладает руководитель, тем больших успехов он может добиться в конкурентной борьбе. На успех может рассчитывать тот, кто быстрее и полнее соберет необходимую информацию, переработает ее и примет правильное решение.

В общем плане мероприятия по противодействию несанкционированному доступу к источникам конфиденциальной информации с по-

мощью технических средств можно свести к следующим основным направлениям:

- защита от наблюдения и фотографирования;
- защита от подслушивания;
- защита от незаконного подключения;
- защита от перехвата.

2.2. Технические средства несанкционированного доступа к информации. Защита от разных способов несанкционированного доступа

В последнее время появились специальные устройства съема информации, использующие для передачи акустической информации так называемые нетрадиционные каналы. К ним можно отнести следующие:

1. Устройства съема информации, ведущие передачу в инфракрасном диапазоне (ИК-передатчики). Характеризуются такие изделия крайней сложностью их обнаружения. Срок непрерывной работы – 1–3 суток. Используют эти устройства, как правило, для увеличения дальности передачи информации и размещают их у окон, вентиляционных отверстий и т. п., что может облегчить задачу их поиска. Для приема информации применяют специальный приемник ИК-диапазона, который обеспечивает надежную связь на расстоянии 10–15 м.

2. Устройства съема информации, использующие в качестве канала передачи данных силовую электрическую сеть 127/220/380 В. Такие устройства встраиваются в электрические розетки, удлинители, тройники, бытовую аппаратуру и другие места, где проходит или подключается сеть. К основным достоинствам таких устройств можно отнести неограниченное время работы. Прием информации от таких устройств осуществляется специальными приемниками, подключаемыми к силовой сети, в радиусе до 300 м.

3. Устройства съема информации с ее закрытием, использующие шифровку или преобразование частоты с различными видами модуляции. Попытка прослушать такое устройство даже очень хорошим сканирующим приемником ни к чему не приведет – будет слышен только шум, лишь указывающий на наличие устройства съема информации.

4. Устройства съема информации на основе лазерного микрофона, который позволяет на расстоянии до 300 м регистрировать колебания оконных стекол и преобразовывать их в звуковой сигнал.

Устройства съема информации, использующие «нетрадиционные каналы» передачи, чрезвычайно дороги и сложны в эксплуатации, поэтому использование их частными лицами маловероятно.

В тех случаях, когда нельзя установить устройства съема информации непосредственно на объекте, применяют стетоскопные микрофоны, которые позволяют прослушивать переговоры через твердую преграду (стену, стекло, корпус автомобиля и т. п.), причем чем тверже и однороднее преграда, тем лучше они работают. Стетоскоп представляет собой вибродатчик с усилителем и головными телефонами (или устройством автоматической записи звука на магнитную ленту). С помощью стетоскопного микрофона можно осуществлять прослушивание разговоров через стену толщиной 1 м и более. Основным преимуществом такой системы является трудность ее обнаружения, так как стетоскопный микрофон можно устанавливать в соседнем помещении. Устройства съема информации устанавливаются с согласия хозяина помещения или без него в специально подготовленные места с последующей их маскировкой либо встраиваются в предметы быта, интерьера или свободные полости помещения.

В последнее время одним из основных способов несанкционированного доступа к информации частного и коммерческого характера стало прослушивание телефонных переговоров. Для прослушивания телефонных переговоров используются следующие способы подключения:

• параллельное подключение к телефонной линии. В этом случае телефонные радиоретрансляторы труднее обнаруживаются, но требуют внешнего источника питания;

• последовательное включение телефонных радиоретрансляторов в разрыв провода телефонной линии. В этом случае питание телефонного радиоретранслятора осуществляется от телефонной линии, и в эфир он выходит (т. е. начинает передачу) с момента подъема телефонной трубки абонентом.

Подключение телефонного радиоретранслятора может осуществляться как непосредственно к телефонному аппарату, так и на любом участке линии от телефона абонента до АТС. В настоящее время существуют телефонные радиоретрансляторы, позволяющие прослушивать помещение

через микрофон лежащей трубки. Существуют системы прослушивания телефонных разговоров, не требующие непосредственного электронного соединения с телефонной линией. Эти системы используют индуктивный способ съема информации. Они достаточно громоздки, поэтому не нашли широкого практического применения. Для приема информации от телефонных радиотрансляторов используются такие же приемники, как в акустических устройствах съема информации по радиоканалу. В настоящее время появились системы перехвата факсовой и модемной связи, которые при использовании персонального компьютера (ПК) со специальным программным обеспечением позволяют получить расшифровку информации. Однако такие системы очень дорогие и пока не нашли широкого применения в нашей стране. Способы, которыми может вестись прослушивание телефонных линий, следующие.

Непосредственное подключение к телефонной линии – наиболее простой и надежный способ получения информации. В простейшем случае применяется трубка ремонтника-телефониста, подключаемая к линии в распределительной коробке, где производится разводка кабелей. Чаще всего это почерк «специалистов» нижнего звена уголовного мира (верхнее звено оснащено аппаратурой не хуже государственных секретных служб). Необходимо помнить, что АТС переключает линию на разговор при шунтировании ее сопротивлением около 1 кОм. Применение аппаратуры подслушивания с низкоомным входным сопротивлением можно обнаружить достаточно быстро. Если вы услышите щелчки в линии или перепады громкости – есть вероятность того, что вас пытаются прослушать не совсем профессиональным способом.

Подкуп обслуживающего персонала на АТС – весьма распространенный способ раскрытия ваших секретов. Особенно это касается небольших городов, где до сих пор используются старые декадно-шаговые АТС. Скорее всего таким способом могут воспользоваться преступные группы либо конкурирующие фирмы.

Телефонные аппараты, где в качестве вызывного устройства используется электромагнитный звонок, пока еще широко распространены в нашей стране. Звонок обладает свойством дуальности, т. е., если на электромагнитный звонок действуют звуковые волны, он начинает вырабатывать соответствующим образом модулированный ток. Амплитуда его достаточна для дальнейшей обработки. Эксперименты показали, что амплитуда

электродвижущей силы, наводимая в линии, для некоторых типов телефонных аппаратов может достигать нескольких милливольт. Корпус аппарата является дополнительным резонирующим устройством.

Этот способ не является синонимом непосредственного подключения к линии. Он гораздо сложнее. Микрофон является частью электронной схемы телефонного аппарата: он либо соединен с линией (через отдельные элементы схемы) при разговоре, либо отключен от нее, когда телефонный аппарат находится в готовности к приему вызова (трубка находится на аппарате). На первый взгляд, когда трубка лежит на аппарате, нет никакой возможности использовать микрофон в качестве источника съема информации. Но это только на первый взгляд. Для защиты телефонного аппарата от снятия информации таким способом достаточно параллельно микрофону подключить конденсатор емкостью 0,01–0,05 мкФ. При этом последний будет шунтировать микрофон по высокой частоте и глубина модуляции высокочастотных (ВЧ) колебаний уменьшится более чем в 10 тыс. раз, что делает дальнейшую демодуляцию сигнала практически невозможной.

Теперь рассмотрим способы доступа профессионала к информации, находящейся в персональном компьютере. Ограничение доступа к ПК путем введения кодов не обеспечивает полной защиты информации. Включить компьютер и снять код доступа к системе не вызывает особых затруднений – достаточно отключить аккумулятор на материнской плате. На некоторых моделях материнских плат для этого предусмотрен специальный переключатель. Также у каждого изготовителя программы BIOS (AMI, AWARD и др.) есть коды, имеющие приоритет перед любыми пользовательскими, набрав которые можно получить доступ к системе. В крайнем случае можно украсть системный блок компьютера или извлечь из него жесткий диск и уже в спокойной обстановке получить доступ к необходимой информации. Другое дело, когда попасть в помещение, где установлен компьютер, не удается. В этом случае используют дистанционные способы съема информации. Естественно, они эффективны только тогда, когда компьютер включен. Существуют два способа дистанционного считывания информации: первый способ основан на приеме ВЧ-наводок в силовую сеть, а второй – на приеме побочных электромагнитных излучений соединительных цепей ПК. Распространение побочных электромагнитных излучений за пределы контролируемой территории создает предпосылки для утечки информации, так как возможен ее перехват с помощью специальных технических средств.

Исследования показывают, что излучение видеосигнала монитора является достаточно мощным, широкополосным и охватывает диапазон метровых и дециметровых волн. Причиной мощного излучения является наложение радиосигнала на импульсы развертки изображения, вырабатываемые строчным трансформатором. При кажущейся сложности проблемы аппаратура для этого вида коммерческой разведки достаточно проста и изготавливается на базе обычного малогабаритного телевизора. Такие устройства позволяют на удалении 50 м получать устойчивую картинку – копию изображения, отображаемого в настоящий момент на экране монитора вашего ПК. Для уменьшения уровня побочных электромагнитных излучений применяют специальные средства защиты информации: экранирование помещений, фильтрацию источников питания, дополнительное заземление, электромагнитное заземление, а также средства ослабления уровней нежелательных электромагнитных излучений и наводок при помощи различных резистивных и поглощающих согласованных нагрузок.

В последнее время все чаще говорят о несанкционированном внедрении в базы данных. Этот вид пиратства очень быстро прогрессирует вследствие бурного развития компьютеризации при обработке информации в коммерческих кругах с выходом информационных сетей в телефонную сеть общего пользования. Компьютерные взломщики, «хакеры» не ограничиваются вопросами бесплатного получения коммерческой информации – достаточно случаев вскрытия и перевода денежных счетов из одного банка в другой через информационную сеть общего пользования.

В настоящее время для сбора информации могут использоваться миниатюрные скрытые и специальные (камуфлированные под обычные предметы) фото- и видеокамеры:

- миниатюрные (скрытые) встраиваются в бытовую технику и передают видеоинформацию по кабелю или по ВЧ-каналу при помощи телевизионного передатчика;
- специальные, т. е. замаскированные под бытовые предметы, например пачку сигарет, кейс, книгу, наручные часы и т. п.

Аппаратура для скрытой фото- и видеосъемки, как правило, оборудуется специальными объективами и насадками:

- миниатюрными объективами, предназначенными для съемки через отверстия небольшого диаметра (до 5 мм);

• телескопическими объективами, позволяющими вести съемку с дальних расстояний. Такие объективы обладают высокой кратностью увеличения (до 1,5 тыс. крат);

• камуфляжными объективами, используемыми для скрытой съемки из различных бытовых предметов, например из кейсов;

• объективами, совмещенными с приборами ночного видения (с инфракрасной подсветкой) и предназначенными для проведения съемки в темное время суток.

В качестве примера оборудования для скрытого наблюдения рассмотрим миниатюрную телевизионную камеру ЛТ-241s, которая позволяет сделать наблюдение абсолютно незаметным, информативным и безопасным. Использование телекамеры ЛТ-241s наиболее эффективно в системах охраны, системах телевизионного наблюдения, системах скрытого аудиовидеопротокола и т. д. Сверхминиатюрный зрачок объектива позволяет вести наблюдение через отверстие диаметром 0,3–1,2 мм при угле поля зрения 110°, а высокая чувствительность (0,04 лк) – видеть в темноте лучше, чем человеческий глаз. Малые размеры телекамеры (39×39×20 мм) позволяют установить ее в любые элементы интерьера: часы, книгу, картину, входную дверь, стену и т. п. Телекамера может быть оснащена другими объективами с иным полем зрения.

Перечень технических средств фото- и видеосъемки можно было бы продолжить, но вероятность ее использования частными лицами очень мала из-за сложности в эксплуатации и высокой стоимости.

Защита от наблюдения и фотографирования предполагает:

• выбор оптимального расположения средств документирования, размножения и отображения информации (экраны ПЭВМ, экраны общего пользования и др.) с целью исключения прямого или дистанционного наблюдения (фотографирования);

• использование светонепроницаемых стекол, занавесок, драпировок, пленок и других защитных материалов (решетки, ставни и пр.);

• выбор помещений, обращенных окнами в безопасные зоны (направления);

• использование средств гашения экранов ЭВМ и табло коллективного пользования после определенного времени работы (работа по режиму времени).

Защита от наблюдения и фотографирования на местности предполагает применение мер маскирования, скрытия объектов в рельефе местно-

сти, лесных массивах и, естественно, организацию режима охраны на удалении, обеспечивающем скрытность деятельности.

В более сложных условиях можно применять средства активного маскирования: маскирующие дымы, аэрозоли и др.

При прослушивании широкое распространение получили такие технические средства, как микрофоны, лазеры высокочастотных колебаний.

Микрофон является первым звеном в системе подслушивания с помощью технических средств, как микрофонных, так и радиозакладных. Каждый микрофон обладает двумя основными параметрами:

• чувствительностью. Чувствительность – это отношение напряжения на выходе микрофона к воздействующему на него звуковому давлению, выраженному в милливольтах на паскаль (мВ/Па);

• частотной характеристикой. Частотная характеристика – это зависимость чувствительности от частоты звукового давления.

Известно, что звуковое давление по степени его восприятия человеком можно разделить на слышимый звук, лежащий в полосе 16–20 000 Гц, инфразвук – ниже 16 Гц, и ультразвук, диапазон частот которого находится выше 20 000 Гц.

В качестве меры противодействия избирается акустическое воздействие на микрофон частотами ультразвукового диапазона.

Вопросы и задания для самоконтроля

1. Дайте понятие надежности информации.

2. Перечислите способы несанкционированного доступа.

3. Какие существуют мероприятия по противодействию несанкционированному доступу?

4. Назовите технические средства несанкционированного доступа к информации и особенности их использования.

5. Что понимается под наблюдением?

6. Как можно защититься от наблюдения и фотографирования?

Глава 3. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЧЕЛОВЕКА И ОБЩЕСТВА

3.1. Информационная безопасность: определение, составляющие

Информационная безопасность является одной из проблем, с которой столкнулось современное общество в процессе массового использования автоматизированных средств обработки информации.

Проблема информационной безопасности обусловлена возрастающей ролью информации в общественной жизни. Современное общество все более приобретает черты информационного общества.

С понятием «информационная безопасность» в разных контекстах связаны различные определения. Так, в Законе РФ «Об участии в международном информационном обмене» информационная безопасность определяется как состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства [10]. Подобное же определение дается и в Доктрине информационной безопасности Российской Федерации, где указывается, что информационная безопасность характеризует состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.

Оба эти определения рассматривают информационную безопасность в национальных масштабах и поэтому имеют очень широкое содержание.

Наряду с этим характерно, что применительно к различным сферам деятельности, так или иначе связанным с информацией, понятие «информационная безопасность» принимает более конкретные очертания. Так,

например, в Концепции информационной безопасности сетей связи общего пользования Российской Федерации даны два определения этого понятия.

1. Информационная безопасность – это свойство сетей связи общего пользования противостоять возможности реализации нарушителем угрозы информационной безопасности.

2. Информационная безопасность – свойство сетей связи общего пользования сохранять неизменными характеристики информационной безопасности в условиях возможных воздействий нарушителя.

Необходимо иметь в виду, что при рассмотрении проблемы информационной безопасности нарушитель необязательно является злоумышленником. Нарушителем информационной безопасности может быть сотрудник, нарушивший режим информационной безопасности, или внешняя среда, например, высокая температура, которая может привести к сбоям в работе технических средств хранения информации и т. д.

На основе анализа научной литературы в данной области можно сформулировать следующее определение информационной безопасности.

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

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

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

Именно потому при определении понятия «информационная безопасность» на первое место ставится защита информации от различных воздействий. Поэтому под защитой информации понимается комплекс мероприятий, направленных на обеспечение информационной безопасности.

Согласно ГОСТ 350922–96, защита информации – это деятельность, направленная на предотвращение утечки защищаемой информации, не-

санкционированных и непреднамеренных воздействий на защищаемую информацию.

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

Исходя из этого, можно сделать следующие важные выводы:

• задачи по обеспечению информационной безопасности для разных категорий субъектов могут существенно различаться;

• информационная безопасность не сводится исключительно к защите от несанкционированного доступа к информации – это принципиально более широкое понятие.

При анализе проблематики, связанной с информационной безопасностью, необходимо учитывать специфику данного аспекта безопасности, состоящую в том, что информационная безопасность есть составная часть информационных технологий – области, развивающейся беспрецедентно высокими темпами. В области информационной безопасности важны не столько отдельные решения (законы, учебные курсы, программно-технические изделия), находящиеся на современном уровне, сколько механизмы генерации новых решений, позволяющие как минимум адекватно реагировать на угрозы информационной безопасности или предвидеть новые угрозы и уметь им противостоять.

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

Согласно определению, компьютерная безопасность зависит не только от компьютеров, но и от поддерживающей инфраструктуры, к кото-

рой можно отнести системы электроснабжения, жизнеобеспечения, вентиляции, средства коммуникаций, а также обслуживающий персонал.

Как уже было отмечено ранее, информационная безопасность – многогранная область деятельности, в которой успех может принести только систематический, комплексный подход.

Создание режима информационной безопасности в большинстве случаев связано с комплексным решением трех задач по обеспечению:

1) доступности информации;

2) целостности информации;

3) конфиденциальности информации.

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

Доступность информации

Информационные системы создаются для получения определенных информационных услуг. Если по тем или иным причинам предоставить эти услуги пользователям становится невозможно, то это, очевидно, наносит ущерб всем пользователям.

Роль доступности информации особенно ярко проявляется в разного рода системах управления – производством, транспортом и т. п. Менее драматичные, но также весьма неприятные последствия – и материальные, и моральные – может иметь длительная недоступность информационных услуг, которыми пользуется большое количество людей, например продажа железнодорожных и авиабилетов, банковские услуги, доступ в информационную сеть Интернет и т. п.

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

Фактор времени в определении доступности информации в ряде случаев является очень важным, поскольку некоторые виды информации и информационных услуг имеют смысл только в определенный промежуток времени. Например, получение заранее заказанного билета на самолет после его вылета теряет всякий смысл. Точно так же получение прогноза погоды на вчерашний день не имеет никакого смысла, поскольку это событие уже наступило.

Целостность информации

Целостность информации условно подразделяется на статическую и динамическую. Статическая целостность информации предполагает не-

изменность информационных объектов от их исходного состояния, определяемого автором или источником информации.

Динамическая целостность информации включает вопросы корректного выполнения сложных действий с информационными потоками, например, анализ потока сообщений для выявления некорректных, контроль правильности передачи сообщений, подтверждение отдельных сообщений и др.

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

Так, ошибка в управляющей программе приведет к остановке управляемой системы, неправильная трактовка закона может привести к его нарушениям; точно так же неточный перевод инструкции по применению лекарственного препарата может нанести вред здоровью. Все эти примеры иллюстрируют нарушение целостности информации, что может привести к катастрофическим последствиям. Именно поэтому целостность информации выделяется в качестве одной из базовых составляющих информационной безопасности.

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

Конфиденциальность информации

Конфиденциальность – самый проработанный у нас в стране аспект информационной безопасности. К сожалению, практическая реализация мер по обеспечению конфиденциальности современных информационных систем в России связана с серьезными трудностями. Во-первых, сведения о технических каналах утечки информации являются закрытыми, так что большинство пользователей лишено возможности составить представление о потенциальных рисках. Во-вторых, на пути пользовательской криптографии как основного средства обеспечения конфиденциальности стоят многочисленные законодательные и технические проблемы.

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

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

Нарушение каждой из трех составляющих приводит к нарушению информационной безопасности в целом. Так, нарушение доступности приводит к отказу в доступе к информации, нарушение целостности имеет следствием фальсификацию информации, и, наконец, нарушение конфиденциальности влечет за собой раскрытие информации.

Выделение этих категорий в качестве базовых составляющих информационной безопасности обусловлено необходимостью реализации комплексного подхода при обеспечении режима информационной безопасности. Кроме того, нарушение одной из этих категорий может привести к нарушению или полной бесполезности двух других. Например, хищение пароля для доступа к компьютеру (нарушение конфиденциальности) может привести к его блокировке, уничтожению данных (нарушение доступности информации) или фальсификации информации, содержащейся в памяти компьютера (нарушение целостности информации).

3.2. Уровни формирования режима информационной безопасности. Задачи информационной безопасности общества

Анализ основ информационной безопасности показал, что обеспечение режима информационной безопасности является задачей комплексной. С одной стороны, информационная безопасность предполагает как минимум обеспечение трех ее составляющих – доступности, целостности и конфиденциальности данных. И уже с учетом этого проблему информационной безопасности следует рассматривать комплексно. С другой стороны, информацией и информационными системами в буквальном смысле «пронизаны» все сферы общественной деятельности, и влияние информации на общество все нарастает, поэтому обеспечение информационной безопасности также требует комплексного подхода.

В этой связи вполне закономерным является рассмотрение проблемы обеспечения информационной безопасности на нескольких уровнях, которые в совокупности обеспечивали бы защиту информации и информационных систем от вредных воздействий, наносящих ущерб субъектам информационных отношений.

Рассматривая проблему информационной безопасности в *широком смысле,* можно отметить, что в этом случае речь идет об информационной безопасности всего общества и его жизнедеятельности, при этом на информационную безопасность возлагается задача по минимизации всех отрицательных последствий от всеобщей информатизации и содействию развития всего общества при использовании информации как ресурса его развития.

В этой связи основными задачами информационной безопасности в широком смысле являются:

- защита государственной тайны, т. е. секретной и другой конфиденциальной информации, являющейся собственностью государства, от всех видов несанкционированного доступа, манипулирования и уничтожения;
- защита прав граждан на владение, распоряжение и управление принадлежащей им информацией;
- защита прав предпринимателей при осуществлении ими коммерческой деятельности;
- защита конституционных прав граждан на тайну переписки, переговоров, личную тайну.

Рассматривая проблему информационной безопасности в *узком смысле*, отметим, что в этом случае речь идет о совокупности методов и средств защиты информации и ее материальных носителей, направленных на обеспечение целостности, конфиденциальности и доступности информации.

Выделим следующие задачи информационной безопасности:

- защита технических и программных средств информатизации от ошибочных действий персонала и техногенных воздействий, а также стихийных бедствий;
- защита технических и программных средств информатизации от преднамеренных воздействий.

Можно выделить три *уровня формирования режима информационной безопасности:*

- законодательно-правовой;
- административный (организационный);
- программно-технический.

Законодательно-правовой уровень включает комплекс законодательных и иных правовых актов, устанавливающих правовой статус субъектов информационных отношений, субъектов и объектов защиты, мето-

ды, формы и способы защиты, их правовой статус. Кроме того, к этому уровню относятся стандарты и спецификации в области информационной безопасности. Система законодательных актов и разработанных на их базе нормативных и организационно-распорядительных документов должна обеспечивать организацию эффективного надзора за их исполнением со стороны правоохранительных органов и реализацию мер судебной защиты и ответственности субъектов информационных отношений. К этому уровню можно отнести и морально-этические нормы поведения, которые сложились традиционно или складываются по мере распространения вычислительных средств в обществе. Морально-этические нормы могут быть регламентированы в законодательном порядке, т. е. в виде свода правил и предписаний.

Административный уровень включает комплекс взаимокоординируемых мероприятий и технических мер, реализующих практические механизмы защиты в процессе создания и эксплуатации систем защиты информации. Организационный уровень должен охватывать все структурные элементы систем обработки данных на всех этапах их жизненного цикла: строительство помещений, проектирование системы, монтаж и наладка оборудования, испытания и проверки, эксплуатация.

Программно-технический уровень включает три подуровня: физический, технический (аппаратный) и программный. Физический подуровень решает задачи с ограничением физического доступа к информации и информационным системам, соответственно, к нему относятся технические средства, реализуемые в виде автономных устройств и систем, не связанных с обработкой, хранением и передачей информации: система охранной сигнализации, система наблюдения, средства физического воспрепятствования доступу (замки, ограждения, решетки и т. д.).

Средства защиты аппаратного и программного подуровней непосредственно связаны с системой обработки информации. Эти средства либо встроены в аппаратные средства обработки, либо сопряжены с ними по стандартному интерфейсу. К аппаратным средствам относятся схемы контроля информации по четности, схемы доступа по ключу и т. д. К программным средствам защиты, образующим программный подуровень, относятся специальное программное обеспечение, используемое для защиты информации, например антивирусный пакет и т. д. Программы защиты могут быть как отдельными, так и встроенными. Так, шифрование данных можно

выполнить встроенной в операционную систему файловой шифрующей системой EP8 или при помощи специальной программы шифрования.

Формирование режима информационной безопасности является сложной системной задачей, решение которой в разных странах различается по содержанию и зависит от таких факторов, как научный потенциал страны, степень внедрения средств информатизации в жизнь общества и экономику, развитие производственной базы, общей культуры общества и, наконец, традиций и норм поведения.

3.3. Нормативно-правовые основы информационной безопасности в Российской Федерации

Законодательные меры в сфере информационной безопасности направлены на создание в стране законодательной базы, упорядочивающей и регламентирующей поведение субъектов и объектов информационных отношений, а также определяющей ответственность за нарушение установленных норм.

Деятельность по созданию нормативной базы предусматривает разработку новых или корректировку существующих законов, положений, постановлений и инструкций, а также создание действенной системы контроля за исполнением указанных документов. Необходимо отметить, что такая работа в последнее время ведется практически непрерывно, поскольку сфера информационных технологий развивается стремительно, соответственно, появляются новые формы информационных отношений, существование которых должно быть определено законодательно.

Законодательная база в сфере информационной безопасности включает пакет федеральных законов, указов Президента РФ, постановлений Правительства РФ, межведомственных руководящих документов и стандартов.

Основополагающими документами по информационной безопасности в РФ являются Конституция РФ и Концепция национальной безопасности.

В Конституции РФ гарантируется тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (ст. 23, ч. 2), а также право свободно искать, получать, передавать, производить и распространять информацию любым законным способом (ст. 29, ч. 4). Кроме этого Конституцией РФ гарантируется свобода массовой информации (ст. 29, ч. 5), т. е. массовая информация должна быть доступна гражданам.

Концепция национальной безопасности РФ, введенная Указом Президента РФ № 24 в январе 2000 г., определяет следующие важнейшие задачи обеспечения информационной безопасности Российской Федерации:

• реализация конституционных прав и свобод граждан Российской Федерации в сфере информационной деятельности;

• совершенствование и защита отечественной информационной инфраструктуры, интеграция России в мировое информационное пространство;

• противодействие угрозе развязывания противоборства в информационной сфере.

Для обеспечения прав граждан в сфере информационных технологий и решения задач информационной безопасности, сформулированных в Концепции национальной безопасности РФ, разработаны и продолжают разрабатываться и совершенствоваться нормативные документы в сфере информационных технологий.

Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации следующие.

Закон Российской Федерации от 21 июля 1993 г. № 5485–1 «О государственной тайне» с изменениями и дополнениями, внесенными после его принятия, регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации.

В законе определены следующие основные понятия:

• **государственная тайна** – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации;

• **носители сведений, составляющих государственную тайну,** – материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов;

• **система защиты государственной тайны** – совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях;

• **доступ к сведениям, составляющим государственную тайну,** – санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну;

• **гриф секретности** – реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него;

• **средства защиты информации** – технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

Законом определено, что средства защиты информации должны иметь сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности.

Организация сертификации средств защиты информации возлагается на Государственную техническую комиссию при Президенте Российской Федерации, Федеральную службу безопасности Российской Федерации, Министерство обороны Российской Федерации в соответствии с функциями, возложенными на них законодательством Российской Федерации.

Закон РФ «Об информации, информатизации и защите информации» от 20 февраля 1995 г. № 24-ФЗ является одним из основных базовых законов в области защиты информации, который регламентирует отношения, возникающие при формировании и использовании информационных ресурсов Российской Федерации на основе сбора, накопления, хранения, распространения и предоставления потребителям документированной информации, а также при создании и использовании информационных технологий, при защите информации и прав субъектов, участвующих в информационных процессах и информатизации.

Основными задачами системы защиты информации, нашедшими отражение в Законе «Об информации, информатизации и защите информации», являются:

• предотвращение утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования, блокирования информации и т. п., вмешательства в информацию и информационные системы;

• сохранение полноты, достоверности, целостности информации, ее массивов и программ обработки данных, установленных собственником или уполномоченным им лицом;

• сохранение возможности управления процессом обработки, пользования информацией в соответствии с условиями, установленными собственником или владельцем информации;

• обеспечение конституционных прав граждан на сохранение личной тайны и конфиденциальности персональной информации, накапливаемой в банках данных;

• сохранение секретности или конфиденциальности информации в соответствии с правилами, установленными действующим законодательством и другими законодательными или нормативными актами;

• соблюдение прав авторов программно-информационной продукции, используемой в информационных системах.

В соответствии с законом:

• информационные ресурсы делятся на государственные и негосударственные (ст. 6, ч. 1);

• государственные информационные ресурсы являются открытыми и общедоступными. Исключение составляет документированная информация, отнесенная законом к категории ограниченного доступа (ст. 10, ч. 1);

• документированная информация с ограниченными правами доступа по условиям ее правового режима подразделяется на информацию, отнесенную к государственной тайне, и конфиденциальную (ст. 10, ч. 2).

Закон определяет пять *категорий государственных информационных ресурсов:*

• открытая общедоступная информация во всех областях знаний и деятельности;

• информация с ограниченным доступом;

• информация, отнесенная к государственной тайне;

• конфиденциальная информация;

• персональные данные о гражданах (относятся к категории конфиденциальной информации, но регламентируются отдельным законом).

Ст. 22 Закона «Об информации, информатизации и защите информации» определяет права и обязанности субъектов в области защиты информации. В частности, пп. 2 и 5 обязывают владельца информационной системы обеспечивать необходимый уровень защиты конфиденциальной информации и оповещать собственников информационных ресурсов о фактах нарушения режима защиты информации.

Следует отметить, что процесс законотворчества идет достаточно сложно. Если в вопросах защиты государственной тайны создана более или менее надежная законодательная система, то в вопросах защиты частной информации существует достаточно много противоречий и «нестыковок».

При разработке и использовании законодательных и других правовых и нормативных документов, а также при организации защиты информации важно правильно ориентироваться во всем блоке действующей законодательной базы в этой области.

Проблемы, связанные с правильной трактовкой и применением законодательства Российской Федерации, периодически возникают в практической работе по организации защиты информации от ее утечки по техническим каналам, от несанкционированного доступа к информации и от воздействий на нее при обработке в технических средствах информатизации, а также в ходе контроля эффективности принимаемых мер защиты.

Немаловажная роль в системе правового регулирования информационных отношений отводится ответственности субъектов за нарушения в сфере информационной безопасности.

Основными документами в этом направлении являются:

- Уголовный кодекс Российской Федерации;
- Кодекс Российской Федерации об административных правонарушениях.

В принятом в 1996 г. Уголовном кодексе Российской Федерации как наиболее «сильнодействующем» законодательном акте по предупреждению преступлений и привлечению преступников и нарушителей к уголовной ответственности вопросам безопасности информации посвящены следующие главы и статьи.

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

Ст. 140. Отказ в предоставлении гражданину информации.

Ст. 183. Незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну.

Ст. 237. Сокрытие информации об обстоятельствах, создающих опасность для жизни и здоровья людей.

Ст. 283. Разглашение государственной тайны.

Ст. 284. Утрата документов, содержащих государственную тайну.

Особое внимание уделяется компьютерным преступлениям, ответственность за которые предусмотрена в специальной главе – гл. 28 кодекса «Преступления в сфере компьютерной информации». Гл. 28 включает следующие статьи:

Ст. 272. Неправомерный доступ к компьютерной информации:

1. Неправомерный доступ к охраняемой законом компьютерной информации, т. е. 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 другого 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.

Ст. 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, наказывается 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.

Ст. 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.

3.4. Особенности обеспечения информационной безопасности Российской Федерации в различных сферах общественной жизни

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

В каждой из них имеются свои особенности обеспечения информационной безопасности, связанные со спецификой объектов обеспечения безопасности, степенью их уязвимости в отношении угроз информационной безопасности Российской Федерации. В каждой сфере жизнедеятельности общества и государства наряду с общими методами обеспечения информационной безопасности Российской Федерации могут использоваться частные методы и формы, обусловленные спецификой факторов, влияющих на состояние информационной безопасности Российской Федерации.

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

- система государственной статистики;
- кредитно-финансовая система;

• информационные и учетные автоматизированные системы подразделений федеральных органов исполнительной власти, обеспечивающих деятельность общества и государства в сфере экономики;

• системы бухгалтерского учета предприятий, учреждений и организаций независимо от формы собственности;

• системы сбора, обработки, хранения и передачи финансовой, биржевой, налоговой, таможенной информации и информации о внешнеэкономической деятельности государства, а также предприятий, учреждений и организаций независимо от формы собственности.

Переход к рыночным отношениям в экономике вызвал появление на внутреннем российском рынке товаров и услуг множества отечественных и зарубежных коммерческих структур – производителей и потребителей информации, средств информатизации и защиты информации. Бесконтрольная деятельность этих структур по созданию и защите систем сбора, обработки, хранения и передачи статистической, финансовой, биржевой, налоговой, таможенной информации создает реальную угрозу безопасности России в экономической сфере. Аналогичные угрозы возникают при бесконтрольном привлечении иностранных фирм к созданию подобных систем, поскольку при этом складываются благоприятные условия для несанкционированного доступа к конфиденциальной экономической информации и для контроля за процессами ее передачи и обработки со стороны иностранных спецслужб.

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

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

Недостаточность нормативной правовой базы, определяющей ответственность хозяйствующих субъектов за недостоверность или сокрытие сведений об их коммерческой деятельности, о потребительских свойствах производимых ими товаров и услуг, о результатах их хозяйственной деятельности, об инвестициях и тому подобном, препятствует нормальному

функционированию хозяйствующих субъектов. В то же время существенный экономический ущерб хозяйствующим субъектам может быть нанесен вследствие разглашения информации, содержащей коммерческую тайну. В системах сбора, обработки, хранения и передачи финансовой, биржевой, налоговой, таможенной информации наиболее опасны противоправное копирование информации и ее искажение вследствие преднамеренных или случайных нарушений технологии работы с информацией, несанкционированного доступа к ней. Это касается и федеральных органов исполнительной власти, занятых формированием и распространением информации о внешнеэкономической деятельности Российской Федерации.

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

• организация и осуществление государственного контроля за созданием, развитием и защитой систем и средств сбора, обработки, хранения и передачи статистической, финансовой, биржевой, налоговой, таможенной информации;

• коренная перестройка системы государственной статистической отчетности в целях обеспечения достоверности, полноты и защищенности информации, осуществляемая путем введения строгой юридической ответственности должностных лиц за подготовку первичной информации, организацию контроля за деятельностью этих лиц и служб обработки и анализа статистической информации, а также путем ограничения коммерциализации такой информации;

• разработка национальных сертифицированных средств защиты информации и внедрение их в системы и средства сбора, обработки, хранения и передачи статистической, финансовой, биржевой, налоговой, таможенной информации;

• разработка и внедрение национальных защищенных систем электронных платежей на базе интеллектуальных карт, систем электронных денег и электронной торговли, стандартизация этих систем, а также разработка нормативной правовой базы, регламентирующей их использование;

• совершенствование нормативной правовой базы, регулирующей информационные отношения в сфере экономики;

• совершенствование методов отбора и подготовки персонала для работы в системах сбора, обработки, хранения и передачи экономической информации.

Наиболее важными объектами обеспечения информационной безопасности Российской Федерации **в сфере внутренней политики** являются:

• конституционные права и свободы человека и гражданина;

• конституционный строй, национальное согласие, стабильность государственной власти, суверенитет и территориальная целостность Российской Федерации;

• открытые информационные ресурсы федеральных органов исполнительной власти и средств массовой информации.

Наибольшую опасность в сфере внутренней политики представляют следующие угрозы информационной безопасности Российской Федерации:

• нарушение конституционных прав и свобод граждан, реализуемых в информационной сфере;

• недостаточное правовое регулирование отношений в области прав различных политических сил на использование средств массовой информации для пропаганды своих идей;

• распространение дезинформации о политике Российской Федерации, деятельности федеральных органов государственной власти, событиях, происходящих в стране и за рубежом;

• деятельность общественных объединений, направленная на насильственное изменение основ конституционного строя и нарушение целостности Российской Федерации, разжигание социальной, расовой, национальной и религиозной вражды, на распространение этих идей в средствах массовой информации.

Основными мероприятиями в области обеспечения информационной безопасности Российской Федерации в сфере внутренней политики являются:

• создание системы противодействия монополизации отечественными и зарубежными структурами составляющих информационной инфраструктуры, включая рынок информационных услуг и средства массовой информации;

• активизация контрпропагандистской деятельности, направленной на предотвращение негативных последствий распространения дезинформации о внутренней политике России.

К наиболее важным объектам обеспечения информационной безопасности Российской Федерации **в сфере внешней политики** относятся:

• информационные ресурсы федеральных органов исполнительной власти, реализующих внешнюю политику Российской Федерации, российских представительств и организаций за рубежом, представительств Российской Федерации при международных организациях;

• информационные ресурсы представительств федеральных органов исполнительной власти, реализующих внешнюю политику Российской Федерации, на территориях субъектов Российской Федерации;

• информационные ресурсы российских предприятий, учреждений и организаций, подведомственных федеральным органам исполнительной власти, реализующим внешнюю политику Российской Федерации;

Из внешних угроз информационной безопасности Российской Федерации в сфере внешней политики наибольшую опасность представляют:

• блокирование деятельности российских средств массовой информации по разъяснению зарубежной аудитории целей и основных направлений государственной политики Российской Федерации, ее мнения по социально значимым событиям российской и международной жизни;

• информационное воздействие иностранных политических, экономических, военных и информационных структур на разработку и реализацию стратегии внешней политики Российской Федерации;

• распространение за рубежом дезинформации о внешней политике Российской Федерации;

• нарушение прав российских граждан и юридических лиц в информационной сфере за рубежом;

• попытки несанкционированного доступа к информации и воздействия на информационные ресурсы, информационную инфраструктуру федеральных органов исполнительной власти, реализующих внешнюю политику Российской Федерации, российских представительств и организаций за рубежом, представительств Российской Федерации при международных организациях.

Из внутренних угроз информационной безопасности Российской Федерации в сфере внешней политики наибольшую опасность представляют:

• нарушение установленного порядка сбора, обработки, хранения и передачи информации в федеральных органах исполнительной власти, реализующих внешнюю политику Российской Федерации, и на подведомственных им предприятиях, в учреждениях и организациях;

• информационно-пропагандистская деятельность политических сил, общественных объединений, средств массовой информации и отдельных лиц, искажающая стратегию и тактику внешнеполитической деятельности Российской Федерации;

• недостаточная информированность населения о внешнеполитической деятельности Российской Федерации.

Основными мероприятиями по обеспечению информационной безопасности Российской Федерации в сфере внешней политики являются:

• разработка основных направлений государственной политики в области совершенствования информационного обеспечения внешнеполитического курса Российской Федерации;

• разработка и реализация комплекса мер по усилению информационной безопасности информационной инфраструктуры федеральных органов исполнительной власти, реализующих внешнюю политику Российской Федерации, российских представительств и организаций за рубежом, представительств Российской Федерации при международных организациях;

• создание российским представительствам и организациям за рубежом условий для работы по нейтрализации распространяемой там дезинформации о внешней политике Российской Федерации;

• совершенствование информационного обеспечения работы по противодействию нарушениям прав и свобод российских граждан и юридических лиц за рубежом;

• совершенствование информационного обеспечения субъектов Российской Федерации по вопросам внешнеполитической деятельности, которые входят в их компетенцию.

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

• результаты фундаментальных, поисковых и прикладных научных исследований, потенциально важные для научно-технического, технологического и социально-экономического развития страны, включая сведения, утрата которых может нанести ущерб национальным интересам и престижу Российской Федерации;

• открытия, незапатентованные технологии, промышленные образцы, полезные модели и экспериментальное оборудование;

• научно-технические кадры и система их подготовки;

• системы управления сложными исследовательскими комплексами (ядерными реакторами, ускорителями элементарных частиц, плазменными генераторами и др.).

К числу основных внешних угроз информационной безопасности Российской Федерации в области науки и техники следует отнести:

• стремление развитых иностранных государств получить противоправный доступ к научно-техническим ресурсам России для использования полученных российскими учеными результатов в собственных интересах;

• создание льготных условий на российском рынке для иностранной научно-технической продукции и стремление развитых стран в то же время ограничить развитие научно-технического потенциала России (скупка акций передовых предприятий с их последующим перепрофилированием, сохранение экспортно-импортных ограничений и т. п.);

• политику западных стран, направленную на дальнейшее разрушение унаследованного от СССР единого научно-технического пространства государств – участников Содружества Независимых Государств за счет переориентации на западные страны их научно-технических связей, а также отдельных наиболее перспективных научных коллективов;

• активизацию деятельности иностранных государственных и коммерческих предприятий, учреждений и организаций в области промышленного шпионажа с привлечением к ней разведывательных и специальных служб.

К числу основных внутренних угроз информационной безопасности Российской Федерации в области науки и техники следует отнести:

• сохраняющуюся сложную экономическую ситуацию в России, ведущую к резкому снижению финансирования научно-технической деятельности, временному падению престижа научно-технической сферы, утечке за рубеж идей и передовых разработок;

• неспособность предприятий национальных отраслей электронной промышленности производить на базе новейших достижений микроэлектроники, передовых информационных технологий конкурентоспособную наукоемкую продукцию, позволяющую обеспечить достаточный уровень технологической независимости России от зарубежных стран, что приводит к вынужденному широкому использованию импортных программно-аппаратных средств при создании и развитии в России информационной инфраструктуры;

• серьезные проблемы в области патентной защиты результатов научно-технической деятельности российских ученых;

• сложности реализации мероприятий по защите информации, особенно на акционированных предприятиях, в научно-технических учреждениях и организациях.

Реальный путь противодействия угрозам информационной безопасности Российской Федерации в области науки и техники – это совершенствование законодательства Российской Федерации, регулирующего отношения в данной области, и механизмов его реализации.

В этих целях государство должно способствовать созданию системы оценки возможного ущерба от реализации угроз наиболее важным объектам обеспечения информационной безопасности Российской Федерации в области науки и техники, включая общественные научные советы и организации независимой экспертизы, вырабатывающие рекомендации для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации по предотвращению противоправного или неэффективного использования интеллектуального потенциала России.

Обеспечение информационной безопасности Российской Федерации **в сфере духовной жизни** имеет целью защиту конституционных прав и свобод человека и гражданина, связанных с развитием, формированием и поведением личности, свободой массового информирования, использования культурного, духовно-нравственного наследия, исторических традиций и норм общественной жизни, с сохранением культурного достояния всех народов России, реализацией конституционных ограничений прав и свобод человека и гражданина в интересах сохранения и укрепления нравственных ценностей общества, традиций патриотизма и гуманизма, здоровья граждан, культурного и научного потенциала Российской Федерации, обеспечения обороноспособности и безопасности государства.

К числу основных объектов обеспечения информационной безопасности Российской Федерации в сфере духовной жизни относятся:

• достоинство личности, свобода совести, включая право свободно выбирать, иметь и распространять религиозные и иные убеждения и действовать в соответствии с ними, свобода мысли и слова (за исключением пропаганды или агитации, возбуждающей социальную, расовую, национальную или религиозную ненависть и вражду), а также свобода литературно-

го, художественного, научного, технического и других видов творчества, преподавания;

• свобода массовой информации;

• неприкосновенность частной жизни, личная и семейная тайна;

• русский язык как фактор духовного единения народов многонациональной России, язык межгосударственного общения народов государств – участников Содружества Независимых Государств;

• языки, нравственные ценности и культурное наследие народов и народностей Российской Федерации;

• объекты интеллектуальной собственности.

Наибольшую опасность в сфере духовной жизни представляют следующие угрозы информационной безопасности Российской Федерации:

• деформация системы массового информирования как за счет монополизации средств массовой информации, так и за счет неконтролируемого расширения сектора зарубежных средств массовой информации в отечественном информационном пространстве;

• ухудшение состояния и постепенный упадок объектов российского культурного наследия, включая архивы, музейные фонды, библиотеки, памятники архитектуры, ввиду недостаточного финансирования соответствующих программ и мероприятий;

• возможность нарушения общественной стабильности, нанесение вреда здоровью и жизни граждан вследствие деятельности религиозных объединений, проповедующих религиозный фундаментализм, а также тоталитарных религиозных сект;

• использование зарубежными специальными службами средств массовой информации, действующих на территории Российской Федерации, для нанесения ущерба обороноспособности страны и безопасности государства, распространения дезинформации;

• неспособность современного гражданского общества России обеспечить формирование у подрастающего поколения и поддержание в обществе общественно необходимых нравственных ценностей, патриотизма и гражданской ответственности за судьбу страны.

Основными направлениями обеспечения информационной безопасности Российской Федерации в сфере духовной жизни являются:

• развитие в России основ гражданского общества;

• создание социально-экономических условий для осуществления творческой деятельности и функционирования учреждений культуры;

• выработка цивилизованных форм и способов общественного контроля за формированием в обществе духовных ценностей, отвечающих национальным интересам страны, воспитанием патриотизма и гражданской ответственности за ее судьбу;

• совершенствование законодательства Российской Федерации, регулирующего отношения в области конституционных ограничений прав и свобод человека и гражданина;

• государственная поддержка мероприятий по сохранению и возрождению культурного наследия народов и народностей Российской Федерации;

• формирование правовых и организационных механизмов обеспечения конституционных прав и свобод граждан, повышения их правовой культуры в интересах противодействия сознательному или непреднамеренному нарушению этих конституционных прав и свобод в сфере духовной жизни;

• разработка действенных организационно-правовых механизмов доступа средств массовой информации и граждан к открытой информации о деятельности федеральных органов государственной власти и общественных объединений, обеспечение достоверности сведений о социально значимых событиях общественной жизни, распространяемых через средства массовой информации;

• разработка специальных правовых и организационных механизмов недопущения противоправных информационно-психологических воздействий на массовое сознание общества, неконтролируемой коммерциализации культуры и науки, а также механизмов, обеспечивающих сохранение культурных и исторических ценностей народов и народностей Российской Федерации, рациональное использование накопленных обществом информационных ресурсов, составляющих национальное достояние;

• введение запрета на использование эфирного времени в электронных средствах массовой информации для проката программ, пропагандирующих насилие и жестокость, антиобщественное поведение;

• противодействие негативному влиянию иностранных религиозных организаций и миссионеров.

Основными объектами обеспечения информационной безопасности Российской Федерации **в общегосударственных информационных и телекоммуникационных системах** являются:

• информационные ресурсы, содержащие сведения, отнесенные к государственной тайне, и конфиденциальную информацию;

• средства и системы информатизации (средства вычислительной техники, информационно-вычислительные комплексы, сети и системы), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), автоматизированные системы управления, системы связи и передачи данных, осуществляющие прием, обработку, хранение и передачу информации ограниченного доступа, их информативные физические поля;

• технические средства и системы, обрабатывающие открытую информацию, но размещенные в помещениях, в которых обрабатывается информация ограниченного доступа, а также сами помещения, предназначенные для обработки такой информации;

• помещения, предназначенные для ведения закрытых переговоров, а также переговоров, в ходе которых оглашаются сведения ограниченного доступа.

Основными угрозами информационной безопасности Российской Федерации в общегосударственных информационных и телекоммуникационных системах являются:

• деятельность специальных служб иностранных государств, преступных сообществ, организаций и групп, противозаконная деятельность отдельных лиц, направленная на получение несанкционированного доступа к информации и осуществление контроля за функционированием информационных и телекоммуникационных систем;

• нарушение установленного регламента сбора, обработки и передачи информации, преднамеренные действия и ошибки персонала информационных и телекоммуникационных систем, отказ технических средств и сбои программного обеспечения в информационных и телекоммуникационных системах;

• использование не сертифицированных в соответствии с требованиями безопасности средств и систем информатизации и связи, а также средств защиты информации и контроля их эффективности;

• привлечение к работам по созданию, развитию и защите информационных и телекоммуникационных систем организаций и фирм, не имеющих государственных лицензий на осуществление этих видов деятельности.

Основными направлениями обеспечения информационной безопасности Российской Федерации в общегосударственных информационных и телекоммуникационных системах являются:

• предотвращение перехвата информации из помещений и с объектов, а также информации, передаваемой по каналам связи с помощью технических средств;

• исключение несанкционированного доступа к обрабатываемой или хранящейся в технических средствах информации;

• предотвращение утечки информации по техническим каналам, возникающей при эксплуатации технических средств ее обработки, хранения и передачи;

• предотвращение специальных программно-технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств информатизации;

• обеспечение информационной безопасности при подключении общегосударственных информационных и телекоммуникационных систем к внешним информационным сетям, включая международные;

• обеспечение безопасности конфиденциальной информации при взаимодействии информационных и телекоммуникационных систем различных классов защищенности;

• выявление внедренных на объекты и в технические средства электронных устройств перехвата информации.

Основными организационно-техническими мероприятиями по защите информации в общегосударственных информационных и телекоммуникационных системах являются:

• лицензирование деятельности организаций в области защиты информации;

• аттестация объектов информатизации по выполнению требований обеспечения защиты информации при проведении работ, связанных с использованием сведений, составляющих государственную тайну;

• сертификация средств защиты информации и контроля эффективности их использования, а также защищенности информации от утечки по техническим каналам систем и средств информатизации и связи;

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

• создание и применение информационных и автоматизированных систем управления в защищенном исполнении.

К объектам обеспечения информационной безопасности Российской Федерации **в сфере обороны** относятся: информационная инфраструктура центральных органов военного управления и органов военного управления видов Вооруженных сил Российской Федерации и родов войск, объединений, соединений, воинских частей и организаций, входящих в Вооруженные силы Российской Федерации, научно-исследовательских учреждений Министерства обороны Российской Федерации;

• информационные ресурсы предприятий оборонного комплекса и научно-исследовательских учреждений, выполняющих государственные оборонные заказы либо занимающихся оборонной проблематикой;

• программно-технические средства автоматизированного управления войсками и оружием, вооружения и военной техники, оснащенных средствами информатизации;

• информационные ресурсы, системы связи и информационная инфраструктура других войск, воинских формирований и органов.

Внешними угрозами, представляющими наибольшую опасность для объектов обеспечения информационной безопасности Российской Федерации в сфере обороны, являются:

• все виды разведывательной деятельности зарубежных государств;

• информационно-технические воздействия (в том числе радиоэлектронная борьба, проникновение в компьютерные сети) со стороны вероятных противников;

• диверсионно-подрывная деятельность специальных служб иностранных государств, осуществляемая методами информационно-психологического воздействия;

• деятельность иностранных политических, экономических и военных структур, направленная против интересов Российской Федерации в сфере обороны.

Внутренними угрозами, представляющими наибольшую опасность для указанных объектов, являются:

• нарушение установленного регламента сбора, обработки, хранения и передачи информации, находящейся в штабах и учреждениях Министерства обороны Российской Федерации, на предприятиях оборонного комплекса;

• преднамеренные действия, а также ошибки персонала информационных и телекоммуникационных систем специального назначения;

• ненадежное функционирование информационных и телекоммуникационных систем специального назначения;

• возможная информационно-пропагандистская деятельность, подрывающая престиж Вооруженных сил Российской Федерации и их боеготовность;

• нерешенность вопросов защиты интеллектуальной собственности предприятий оборонного комплекса, приводящая к утечке за рубеж ценнейших государственных информационных ресурсов;

• нерешенность вопросов социальной защиты военнослужащих и членов их семей.

Перечисленные внутренние угрозы будут представлять особую опасность в условиях обострения военно-политической обстановки.

Главными специфическими направлениями совершенствования системы обеспечения информационной безопасности Российской Федерации в сфере обороны являются:

• систематическое выявление угроз и их источников, структуризация целей обеспечения информационной безопасности в сфере обороны и определение соответствующих практических задач;

• проведение сертификации общего и специального программного обеспечения, пакетов прикладных программ и средств защиты информации в существующих и создаваемых автоматизированных системах управления военного назначения и системах связи, имеющих в своем составе элементы вычислительной техники;

• постоянное совершенствование средств защиты информации от несанкционированного доступа, развитие защищенных систем связи и управления войсками и оружием, повышение надежности специального программного обеспечения;

• совершенствование структуры функциональных органов системы обеспечения информационной безопасности в сфере обороны и координация их взаимодействия;

• совершенствование приемов и способов стратегической и оперативной маскировки, разведки и радиоэлектронной борьбы, методов и средств активного противодействия информационно-пропагандистским и психологическим операциям вероятного противника;

• подготовка специалистов в области обеспечения информационной безопасности в сфере обороны.

К наиболее важным объектам обеспечения информационной безопасности **в правоохранительной и судебной сферах** относятся:

• информационные ресурсы федеральных органов исполнительной власти, реализующих правоохранительные функции, судебных органов, их информационно-вычислительных центров, научно-исследовательских учреждений и учебных заведений, содержащие специальные сведения и оперативные данные служебного характера;

• информационно-вычислительные центры, их информационное, техническое, программное и нормативное обеспечение;

• информационная инфраструктура (информационно-вычислительные сети, пункты управления, узлы и линии связи).

Внешними угрозами, представляющими наибольшую опасность для объектов обеспечения информационной безопасности в правоохранительной и судебной сферах, являются:

• разведывательная деятельность специальных служб иностранных государств, международных преступных сообществ, организаций и групп, связанная со сбором сведений, раскрывающих задачи, планы деятельности, техническое оснащение, методы работы и места дислокации специальных подразделений и органов внутренних дел Российской Федерации;

• деятельность иностранных государственных и частных коммерческих структур, стремящихся получить несанкционированный доступ к информационным ресурсам правоохранительных и судебных органов.

Внутренними угрозами, представляющими наибольшую опасность для указанных объектов, являются:

• нарушение установленного регламента сбора, обработки, хранения и передачи информации, содержащейся в картотеках и автоматизированных банках данных и использующейся для расследования преступлений;

• недостаточность законодательного и нормативного регулирования информационного обмена в правоохранительной и судебной сферах;

• отсутствие единой методологии сбора, обработки и хранения информации оперативно-розыскного, справочного, криминалистического и статистического характера;

• отказ технических средств и сбои программного обеспечения в информационных и телекоммуникационных системах;

• преднамеренные действия, а также ошибки персонала, непосредственно занятого формированием и ведением картотек и автоматизированных банков данных.

Наряду с широко используемыми общими методами и средствами защиты информации применяются также специфические методы и средства обеспечения информационной безопасности в правоохранительной и судебной сферах.

Главными из них являются:

• создание защищенной многоуровневой системы интегрированных банков данных оперативно-розыскного, справочного, криминалистического и статистического характера на базе специализированных информационно-телекоммуникационных систем;

• повышение уровня профессиональной и специальной подготовки пользователей информационных систем.

Наиболее уязвимыми объектами обеспечения информационной безопасности Российской Федерации **в условиях чрезвычайных ситуаций** являются система принятия решений по оперативным действиям (реакциям), связанным с развитием таких ситуаций и ходом ликвидации их последствий, а также система сбора и обработки информации о возможном возникновении чрезвычайных ситуаций.

Особое значение для нормального функционирования указанных объектов имеет обеспечение безопасности информационной инфраструктуры страны при авариях, катастрофах и стихийных бедствиях. Сокрытие, задержка поступления, искажение и разрушение оперативной информации, несанкционированный доступ к ней отдельных лиц или групп лиц могут привести к человеческим жертвам.

Отсутствие надлежащего функционирования всех элементов информационной инфраструктуры страны может привести к возникновению разного рода сложностей при ликвидации последствий чрезвычайной ситуации, связанных с особенностями информационного воздействия в экстремальных условиях: к приведению в движение больших масс людей, испытывающих психический стресс; к быстрому возникновению и распространению среди них паники и беспорядков на основе слухов, ложной или недостоверной информации.

К специфическим для данных условий направлениям обеспечения информационной безопасности относятся:

• разработка эффективной системы мониторинга объектов повышенной опасности, нарушение функционирования которых может привести

к возникновению чрезвычайных ситуаций, и прогнозирования чрезвычайных ситуаций;

• совершенствование системы информирования населения об угрозах возникновения чрезвычайных ситуаций, условиях их возникновения и развития;

• повышение надежности систем обработки и передачи информации, обеспечивающих деятельность федеральных органов исполнительной власти;

• прогнозирование поведения населения под воздействием ложной или недостоверной информации о возможных чрезвычайных ситуациях и выработка мер по оказанию помощи большим массам людей в условиях этих ситуаций;

• разработка специальных мер по защите информационных систем, обеспечивающих управление экологически опасными и экономически важными производствами.

Вопросы и задания для самоконтроля

1. Дайте понятие информационной безопасности.

2. Определите составляющие информационной безопасности.

3. Какие основные задачи призвана выполнять информационная безопасность?

4. Охарактеризуйте уровни формирования режима информационной безопасности.

5. Проанализируйте законодательную базу в сфере информационной безопасности и определите ее сильные и слабые стороны.

6. В чем заключаются особенности обеспечения информационной безопасности в различных сферах общественной жизни (политике, экономике, культуре и т. д.)?

Глава 4. КЛАССИФИКАЦИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1. Классы угроз информационной безопасности

4.2. Характер происхождения угроз: умышленные факторы, естественные факторы. Источники угроз

4.3. Каналы утечки информации: технические, электромагнитные, индукционные и др.

4.4. Вирусы как угроза информационной безопасности

4.1. Классы угроз информационной безопасности

Анализ и выявление угроз информационной безопасности является важной функцией административного уровня обеспечения информационной безопасности [22]. Во многом облик разрабатываемой системы защиты и состав механизмов ее реализации определяется потенциальными угрозами. Например, если пользователи вычислительной сети организации имеют доступ в Интернет, то количество угроз информационной безопасности резко возрастает, соответственно, это отражается на методах и средствах защиты.

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

Чаще всего угроза является следствием наличия уязвимых мест в защите информационных систем, например неконтролируемый доступ к персональным компьютерам или нелицензионное программное обеспечение (к сожалению, даже лицензионное программное обеспечение не лишено уязвимостей).

История развития информационных систем показывает, что новые уязвимые места появляются постоянно. С такой же регулярностью, но с небольшим отставанием появляются и средства защиты. В большинстве своем средства защиты появляются в ответ на возникающие угрозы. Такой подход к обеспечению безопасности малоэффективен, поскольку всегда существует промежуток времени между моментом выявления угрозы и ее

устранением. Именно в этот промежуток времени злоумышленник может нанести непоправимый вред информации.

В этой связи более приемлемым является другой способ – способ упреждающей защиты, заключающийся в разработке механизмов защиты от возможных, предполагаемых и потенциальных угроз.

Отметим, что некоторые угрозы нельзя считать следствием целенаправленных действий вредного характера. Существуют угрозы, вызванные случайными ошибками или техногенными явлениями.

Знание возможных угроз информационной безопасности, а также уязвимых мест системы защиты необходимо для того, чтобы выбрать наиболее экономичные и эффективные средства обеспечения безопасности.

Угрозы информационной безопасности классифицируются по нескольким признакам:

• **по составляющим информационной безопасности** (доступность, целостность, конфиденциальность), против которых в первую очередь направлены угрозы;

• **компонентам информационных систем,** на которые угрозы нацелены (данные, программы, аппаратура, персонал);

• **характеру воздействия** (случайные или преднамеренные, действия природного или техногенного характера);

• **по расположению источника угроз** (внутри или вне рассматриваемой информационной системы).

Отправной точкой при анализе угроз информационной безопасности является определение составляющей информационной безопасности, которая может быть нарушена той или иной угрозой: конфиденциальность, целостность или доступность.

Все виды угроз, классифицируемые по другим признакам, могут воздействовать на все составляющие информационной безопасности. Рассмотрим угрозы по характеру воздействия. Опыт проектирования, изготовления и эксплуатации информационных систем показывает, что информация подвергается различным случайным воздействиям на всех этапах цикла жизни системы.

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

• аварийные ситуации из-за стихийных бедствий и отключений электропитания (природные и техногенные воздействия);

• отказы и сбои аппаратуры;

• ошибки в программном обеспечении;

• ошибки в работе персонала;

• помехи в линиях связи из-за воздействий внешней среды.

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

• недовольством служащего служебным положением;

• любопытством;

• конкурентной борьбой;

• уязвленным самолюбием и т. д.

Угрозы, классифицируемые по расположению источника угроз, бывают внутренние и внешние.

Внешние угрозы обусловлены применением вычислительных сетей и созданием на их основе информационных систем.

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

4.2. Характер происхождения угроз: умышленные факторы, естественные факторы. Источники угроз

Носителями угроз безопасности информации являются источники угроз. Источники угроз могут использовать уязвимости для нарушения безопасности информации, получения незаконной выгоды (нанесения ущерба собственнику, владельцу, пользователю информации). Кроме того, возможны незлонамеренные действия источников угроз по активизации тех или иных уязвимостей, наносящих вред. В качестве источников угроз могут выступать как субъекты (личность), так и объективные проявления, причем источники угроз могут находиться как внутри защищаемой организации – внутренние источники, так и вне ее – внешние источники.

Деление источников на субъективные и объективные оправдано исходя из того, что субъективные уязвимости зависят от действий сотрудни-

ков и в основном устраняются организационными и программно-аппаратными методами, а объективные уязвимости зависят от особенностей построения и технических характеристик оборудования, применяемого на защищаемом объекте. Полное устранение этих уязвимостей невозможно, но они могут существенно ослабляться техническими и инженерно-техническими методами парирования угроз безопасности информации.

А деление на внутренние и внешние источники оправдано тем, что для одной и той же угрозы методы парирования для внешних и внутренних источников могу быть разными.

Все источники угроз безопасности информации можно разделить на три основные группы:

1. Обусловленные действиями субъекта (антропогенные источники угроз).

2. Обусловленные техническими средствами (техногенные источники угроз).

3. Обусловленные стихийными источниками.

Антропогенные источники угроз

Антропогенными источниками угроз безопасности информации выступают субъекты, действия которых могут быть квалифицированы как умышленные или случайные преступления. Только в этом случае можно говорить о причинении ущерба. Эта группа источников наиболее обширна и представляет наибольший интерес с точки зрения организации защиты, так как действия субъекта всегда можно оценить, спрогнозировать и принять адекватные меры. Методы противодействия в этом случае управляемы и напрямую зависят от воли организаторов защиты информации.

В качестве антропогенного источника угроз можно рассматривать субъекта, имеющего доступ (санкционированный или несанкционированный) к работе со штатными средствами защищаемого объекта. Субъекты (источники), действия которых могут привести к нарушению безопасности информации, могут быть как внешними, так и внутренними.

Внешние источники могут быть случайными или преднамеренными и иметь разный уровень квалификации. К ним относятся:

1) криминальные структуры;

2) потенциальные преступники и хакеры;

3) недобросовестные партнеры;

4) технический персонал поставщиков телематических услуг;

5) представители надзорных организаций и аварийных служб;

6) представители силовых структур.

Внутренние субъекты (источники), как правило, представляют собой высококвалифицированных специалистов в области разработки и эксплуатации программного обеспечения и технических средств, знакомы со спецификой решаемых задач, структурой и основными функциями и принципами работы программно-аппаратных средств защиты информации, имеют возможность использования штатного оборудования и технических средств сети. К ним относятся:

1) основной персонал (пользователи, программисты, разработчики);

2) представители службы защиты информации;

3) вспомогательный персонал (уборщики, охрана);

4) технический персонал.

Необходимо учитывать также, что особую группу внутренних антропогенных источников составляют лица с нарушенной психикой и специально внедренные и завербованные агенты, которые могут быть из числа основного, вспомогательного и технического персонала, а также представителей службы защиты информации. Данная группа рассматривается в составе перечисленных выше источников угроз, но методы парирования угроз для этой группы могут иметь свои отличия.

Квалификация антропогенных источников информации играет важную роль в оценке их влияния и учитывается при ранжировании источников угроз.

Техногенные источники угроз

Данная группа содержит источники угроз, определяемые технократической деятельностью человека и развитием цивилизации. Однако последствия такой деятельности вышли из-под контроля человека и существуют сами по себе. Эти источники угроз менее прогнозируемые, напрямую зависят от свойств техники и поэтому требуют особого внимания. Данный класс источников угроз безопасности информации особенно актуален в настоящее время, так как в сложившихся условиях эксперты ожидают резкого роста числа техногенных катастроф, вызванных физическим и моральным устареванием технического парка используемого оборудования, а также отсутствием материальных средств на его обновление.

Технические средства, являющиеся источниками потенциальных угроз безопасности информации, также могут быть внешними:

1) средства связи;

2) сети инженерных коммуникаций (водоснабжения, канализации);

3) некачественные технические средства обработки информации;

4) некачественные программные средства обработки информации;

5) вспомогательные средства (охраны, сигнализации, телефонии);

6) другие технические средства, применяемые в учреждении.

Стихийные источники угроз

Данная группа источников угроз объединяет обстоятельства, составляющие непреодолимую силу, т. е. такие обстоятельства, которые носят объективный и абсолютный характер, распространяющийся на всех. К непреодолимой силе в законодательстве и договорной практике относят стихийные бедствия или иные обстоятельства, которые невозможно предусмотреть или предотвратить или возможно предусмотреть, но невозможно предотвратить при современном уровне человеческого знания и возможностей. Такие источники угроз совершенно не поддаются прогнозированию, и поэтому меры защиты от них должны применяться всегда.

Стихийные источники потенциальных угроз информационной безопасности, как правило, являются внешними по отношению к защищаемому объекту, и под ними понимаются прежде всего природные катаклизмы:

1) пожары;

2) землетрясения;

3) наводнения;

4) ураганы;

5) различные непредвиденные обстоятельства;

6) необъяснимые явления;

7) другие форс-мажорные обстоятельства.

Человеческий фактор как антропогенный источник угроз

Чаще всего к возникновению значительного ущерба приводят злонамеренные или ошибочные действия людей, а техногенные источники, как правило, выступают в качестве предпосылки.

Внешние источники угроз

Хакеры и криминальные структуры. Популярность такого источника угроз, как хакеры, к сожалению, активно поддерживается средствами массовой информации.

Важный мотив действий хакера – материальная выгода. Особенно часто совершаются попытки кражи номеров кредитных карт либо конфиденциальной информации с последующим шантажом с целью вымогатель-

ства. Сюда же можно отнести случаи взлома финансовых систем или мошенничества.

Распространенным мотивом действий хакеров являются межнациональные конфликты. В качестве примеров можно привести хакерские «войны» между Арменией и Азербайджаном, атаки на российские сайты представителей исламских стран, массированные нападения китайских хакеров на сервера Японии, Тайваня, США.

Реальная квалификация большинства хакеров ниже, чем профессиональных программистов. Иногда попытки злоупотреблений совершаются лицами с преступными наклонностями, совсем не обладающими специальными знаниями.

Практика показывает, что в большинстве случаев хакеры, представляющие реальную опасность, работают по заказу и под контролем криминальных структур.

Время от времени появляются сообщения о том, как в качестве заказчиков компьютерных преступлений выступают спецслужбы различных стран.

Недобросовестные партнеры и конкуренты. В течение последних лет наряду с пособиями для хакеров на полках магазинов в изобилии появились книги по промышленному шпионажу, и некоторые из них уже являются рекордсменами продаж. В списках услуг охранно-сыскных структур присутствует получение информации и наблюдение за конкурентами и партнерами, подобные функции выполняют и собственные службы безопасности многих компаний. Еще одним инструментом добычи сведений являются недобросовестные собственные сотрудники государственных структур.

Конкуренты могут получать информацию в ходе беседы после выступлений и на специально организованных переговорах. При соответствующей подготовке недоброжелатели могут эффективно использовать современные психотехнологии, эксплуатировать желание субъекта показать себя влиятельным, осведомленным, компетентным, использовать вредные привычки и скрытые потребности.

В первую очередь объектом воздействия становятся менеджеры и высококвалифицированные специалисты, так как именно они осведомлены в наибольшей степени.

Особенно полезными для конкурентов могут оказаться уволенные сотрудники, а также сотрудники, получившие приглашение, в том числе

мнимое, на работу. Находящиеся в штате работники также не всегда следуют интересам организации.

Не менее опасным для компании может оказаться воздействие заведомо ложной и модифицированной информации, которая передается по «доверенным» каналам, распространяется через средства массовой информации, веб-сайты, публичные выступления (пиар, антипиар).

Внутренние источники угроз

Менеджеры. Как лица, обладающие большими организационными полномочиями, они представляют наибольшую потенциальную угрозу для информационных ресурсов компании. Например, к потерям могут привести распоряжения предоставить пользователю неоправданно высокие права, реализовать в информационной системе небезопасный, но удобный функционал. Иногда информационные угрозы возникают вследствие неудовлетворительного выполнения руководителями контролирующих функций. Известны случаи, когда продавалось компьютерное оборудование, с дисков которого не удалялась информация компании и партнеров.

Во избежание возникновения ущерба целесообразно обязать менеджеров согласовывать решение вопросов, связанных с информационными рисками, с руководителем службы информационной безопасности.

Сотрудники. Значительной угрозой информационной безопасности компании является низкая квалификация персонала, недостаточная для корректной работы с корпоративной информационной системой. Особо опасными являются некомпетентные сотрудники, выдающие себя за грамотных пользователей или считающие себя таковыми.

Во многих компаниях отсутствует контроль за установкой на рабочих станциях программного обеспечения. Не понимая возможных последствий, сотрудник может установить на своем рабочем месте заинтересовавшую его программу, существенно снизив эффективность усилий по обеспечению корпоративной сетевой безопасности. Подобная угроза возникает и в случае подключения находящейся в локальной сети рабочей станции к Интернету через модем или мобильный телефон, оснащенный функцией цифровой связи.

Конечно, не будет лишним упомянуть об угрозах, исходящих от приклеенных к мониторам стикеров с паролями и практики обмена паролями между работниками, выполняющими сходные функции.

В ряде случаев проблемы безопасности связаны с тем, что легальные пользователи используют необходимую для работы информацию не по на-

значению. Причинами могут быть злой умысел, халатность, непонимание последствий распространения доступных им сведений. Очевидно, что данная проблема не разрешима только технологическими мерами.

Наибольшую опасность представляют сотрудники, обиженные на организацию и ее руководителей. Поэтому случаи возникновения явных и скрытых конфликтов, несоответствия сложившейся ситуации ожиданиям сотрудников могут рассматриваться как потенциальные предпосылки нарушений информационной безопасности. Особого внимания требуют связанные с такими ситуациями случаи увольнения. Как отмечалось выше, сотрудник, уволившийся из компании с чувством обиды, легко может стать источником информации для недоброжелателей.

Администраторы и лица, выполняющие критичные операции. Хочется обратить внимание на отбор кандидатов, которым предполагается доверить выполнение операций, требующих больших прав в информационной системе. Не меньшее значение, чем профессиональные навыки, имеют лояльность кандидата и способность сохранять приверженность интересам компании даже в сложных ситуациях. По этой причине лица, на вершине системы ценностей которых находится материальное вознаграждение, скорее всего получат отказ. С особой осторожностью следует относиться к кандидатам, слишком часто меняющим работу, предоставившим недостоверные сведения, привлекавшимся к административной и уголовной ответственности, имевшим психические или невротические расстройства.

Желательно, чтобы кроме собеседования со своим руководителем, кандидат встретился с профессиональным психологом. Часто психолог проводит тестирование, которое выявляет особенности характера и потенциальные возможности кандидата. Также важно провести с кандидатом беседу, в ходе которой будут выявлены его система ценностей и особенности поведения. Это позволит убедиться в том, что кандидат гладко «впишется» в корпоративную культуру, понять, какая система мотивации будет для него наиболее подходящей.

Особое внимание следует уделить тому, чтобы работа сотрудника в организации соответствовала его ожиданиям. В частности, руководителю следует воздержаться от необоснованных обещаний. Психологический контакт важен так же, как формальный.

Традиционной проблемой, связанной с IT-сотрудниками, является контроль и оценка результатов деятельности. Немногие, владеющие глубокими знаниями в IT, компетентны в вопросах управления.

Например, в IT-подразделениях часто отсутствуют должностные инструкции и не проводятся аттестации. Иногда IT-специалистов рассматривают как обслуживающий персонал, пытаются нагрузить дополнительной работой. Это ухудшает выполнение прямых обязанностей, вызывает недовольство, отрицательно сказывается на лояльности, приводит к высокой текучести кадров. Известны случаи, когда увольняющийся администратор блокирует пароли сервера.

4.3. Каналы утечки информации: технические, электромагнитные, индукционные и др.

Современные информационные технологии разделили судьбу всех прогрессивных технологий XX в. Широкое внедрение средств компьютерной техники (СКТ) и телекоммуникаций в производственную, хозяйственную, финансовую деятельность предприятий, учреждений, организаций значительно повышает эффективность их работы. Рубеж тысячелетий знаменуется все большим проникновением СКТ в повседневную жизнь людей, вовлечением их в глобальную сеть Интернет. Так, например, по оценкам зарубежных специалистов, темп роста пользователей Интернета составляет порядка 15 % в месяц. Обратной стороной глобальной информатизации явилось появление компьютерной преступности.

На локальном уровне угроз компьютерной безопасности (например, для помещений, занимаемых учреждением, организацией, предприятием, и размещенных в них СКТ) выделяют каналы утечки информации, под которыми понимают совокупность источников информации, материальных носителей или среды распространения несущих эту информацию сигналов и средств выделения информации из сигналов или носителей.

Факторы информационных угроз следует рассматривать как потенциальную возможность использования каналов утечки информации. Объективное существование данных каналов утечки предполагает их возможное использование злоумышленниками для несанкционированного доступа к информации, ее модификации, блокированию и иных неправомерных манипуляций, т. е. наличие каналов утечки информации влияет на избрание способа совершения преступления.

Каналы утечки информации можно разделить на традиционные каналы утечки информации (каналы утечки информации в широком смысле) и каналы утечки информации непосредственно из СКТ (каналы утечки

в узком смысле). Наличие первых предопределяет широкое их использование с применением специальных технических средств для проведения различных разведывательных мероприятий. Они были известны задолго до появления современных средств вычислительной техники.

Каналы утечки информации непосредственно из СКТ и технические устройства съема такой информации стали использоваться злоумышленниками сравнительно недавно.

Для получения информации из обозначенных выше традиционных каналов утечки применяются специализированные технические средства ведения разведки, среди которых выделяют следующие основные группы: радиомикрофоны и микрофоны; оптические системы; устройства перехвата телефонных сообщений; видеосистемы записи и наблюдения; системы определения местоположения контролируемого объекта; системы контроля и воздействия на компьютеры и их сети; устройства приема, записи, управления. Эти каналы были подробно рассмотрены во второй главе пособия.

Утечка информации за счет введения программно-аппаратных закладок в СКТ. В настоящее время в основе производства технических средств и программного обеспечения вычислительных систем лежат комплектующие изделия зарубежного производства, что обеспечивает конкурентоспособность выпускаемых изделий. Однако при этом появляется угроза утечки информации, а также управляемого выведения из строя средств вычислительной техники, заложенная в них либо на этапе производства, либо на этапе сборки. Подобные устройства могут быть установлены негласным образом и впоследствии, при эксплуатации СКТ. Использование закладных элементов (ЗЭ) представляется реальной и опасной угрозой при использовании вычислительной техники.

Аппаратные ЗЭ могут быть реализованы в аппаратуре персональных компьютеров и периферийных устройств. При этом возможны утечка информации, искажение вычислительного процесса, а также управляемый выход из строя вычислительной системы.

Программные ЗЭ могут быть представлены в виде модификации компьютерной программы, в результате которой данная программа способна выполняться несколькими способами в зависимости от определенных обстоятельств. При работе программные ЗЭ могут никак не проявляться, однако при определенных условиях программа работает по алго-

ритму, отличному от заданного (подобно компьютерным вирусам). В литературе описан пример внесения программистом в программу начисления заработной платы предприятия нежелательных изменений, работа которых началась после его увольнения, т. е. когда фамилия программиста исчезла из базы данных персонала.

Утечки за счет перехвата побочного электромагнитного излучения и наводок. При функционировании СКТ возникают побочные электромагнитные излучения и наводки (ПЭМИН), несущие обрабатываемую информацию. Они излучаются в пространство клавиатурой, принтером, монитором, накопителями на магнитных дисках, кабелями. Утечка данных обусловлена лишь излучением сигналов при перемене данных. Все прочие излучения сигналов от разных блоков СКТ являются взаимными помехами.

Перехват ПЭМИН осуществляется радиоприемными устройствами, средствами анализа и регистрации информации. При благоприятных условиях с помощью направленной антенны можно осуществлять перехват на расстоянии до 1,5 км. Перехват информации за счет ПЭМИН обладает рядом особенностей:

- информация добывается без непосредственного контакта с источником;
- на прием сигналов не влияет ни время года, ни время суток;
- информация получается в реальном масштабе времени, в момент ее передачи или излучения;
- перехват реализуется скрытно;
- дальность перехвата ограничивается только особенностями распространения радиоволн соответствующих диапазонов.

Утечка за счет съема информации с принтера и клавиатуры по акустическому каналу. Наличие указанного канала утечки позволяет перехватывать и декодировать акустические колебания, средой распространения которых является воздушная среда. Источником данных колебаний являются соответствующие устройства СКТ. Технически возможен перехват и декодирование кодов клавиш клавиатуры. Дальность действия подобных перехватов ограничена мощностью источника акустических и электромагнитных колебаний.

Утечка, модификация, уничтожение или блокирование информации с использованием компьютерных вирусов. Существует множе-

ство типов вирусов, каждый из которых обладает собственными отличительными признаками. Анализ специальной научной литературы дает нам основание утверждать, что все вирусы либо изменяют файлы с данными или программы внутри компьютера, либо разрушают сами компьютеры. Большинство из них представляют собой опасность только для IBM-совместимых компьютеров, однако именно этот тип компьютеров распространен в наибольшей степени.

Последствия вирусной модификации могут быть различными – от незначительных помех до полного уничтожения данных и программ. Вирусы, использующиеся правонарушителями для программного уничтожения, разрушают информацию в зависимости от определенных логических или временных условий.

Попадание вирусов в компьютерную систему может быть спровоцировано различными способами – от высокотехнологичного несанкционированного подключения до основанного на личном доверии обмана оператора системы путем переписывания заранее зараженных игр и сервисных программ с замыслом вывода компьютерной системы из строя. Вирус может попасть в систему и при неумышленных действиях пользователей, при обмене дискетами, дисками, файлами, флешками.

В настоящее время «рассадником» компьютерных вирусов является глобальная сеть Интернет. Особенно активно распространяются в этой сети так называемые макровирусы, которые передаются вместе с файлами документов MS-Word и файлами рабочих книг MS-Excel.

4.4. Вирусы как угроза информационной безопасности

Первые исследования саморазмножающихся программных искусственных конструкций проводились в середине прошлого века. Термин «компьютерный вирус» появился позднее – официально считается, что его впервые употребил сотрудник Лехайского университета (США) Ф. Коэн в 1984 г. на 7-й конференции по безопасности информации, проходившей в США. С тех пор прошло немало времени, острота проблемы вирусов многократно возросла, однако строгого определения, что же такое компьютерный вирус, так и не дано, несмотря на то, что попытки дать такое определение предпринимались неоднократно.

Основная трудность при формулировании определения вируса заключается в том, что либо практически все отличительные черты вируса

(внедрение в другие объекты, скрытность, потенциальная опасность и пр.) присущи другим программам, которые никоим образом вирусами не являются, либо существуют вирусы, которые не содержат указанных выше отличительных черт (за исключением возможности распространения).

Например, если в качестве отличительной характеристики вируса принимается скрытность, то легко привести пример вируса, не скрывающего своего распространения. Такой вирус перед заражением любого файла выводит сообщение, гласящее, что в компьютере находится вирус и этот вирус готов поразить очередной файл, затем выводит имя этого файла и запрашивает разрешение пользователя на внедрение вируса в файл.

Если в качестве отличительной черты вируса рассматривать возможность уничтожения им программ и данных на дисках, то в качестве примера можно привести десятки совершенно безобидных вирусов, которые кроме своего распространения ничем больше не отличаются.

Основная же особенность компьютерных вирусов – возможность их самопроизвольного внедрения в различные объекты операционной системы – присуща многим программам, которые не являются вирусами (любая программа, имеющая инсталлятор, способна к саморазмножению).

Таким образом, первой из причин, не позволяющих дать точное определение вирусу, является невозможность однозначно выделить отличительные признаки, которые соответствовали бы только вирусам. Поэтому представляется возможным сформулировать только обязательное условие для того, чтобы некоторая последовательность выполняемого кода являлась вирусом.

Обязательным (необходимым) свойством компьютерного вируса является возможность создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети и/или файлы, системные области компьютера и прочие выполняемые объекты. При этом дубликаты сохраняют способность к дальнейшему распространению.

Следует отметить, что это условие не является достаточным (т. е. окончательным) для объявления программы вирусом.

Вот почему точного определения вируса нет до сих пор, и вряд ли оно появится в обозримом будущем. Следовательно, нет точно определенного закона, по которому «хорошие» файлы можно отличить от «вирусов». Более того, иногда даже для конкретного файла довольно сложно определить, является он вирусом или нет.

Классификация вирусов

Известно множество типов вирусов. По степени опасности для системы существуют вирусы от совсем безобидных, которые кроме саморазмножения ничем не занимаются, до фатальных, которые могут привести к краху всей системы.

По принципу действия можно привести несколько самых распространенных типов:

- загрузочные;
- файловые;
- макровирусы;
- полиморфные вирусы;
- стелс-вирусы;
- резидентные вирусы;
- IRC-черви;
- сетевые вирусы.

Загрузочные вирусы. Заражают загрузочный (boot) сектор флоппи-диска и boot-сектор или Master Boot Record (MBR) винчестера. Принцип действия загрузочных вирусов основан на алгоритмах запуска операционной системы при включении или перезагрузке компьютера – после необходимых тестов установленного оборудования (памяти, дисков и т. д.) программа системной загрузки считывает первый физический сектор загрузочного диска и передает на него управление.

Файловые вирусы. К данной группе относятся вирусы, которые при своем размножении тем или иным способом используют файловую систему какой-либо операционной системы (ОС). Внедрение файлового вируса возможно практически во все исполняемые файлы всех популярных ОС. На сегодняшний день известны вирусы, поражающие все типы выполняемых объектов стандартной DOS: командные файлы (BAT), загружаемые драйверы (SYS, в том числе специальные файлы IO.SYS и MSDOS.SYS) и выполняемые двоичные файлы (EXE, COM). Существуют вирусы, поражающие исполняемые файлы операционных систем. Существуют вирусы, заражающие файлы, которые содержат исходные тексты программ, библиотечные или объектные модули.

Макровирусы (macro viruses). Являются программами на макроязыках, встроенных в некоторые системы обработки данных (текстовые редакторы, электронные таблицы и т. д.). Макровирусы записывают свой

код в файлы данных – документы или электронные таблицы. Для своего размножения такие вирусы используют возможности макроязыков и при их помощи переносят себя из одного зараженного файла (документа или таблицы) в другие. Наибольшее распространение получили макровирусы для Microsoft Word, Excel и всего Office97–2003.

Большинство макровирусов являются как бы резидентными: они активны не только в момент открытия (закрытия) файла, но и до тех пор, пока активен редактор.

Полиморфные вирусы. К полиморфным вирусам относят те, которые детектировать невозможно или крайне затруднительно осуществить при помощи так называемых вирусных масок – участков постоянного кода, специфичных для конкретного вируса. Достигается это двумя основными способами – шифрованием основного кода вируса с непостоянным ключом и случайным набором команд расшифровщика или изменением самого выполняемого кода вируса. Полиморфизм различной степени сложности встречается в вирусах всех типов – от загрузочных и файловых DOS-вирусов до Windows-вирусов и даже макровирусов.

Стелс-вирусы. Они теми или иными способами скрывают факт своего присутствия в системе. Известны стелс-вирусы всех типов, за исключением Windows-вирусов – загрузочные вирусы, файловые DOS-вирусы и даже макровирусы.

Резидентные вирусы. Под термином «резидентность» понимается способность вирусов оставлять свои копии в системной памяти, перехватывать некоторые события (например, обращения к файлам или дискам) и вызывать при этом процедуры заражения обнаруженных объектов (файлов и секторов). Таким образом, резидентные вирусы активны не только в момент работы зараженной программы, но и после того, как программа закончила свою работу. Резидентные копии таких вирусов остаются жизнеспособными вплоть до очередной перезагрузки, даже если на диске уничтожены все зараженные файлы.

Нерезидентные вирусы, напротив, активны довольно непродолжительное время – только в момент запуска зараженной программы. Для своего распространения они ищут на диске незараженные файлы и записываются в них. После того, как код вируса передает управление программе-носителю, влияние вируса на работу операционной системы сводится к нулю вплоть до очередного запуска какой-либо зараженной программы. Поэто-

му файлы, зараженные нерезидентными вирусами, значительно проще удалить с диска и при этом не позволить вирусу заразить их повторно.

IRC-черви. IRC (Internet Relay Chat) – это специальный протокол, разработанный для коммуникации пользователей Интернет в реальном времени. Этот протокол предоставляет возможность Интернет-«разговора» при помощи специально разработанного программного обеспечения. IRC чем-то похож на телефонный разговор, за исключением того, что в разговоре могут участвовать более двух собеседников, объединяющихся по интересам в различные группы IRC-конференций. Помимо общения существует также возможность передавать и принимать файлы – именно на этой возможности и базируются IRC-черви.

Сетевые вирусы. К сетевым относятся вирусы, которые для своего распространения активно используют протоколы и возможности локальных и глобальных сетей. Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию. «Полноценные» сетевые вирусы при этом обладают еще и возможностью запустить на выполнение свой код на удаленном компьютере или, по крайней мере, «подтолкнуть» пользователя к запуску зараженного файла.

К «вредным программам», помимо вирусов, относятся также троянские программы (логические бомбы), утилиты скрытого администрирования удаленных компьютеров («backdoor»), программы, «ворующие» пароли доступа к ресурсам Интернет и прочую конфиденциальную информацию.

Большинство известных троянских программ «подделываются» под какие-либо полезные программы, новые версии популярных утилит или дополнения к ним. Очень часто они рассылаются по BBS-станциям или электронным конференциям. По сравнению с вирусами «троянские программы» не получают широкого распространения по достаточно простым причинам – они либо уничтожают себя вместе с остальными данными на диске, либо демаскируют свое присутствие и уничтожаются пострадавшим пользователем.

Троянские программы класса «backdoor» по своей сути являются достаточно мощными утилитами удаленного администрирования компьютеров в сети. По своей функциональности они во многом напоминают различные системы администрирования, разрабатываемые и распространяемые различными фирмами – производителями программных продуктов.

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

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

Анализ угроз безопасности информации служит для качественной и количественной оценки реальных угроз безопасности информации бизнеса с целью построения системы обеспечения безопасности информации. Большинство организаций, как правило, не имеет ресурсов и отработанных методик для проведения качественной и количественной оценки угроз безопасности информации, исходящих как извне, так и изнутри компании. Однако без осознания того, что же реально угрожает информационным ресурсам компании, невозможно грамотно проводить политику безопасности и тем более построить систему защиты, адекватную имеющимся угрозам.

Инструменты анализа угроз:

• Расчетно-аналитический метод, основанный на вычислении весовых коэффициентов опасности источников угроз и уязвимостей, сравнении этих коэффициентов с заранее заданным критерием и последовательном сокращении полного перечня возможных источников угроз и уязвимостей до минимально актуального для конкретного объекта.

Анализ угроз безопасности информации включает:

• определение приоритетности целей информационной безопасности;

• анализ информационных потоков компьютерных информационных систем, точек их пересечения, точек обработки и хранения и т. д.;

• определение перечня актуальных источников угроз;

• определение перечня актуальных уязвимостей;

• оценку взаимосвязи угроз, источников угроз и уязвимостей;

• определение перечня возможных атак на объект;

• описание возможных последствий реализации угроз;

• подготовку предложений по изменению структуры информационных потоков в целях повышения уровня защищенности системы.

Услуга по анализу угроз безопасности информации может являться обязательным этапом комплексного обследования (аудита) информационной безопасности, а также предоставляться как самостоятельная услуга.

Результатом оказания данной услуги являются:

• аналитический отчет с описанием реальных угроз безопасности, источников этих угроз и способов реализации, а также описанием уязвимостей системы, возможных для реализации этих угроз;

• рекомендации по выбору адекватных оптимальных методов пресечения угроз;

• рекомендации специалистам от заказчика при определении задач для разработчиков (проектировщиков, поставщиков) систем обеспечения безопасности информации.

Вопросы и задания для самоконтроля

1. Дайте определение следующим понятиям: угроза информационной безопасности, каналы утечки информации, компьютерные вирусы.

2. Приведите примеры классификаций угроз информационной безопасности.

3. Какие источники угроз информационной безопасности вы знаете?

4. Охарактеризуйте основные группы источников угроз.

5. Перечислите традиционные каналы утечки информации.

6. Какие существуют каналы утечки информации из средств компьютерной техники?

7. Дайте характеристику основным типам вирусов.

8. Какие существуют инструменты анализа угроз информационной безопасности?

Глава 5. ПОНЯТИЕ ЗАЩИТЫ ИНФОРМАЦИИ

5.1. Общие положения защиты информации

Одно из фундаментальных положений системно-концептуального подхода к защите информации состоит в том, что предполагается разработка концепции, в рамках которой имелись бы (по крайней мере потенциально) возможности гарантированной защиты информации для самого общего случая архитектурного построения автоматизированных систем (АС), технологии и условий их функционирования. Для того чтобы множество функций соответствовало своему назначению, оно должно удовлетворять требованию полноты, причем под полнотой множества функции понимается свойство, состоящее в том, что при надлежащем обеспечении соответствующего уровня (соответствующей степени) осуществления каждой из функций множества гарантированно может быть достигнут требуемый уровень защищенности информации.

Защита информации может быть эффективной лишь в том случае, если она будет осуществляться как непрерывный и управляемый процесс. Для этого должны быть предусмотрены, с одной стороны, **механизмы непосредственной защиты информации,** а с другой – **механизмы управления механизмами непосредственной защиты.** Соответственно этому и множество функций защиты должно состоять из двух подмножеств: первого, содержащего функции непосредственно защиты, и второго, содержащего функции управления механизмами защиты.

Обеспечение регулярного осуществления функций защиты достигается тем, что решаются специальные задачи защиты. При этом задачей защиты информации называются организованные возможности средств, методов и мероприятий, реализуемых в АС с целью осуществления функций защиты.

Множество функций защиты должно быть полным в том случае, если регулярное их осуществление обеспечивает условия для надежной защиты информации в системном плане.

Требование полноты множества функций защиты применительно к двум отмеченным видам интерпретируется следующим образом.

• Множество функций обеспечения защиты должно быть таким, чтобы осуществлением их в различных комбинациях и с различными усилиями в любой ситуации при функционировании АС могли быть созданы все условия, необходимые для надежной защиты информации.

• Множество функций управления должно создавать все предпосылки для оптимальной реализации функций обеспечения в любых условиях.

Вместе с тем важно подчеркнуть, что регулярных (а тем более формальных) методов решения проблемы не существует (по крайней мере в настоящее время). Вынужденно приходится использовать методы неформальные. Таким образом, формирование функций защиты приходится осуществлять в ситуации, когда требования к формированию являются абсолютными, а методы, которые могут быть при этом использованы, весьма относительны: структурно-логический анализ, экспертные оценки и просто здравый смысл компетентных специалистов.

Совершенно очевидно, что множество функций защиты информации должно быть таким, чтобы надлежащим их осуществлением можно было оказывать желаемое воздействие на любую ситуацию, которая потенциально возможна в процессе организации и обеспечения защиты информации.

Последовательность и содержание структурно-логического анализа ситуаций, потенциально возможных в процессе защиты информации, можно представить в следующем виде.

Для того чтобы защищенность информации могла быть нарушена, должны существовать такие условия, при которых могут проявиться дестабилизирующие факторы. Если таких условий не будет, то не будет необходимости в специальной защите информации. Если же потенциальные возможности для проявления дестабилизирующих факторов будут иметь место, то надо оценивать реальную возможность их проявления, обнаруживать факты их проявления, принимать следующие меры к предотвращению воздействия их на информацию, обнаружению, локализации и ликвидации последствий этих воздействий.

Вариант 1 – защита информации обеспечена, поскольку даже при условии проявления дестабилизирующих факторов предотвращено их воздействие на защищаемую информацию или ликвидированы последствия такого воздействия.

Вариант 2 – защита информации нарушена, поскольку не удалось предотвратить воздействие дестабилизирующих факторов на информацию, однако это воздействие локализовано.

Вариант 3 – защита информации разрушена, поскольку воздействие дестабилизирующих факторов на информацию не только не предотвращено, но даже не локализовано.

Формирование множества задач осуществляется на основе анализа объективных возможностей реализации поставленных целей защиты. Такое множество задач может состоять из ряда классов задач, включающих содержащие однородные в функциональном отношении задачи.

Класс задач – это однородное в функциональном отношении множество задач, обеспечивающих полную или частичную реализацию одной или нескольких целей.

5.2. Классы задач защиты информации

Учитывая, что основными целями обеспечения информационной безопасности являются защита системы от обнаружения и от информационного воздействия, а также защита содержания информации, выделяются задачи соответствующих видов.

Одной из первоочередных целей противника является обнаружение объекта, обрабатывающего конфиденциальную информацию, и выявление сведений о его предназначении. Поэтому к первому виду задач можно отнести **задачи уменьшения степени распознавания объектов.** К этому виду относятся следующие классы задач.

Класс 1. Сокрытие информации о средствах, комплексах, объектах и системах обработки информации. Эти задачи могут подразделяться на организационные и технические.

Организационные задачи по сокрытию информации об объектах направлены на недопущение разглашения этой информации сотрудниками и утечки ее по агентурным каналам.

Технические задачи направлены на устранение или ослабление технических демаскирующих признаков объектов защиты и технических каналов утечки сведений о них. При этом сокрытие осуществляется уменьшением электромагнитной, временной, структурной и признаковой доступности, а также ослаблением адекватности между структурой, топологи-

ей и характером функционирования средств, комплексов, объектов, систем обработки информации и управления.

Решение этой задачи представляет собой реализацию комплекса организационно-технических мероприятий и мер, обеспечивающих выполнение основного требования к средствам, комплексам и системам обработки информации – разведзащищенности, и направлено на достижение одной из главных целей – исключение или существенное затруднение технической разведке поиска, определения местоположения, радионаблюдения источников радиоизлучения, классификации и идентификации объектов технической разведкой по выявленным демаскирующим признакам.

Решение задачи по снижению электромагнитной доступности затрудняет как энергетическое обнаружение, так и определение координат района расположения источников радиоизлучения, а также увеличивает время выявления демаскирующих признаков, уменьшает точность измерения параметров и сигналов средств радиоизлучения.

Снижение временной доступности радиоизлучающих средств предполагает сокращение времени их работы на излучение при передаче информации и увеличение длительности паузы между сеансами обработки информации. Для уменьшения структурной и признаковой доступности информации реализуются организационно-технические мероприятия, ослабляющие демаскирующие признаки и создающие так называемый серый фон.

Технические задачи сокрытия должны решаться, например, для подвижных объектов (автомобилей), оборудованных радиосвязью.

Класс 2. Дезинформация противника. К этому классу относятся задачи, заключающиеся в распространении заведомо ложных сведений относительно истинного назначения каких-то объектов и изделий, действительного состояния какой-то области государственной деятельности, положения дел на предприятии и т. д.

Дезинформация обычно проводится путем распространения ложной информации по различным каналам, имитацией или искажением признаков и свойств отдельных элементов объектов защиты, создания ложных объектов, по внешнему виду или проявлениям похожих на интересующие соперника объекты, и др.

Роль дезинформации подчеркивал А. Ф. Вивиани, специалист в области контршпионажа: «На нас обрушивается, валится, извергается огромное количество информации. Она бывает фальшивой, но выглядит правдо-

подобно; бывает правдивой, а на самом деле хитроумно перекроена, дабы производить впечатление фальшивой; бывает отчасти фальшивой и отчасти правдивой. Все зависит от выбранного способа так называемой дезинформации, цель которой – заставить вас верить, желать, думать, принимать решения в направлении, выгодном для тех, кому зачем-то нужно на нас воздействовать» [Цит. по: 27, с. 30].

Техническая дезинформация на объекте защиты представляет комплекс организационных мероприятий и технических мер, направленных на введение в заблуждение технической разведки относительно истинных целей систем обработки информации, намерений органов управления.

Частными задачами технической дезинформации являются:

• искажение демаскирующих признаков реальных объектов и систем, соответствующих признакам ложных объектов;

• создание (имитация) ложной обстановки, объектов, систем, комплексов путем воспроизведения демаскирующих признаков реальных объектов, структур систем, ситуаций, действий, функций и т. д.

• передача, обработка, хранение в системах обработки ложной информации.

В общем виде эти задачи могут быть сгруппированы в частные задачи радиоимитации, радиодезинформации, демонстративных действий.

Класс 3. Легендирование. Объединяет задачи по обеспечению получения злоумышленником искаженного представления о характере и предназначении объекта, когда наличие объекта и направленность работ на нем полностью не скрываются, а маскируются действительное предназначение и характер мероприятий.

На практике, учитывая очень высокую степень развития современных средств ведения разведки, является чрезвычайно сложным полное сокрытие информации об объектах. Так, современные средства фоторазведки позволяют делать из космоса снимки объектов с разрешающей способностью в несколько десятков сантиметров.

Поэтому наряду с рассмотренным видом задач не менее важными, а по содержанию более объемными являются **задачи защиты содержания обрабатываемой, хранимой и передаваемой информации.** К этому виду относятся следующие классы задач.

Класс 1. Введение избыточности элементов системы. Под избыточностью понимается включение в состав элементов системы обработки

информации дополнительных компонентов, обеспечивающих реализацию заданного множества целей защиты с учетом воздействий внешних и внутренних дестабилизирующих факторов.

Решение этой задачи включает реализацию комплекса организационных мероприятий, технических, программных и других мер, обеспечивающих организационную, аппаратную, программно-аппаратную, информационную, временную избыточность.

Организационная избыточность осуществляется за счет введения дополнительной численности обслуживающего персонала, его обучения, организации и обеспечения режима сохранения государственной тайны и другой конфиденциальной информации, определения порядка передачи информации различной степени важности, выбора мест размещения средств и комплексов обработки и т. п.

Аппаратная избыточность осуществляется за счет введения дополнительных технических устройств, обеспечивающих защиту информации.

Программно-аппаратная избыточность предполагает использование дополнительных программных, аппаратных и комбинированных средств защиты в системе обработки информации.

Информационная избыточность осуществляется за счет создания дополнительных информационных массивов, банков данных.

Временная избыточность предполагает выделение дополнительного времени для проведения обработки информации и др.

Класс 2. Резервирование элементов системы. Резервирование, в отличие от задачи введения избыточности, предполагает не введение дополнительных элементов, обеспечивающих защиту информации, а их исключение и перевод в резерв на случай возникновения необходимости обработки дополнительного массива информации, повышения статуса защищенности информации, возникновения непредвиденных ситуаций. Такое резервирование может быть горячим и холодным.

При горячем резервировании элементы находятся в рабочем состоянии после дополнительных операций включения и подготовки к работе, а при холодном элементы переводятся в рабочее состояние после дополнительных операций.

Класс 3. Регулирование доступа к элементам системы и защищаемой информации. Регулирование доступа к средствам, комплексам и системам обработки информации (на территорию, в помещение, к техническим средствам, к программам, к базам данных и т. п.) предполагает реали-

зацию идентификации, проверки подлинности и контроля доступа, регистрацию субъекта, учет носителей информации в системе ее обработки.

Кроме того, к данному классу относятся задачи по установлению и регулированию контролируемых зон вокруг технических средств обработки информации, за пределами которых становятся невозможными выделение и регистрация с помощью технических средств разведки сигналов, содержащих конфиденциальную информацию. Такие сигналы могут возникать, например, за счет появления вокруг функционирующих средств обработки информации побочных электромагнитных излучений или наводок в проводах, выходящих за пределы контролируемой зоны.

Класс 4. Регулирование использования элементов системы и защищаемой информации. Регулирование использования заключается в осуществлении запрашиваемых процедур (операций) при условии предъявления некоторых заранее обусловленных полномочий.

Для решения данного класса задач относительно конфиденциальной информации могут осуществляться такие операции, как ее дробление и ранжирование.

Дробление (расчленение) информации на части производится с таким условием, что знание какой-то одной части информации (например, знание одной операции технологии производства какого-то продукта) не позволяет восстановить всю картину, всю технологию в целом.

Ранжирование включает, во-первых, деление засекречиваемой информации по степени секретности и, во-вторых, регламентацию допуска и разграничение доступа к защищаемой информации: предоставление индивидуальных прав отдельным пользователям на доступ к необходимой им конкретной информации и на выполнение отдельных операций. Разграничение доступа к информации может осуществляться по тематическому признаку или по признаку секретности информации и определяется матрицей доступа.

Примером данного класса задач является доступ сотрудников к обслуживанию специальной техники только при наличии соответствующего разрешения.

Класс 5. Маскировка информации. Маскировка информации заключается в преобразовании данных, исключающем доступ посторонних лиц к содержанию информации и обеспечивающем доступ разрешенным пользователям при предъявлении ими специального ключа преобразования. Решение этой задачи осуществляется на основе криптографических,

некриптографических и смежных с ними (кодовое зашумление, ортогональные преобразования) преобразований.

Класс 6. Регистрация сведений. Регистрация предполагает фиксацию всех сведений о фактах, событиях, возникающих в процессе функционирования средств и систем обработки информации, относящихся к защите информации, на основании которых осуществляется решение задач оценки состояния безопасности информации с целью повышения эффективности и управления механизмами защиты.

Класс 7. Уничтожение информации. Решение задачи уничтожения информации представляется как процедура своевременного полного или частичного вывода из системы обработки элементов информации, компонентов системы, если они не представляют практической, исторической, научной ценности, а также если их дальнейшее нахождение в системе обработки снижает безопасность информации.

Необходимо отметить, что для различных классов информационно-телекоммуникационных систем уничтожение информации будет иметь определенную специфику. Так, для систем автоматизированной обработки информации типичной процедурой является уничтожение остаточной информации в элементах оперативно-запоминающих устройств, отдельных магнитных носителях, программных модулях, контрольных распечатках, выданных документах после решения соответствующей задачи обработки информации.

Для криптографических систем такой задачей может быть своевременное уничтожение носителей ключевой информации для шифрования данных в целях повышения криптостойкости (способности аппаратуры шифрования противостоять вскрытию секрета шифра).

Одной из разновидностей уничтожения информации является так называемое аварийное уничтожение, осуществляемое при явной угрозе злоумышленного доступа к информации повышенной важности.

Класс 8. Обеспечение сигнализации. Решение задачи обеспечения сигнализации состоит в реализации процедуры сбора, генерирования, передачи, отображения и хранения сигналов о состоянии механизмов защиты с целью обеспечения регулярного управления ими, а также объектами и процессами обработки информации. Этот класс задач обеспечивает обратную связь в системе управления, чем достигается обеспечение активности системы защиты. В основном такие задачи решаются с помощью технических средств сигнализации.

Класс 9. Обеспечение реагирования. Получив по каналам обратной связи информацию о состоянии системы защиты, в соответствии с законами управления орган управления должен при необходимости выработать управленческое решение, т. е. отреагировать на полученный сигнал. Реагирование на проявление дестабилизирующих факторов является признаком активности системы защиты информации, реализация которого направлена на предотвращение или снижение степени воздействия факторов на информацию.

Класс 10. Управление системой защиты информации. Этот класс объединяет широкий круг задач, связанных с контролем правильности функционирования механизмов обработки и защиты информации, оценкой внутренних и внешних угроз, планированием защиты и т. д. При этом понятие «контроль» рассматривается в узком смысле и сводится к проверкам эффективности реализации технических и, в частности, аппаратных мер защиты: соответствия элементов системы заданному их составу, текущего состояния элементов системы, работоспособности элементов системы, правильности функционирования элементов системы, отсутствия несанкционированных устройств и систем съема информации.

Класс 11. Обеспечение требуемого уровня готовности обслуживающего персонала к решению задач информационной безопасности. Приведенный ранее анализ угроз информации показал, что одной из наиболее значимых причин нарушения ее целостности являются ошибки и сбои в работе персонала. В связи с этим к рассматриваемому классу относятся задачи достижения необходимого уровня теоретической подготовки и практических навыков в работе (подготовка персонала), а также задачи формирования высокой психофизиологической устойчивости к воздействию дестабилизирующих факторов и моральной устойчивости к разглашению конфиденциальных сведений (подбор, оценка персонала, стимулирование его деятельности и др.).

К третьему виду относятся **задачи защиты информации от информационного воздействия.** К ним можно отнести следующие классы задач.

Класс 1. Защита от информационного воздействия на технические средства обработки. Информационное воздействие на технические средства обработки, хранения и передачи информации может быть направлено:

- на уничтожение информации (например, электронное подавление средств связи);
- искажение или модификацию информации и логических связей (внедрение компьютерных вирусов);
- на внедрение ложной информации в систему.

Таким образом, данный класс включает задачи реализации технических средств и организационно-технических мероприятий по защите от рассмотренных направлений воздействия.

Класс 2. Защита от информационного воздействия на общество. Задачи предполагают разработку и реализацию методов защиты от негативного воздействия через СМИ на сознание людей. Целями такого воздействия могут быть, например, навязывание общественного мнения (пропаганда), решение экономических вопросов (реклама), разрушение национальных традиций и культуры (навязывание со стороны других государств чуждых культурных ценностей) и др.

Класс 3. Защита от информационного воздействия на психику человека. Включает широкий круг задач, направленных как непосредственно на защиту от технических средств воздействия на психику (психотропного оружия), так и на определение и формирование у человека высокой стрессоустойчивости, высоких моральных качеств, позволяющих противостоять такому воздействию.

Рассмотрев содержание вышеперечисленных классов, можно сделать вывод, что под задачей защиты информации понимаются организованные возможности средств, методов и мероприятий, используемых на объекте обработки информации с целью осуществления функций защиты.

5.3. Функции защиты информации

Под *функцией защиты* понимается множество *действий,* реализаций, проведение функционально однородных мероприятий, осуществляемых на объектах обработки конфиденциальной информации различными средствами, способами и методами с целью обеспечения заданных уровней защищенности информации. Множество функций обеспечения защиты в различных их комбинациях должно создавать условия для обеспечения надежной защиты независимо от условий внешних воздействий, внутренних неопределенностей систем обработки и защиты информации.

Состояния и функции системы защиты информации

В зависимости от событий потенциальных воздействий угроз и мер, снижающих их влияние, система защиты переходит в определенные состояния, соответствующие событиям.

Состояние 1 – защита информации обеспечена, если при наличии условий, способствующих появлению угроз, их воздействие на защищае-

мую информацию предотвращено или ликвидированы последствия такого воздействия.

Состояние 2 – защита информации нарушена, если невозможно предотвратить воздействие на нее угроз, однако оно обнаружено и локализовано.

Состояние 3 – защита информации разрушена, если результаты воздействий на нее угроз не только не предотвращены, но и не локализованы.

Множество функций защиты информации определяется следующей последовательностью действий, обеспечивающей выполнение конечной цели – достижение требуемого уровня информационной безопасности. Прежде всего необходимо попытаться предупредить возникновение условий, благоприятствующих появлению угроз информации. Выполнение этой функции в связи с большим количеством таких угроз и случайным характером их проявлений имеет вероятность, близкую к нулю. Поэтому следующим шагом должно быть своевременное обнаружение проявившихся угроз и предупреждение их воздействия на информацию. Если все-таки такое воздействие произошло, необходимо вовремя его обнаружить и локализовать с целью недопущения распространения этого воздействия на всю конфиденциальную информацию, обрабатываемую на объекте. И последним шагом для защиты должна быть ликвидация последствий указанного воздействия для восстановления требуемого состояния безопасности информации. Рассмотрим эти функции несколько подробнее.

Функция 1 – предупреждение проявления угроз. Реализация этой функции имеет упреждающую цель и должна способствовать такому архитектурно-функциональному построению современных систем обработки и защиты информации, которое обеспечивало бы минимальные возможности появления дестабилизирующих факторов в различных условиях функционирования систем. Например, для предупреждения возможности установки в помещении закладных устройств необходимо с помощью технических средств и организационных мероприятий обеспечить невозможность несанкционированного доступа в него.

Функция 2 – обнаружение проявившихся угроз и предупреждение их воздействия на информацию. Осуществляется комплекс мероприятий, в результате которых проявившиеся угрозы должны быть обнаружены до их воздействия на защищаемую информацию, а также обеспечено недопущение воздействий этих угроз на защищаемую информацию в условиях их

проявления и обнаружения. Так, для нейтрализации закладных устройств необходимо регулярно проводить специальные проверки помещений, устанавливать системы их автоматического поиска, а для предупреждения их воздействия на конфиденциальную информацию – использовать устройства защиты типа генераторов объемного зашумления, позволяющих создавать вокруг устройств обработки информации шумовое поле.

Функция 3 – обнаружение воздействия угроз на защищаемую информацию и локализация этого воздействия. Содержание функции направлено на непрерывный контроль средств, комплексов, систем обработки, защиты информации и различных компонентов защищаемой информации с целью своевременного обнаружения фактов воздействия на них угроз. Своевременное обнаружение предполагает обеспечение реальной возможности локализации воздействия на информацию, т. е. минимизацию возможного нарушения ее целостности и защищенности и недопущение распространения этого воздействия за пределы допустимых размеров. В компьютерных системах, например, эту функцию реализуют аппаратно-программные средства контроля и регистрации попыток несанкционированного доступа в систему или к информации (цифровая подпись).

Функция 4 – ликвидация последствий воздействия угроз. Функция предусматривает проведение мероприятий защиты в отношении обнаруженного и локализованного воздействия угроз на информацию, т. е. осуществляется восстановление системы обработки, защиты информации и состояния защищаемой информации путем применения соответствующего множества средств, способов и мероприятий защиты.

5.4. Стратегии защиты информации

Стратегия – это общая, рассчитанная на перспективу руководящая установка при организации и обеспечении соответствующего вида деятельности, направленная на то, чтобы наиболее важные цели этой деятельности достигались при наиболее рациональном расходовании имеющихся ресурсов.

Организация защиты информации в самом общем виде может быть определена как поиск оптимального компромисса между потребностями в защите и необходимыми для этих целей ресурсами.

Потребности в защите обусловливаются прежде всего важностью и объемами защищаемой информации, а также условиями ее хранения, обработки и использования. Эти условия определяются уровнем (качеством)

структурно-организационного построения объекта обработки информации, уровнем организации технологических схем обработки, местом и условиями расположения объекта и его компонентов и другими параметрами.

Размер ресурсов на защиту информации ограничивается определенным пределом либо определяется условием обязательного достижения требуемого уровня защиты. В первом случае защита должна быть организована так, чтобы при выделенных ресурсах обеспечивался максимально возможный уровень защиты, а во втором – чтобы требуемый уровень защиты обеспечивался при минимальном расходовании ресурсов.

Сформулированные задачи есть не что иное, как прямая и обратная постановка оптимизационных задач. Существует две проблемы, затрудняющие формальное решение.

Первая проблема – процессы защиты информации находятся в значительной зависимости от большого числа случайных и труднопредсказуемых факторов, таких как поведение злоумышленника, воздействие природных явлений, сбои и ошибки в процессе функционирования элементов системы обработки информации и др.

Вторая проблема – среди средств защиты весьма заметное место занимают организационные меры, связанные с действием человека.

Обоснование числа и содержания необходимых стратегий будем осуществлять по двум критериям: требуемому уровню защиты и степени свободы действий при организации защиты. Значения первого критерия лучше всего выразить множеством угроз, относительно которых должна быть обеспечена защита:

1) от наиболее опасных из известных (ранее появившихся) угроз;

2) всех известных угроз;

3) ото всех потенциально возможных угроз.

Второй критерий выбора стратегий защиты сводится к тому, что организаторы и исполнители процессов защиты имеют относительно полную свободу при распоряжении методами и средствами защиты и некоторую степень свободы вмешательства в архитектурное построение системы обработки информации, а также в организацию и обеспечение технологии ее функционирования. По этому аспекту удобно выделить три различные степени свободы.

1. Никакое вмешательство в систему обработки информации не допускается. Такое требование может быть предъявлено к уже действующим

системам обработки информации, и нарушение процесса их функционирования для установки механизмов защиты не разрешается.

2. К архитектурному построению системы обработки информации и технологии ее работы допускается предъявлять требования неконцептуального характера. Другими словами, допускается приостановка процесса функционирования системы обработки информации для установки некоторых механизмов защиты.

3. Требования любого уровня, обусловленные потребностями защиты информации, принимаются в качестве обязательных условий при построении системы обработки информации, организации и обеспечении их функционирования.

Так, выбирая оборонительную стратегию, подразумевают, что при недопущении вмешательства в процесс функционирования системы обработки информации можно нейтрализовать лишь наиболее опасные угрозы. Например, данная стратегия, применяемая для существующего объекта, может включать разработку организационных мер использования технических средств по ограничению несанкционированного допуска к объекту. Упреждающая стратегия предполагает тщательное исследование возможных угроз системы обработки информации и разработку мер по их нейтрализации еще на стадии проектирования и изготовления системы. При этом нет смысла на данном этапе рассматривать ограниченное множество подобных угроз.

Вопросы и задания для самоконтроля

1. Какие существуют условия эффективности защиты информации?

2. В чем заключается особенность методов формирования функций защиты информации?

3. Определите основные виды задач защиты информации и перечислите входящие в каждый вид классы задач.

4. Что такое функции защиты информации?

5. Охарактеризуйте каждую функцию защиты информации.

6. Дайте определение стратегии защиты информации.

Глава 6. ОСНОВНЫЕ МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

6.1. Определения, классификация и характеристика основных методов и средств обеспечения информационной безопасности

Множество и разнообразие возможных средств защиты информации определяется, прежде всего, возможными способами воздействия на дестабилизирующие факторы или порождающие их причины, причем воздействия в направлении, способствующем повышению показателей защищенности или (по крайней мере) сохранению прежних (ранее достигнутых) их значений.

Рассмотрим содержание представленных способов обеспечения безопасности.

Препятствие заключается в создании на пути возникновения или распространения дестабилизирующего фактора некоторого барьера, не позволяющего соответствующему фактору принять опасные размеры. Типичными примерами препятствий являются блокировки, не позволяющие техническому устройству или программе выйти за опасные границы; создание физических препятствий на пути злоумышленников, экранирование помещений и технических средств и т. п.

Управление есть определение на каждом шаге функционирования систем обработки информации таких управляющих воздействий на элементы системы, следствием которых будет решение (или способствование решению) одной или нескольких задач защиты информации. Например, управление доступом на объект включает следующие функции защиты:

- идентификацию лиц, претендующих на доступ, персонала и ресурсов системы (присвоение каждому объекту персонального идентификатора);
- опознавание (установление подлинности) объекта или субъекта по предъявленному идентификатору;

• проверку полномочий (проверка соответствия дня недели, времени суток, запрашиваемых ресурсов и процедур установленному регламенту);

• регистрацию (протоколирование) обращений к защищаемым ресурсам;

• реагирование (сигнализация, отключение, задержка работ, отказ в процессе) при попытках несанкционированных действий.

Маскировка предполагает такие преобразования информации, вследствие которых она становится недоступной для злоумышленников или такой доступ существенно затрудняется, а также комплекс мероприятий по уменьшению степени распознавания самого объекта. К маскировке относятся криптографические методы преобразования информации, скрытие объекта, дезинформация и легендирование, а также меры по созданию шумовых полей, маскирующих информационные сигналы.

Регламентация как способ защиты информации заключается в разработке и реализации в процессе функционирования объекта комплекса мероприятий, создающих такие условия, при которых существенно затрудняются проявление и воздействие угроз. К регламентации относится разработка таких правил обращения с конфиденциальной информацией и средствами ее обработки, которые позволили бы максимально затруднить получение этой информации злоумышленником.

Принуждение – такой метод защиты, при котором пользователи и персонал системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.

Побуждение есть способ защиты информации, при котором пользователи и персонал объекта внутренне (т. е. материальными, моральными, этическими, психологическими и другими мотивами) побуждаются к соблюдению всех правил обработки информации.

Как отдельный, применяемый при ведении активных действий противоборствующими сторонами, можно выделить такой способ, как **нападение.** При этом подразумевается как применение информационного оружия при ведении информационной войны, так и непосредственное физическое уничтожение противника (при ведении боевых действий) или его средств разведки.

Рассмотренные способы обеспечения защиты информации реализуются с применением различных методов и средств. При этом различают формальные и неформальные средства. К формальным относятся такие

средства, которые выполняют свои функции по защите информации формально, т. е. преимущественно без участия человека. К неформальным относятся средства, основу которых составляет целенаправленная деятельность людей. Формальные средства делятся на физические, аппаратные и программные.

Физические средства – механические, электрические, электромеханические и подобные устройства и системы, которые функционируют автономно, создавая различного рода препятствия на пути дестабилизирующих факторов.

Аппаратные средства – различные электронные и электронно-механические и другие устройства, схемно встраиваемые в аппаратуру системы обработки данных или сопрягаемые с ней специально для решения задач защиты информации. Например, для защиты от утечки по техническим каналам используются генераторы шума.

Физические и аппаратные средства объединяются в класс **технических средств** защиты информации.

Программные средства – специальные пакеты программ или отдельные программы, включаемые в состав программного обеспечения автоматизированных систем с целью решения задач защиты информации. Это могут быть различные программы по криптографическому преобразованию данных, контролю доступа, защиты от вирусов и др.

Неформальные средства делятся на организационные, законодательные и морально-этические.

Организационные средства – специально предусматриваемые в технологии функционирования объекта организационно-технические мероприятия для решения задач защиты информации, осуществляемые в виде целенаправленной деятельности людей.

Законодательные средства – существующие в стране или специально издаваемые нормативно-правовые акты, с помощью которых регламентируются права и обязанности, связанные с обеспечением защиты информации, всех лиц и подразделений, имеющих отношение к функционированию системы, а также устанавливается ответственность за нарушение правил обработки информации, следствием чего может быть нарушение защищенности информации.

Морально-этические средства (нормы) – сложившиеся в обществе или данном коллективе моральные нормы или этические правила, соблю-

дение которых способствует защите информации, а нарушение их приравнивается к несоблюдению правил поведения в обществе или коллективе. Именно человек, сотрудник предприятия или учреждения, допущенный к секретам и накапливающий в своей памяти колоссальные объемы информации, в том числе секретной, нередко становится источником утечки этой информации или по его вине соперник получает возможность несанкционированного доступа к носителям защищаемой информации.

Морально-нравственные методы защиты информации предполагают прежде всего воспитание сотрудника, допущенного к секретам, т. е. проведение специальной работы, направленной на формирование у него системы определенных качеств, взглядов и убеждений (патриотизма, понимания важности и полезности защиты информации и для него лично), и обучение сотрудника, владеющего сведениями, составляющими охраняемую тайну, правилам и методам защиты информации, привитие ему навыков работы с носителями секретной и конфиденциальной информации.

А теперь рассмотрим основные способы защиты животного мира в сравнении с рассмотренными способами защиты информации.

1. Пассивная защита. Перекрывает все возможные каналы воздействия угроз и предполагает «надевание брони» на себя и создание территориальных препятствий. Налицо полное соответствие такому способу защиты информации, как препятствие.

2. Изменение местоположения. Желание спрятаться можно соотнести с таким способом, как сокрытие.

3. Изменение собственной внешности, мимикрия – слияние с ландшафтом и т. п. Цель – представиться объектом, неинтересным или незаметным для нападающей стороны. Аналогичную функцию защиты информации реализуют ее маскировкой.

4. Воспитание навыков безопасности у потомства, доведение этих навыков до уровня инстинкта. Для систем защиты информации аналогичные навыки у обслуживающего персонала формируются принуждением и побуждением.

5. Выработка определенных правил жизнедеятельности, способствующих выживанию и сохранению рода. К таким правилам, выработанным природой, можно отнести мирное сосуществование особей одного вида, жизнь в стаях (стадах) и т. д. Другими словами, природа регламентирует необходимые для безопасности правила жизни.

Таким образом, анализ присущих животному миру защитных свойств, положенный в основу так называемой абсолютной системы защиты, показывает, что все они соответствуют рассмотренным способам защиты информации, что подтверждает полноту их формирования.

6.2. Криптографические методы защиты информации

Проблема защиты информации путем ее преобразования, исключающего ее прочтение посторонним лицом, волновала человеческий ум с давних времен. История криптографии – ровесница истории человеческого языка. Более того, первоначально письменность сама по себе была криптографической системой, так как в древних обществах ею владели только избранные. Священные книги Древнего Египта, Древней Индии тому примеры.

Разные люди понимают под шифрованием разные вещи. Дети играют в секретные языки и создают игрушечные шифры. Это, однако, не имеет ничего общего с настоящей криптографией. Настоящая криптография должна обеспечивать такой уровень секретности, чтобы можно было надежно защитить критическую информацию от расшифровки крупными организациями – такими как мафия, транснациональные корпорации и крупные государства. Настоящая криптография в прошлом использовалась лишь в военных целях. Однако сейчас, в связи со становлением информационного общества, она становится центральным инструментом для обеспечения конфиденциальности.

По мере формирования информационного общества крупным государствам становятся доступны технологические средства тотального надзора за миллионами людей. Поэтому криптография становится одним из основных инструментов, обеспечивающих конфиденциальность, доверие, авторизацию, электронные платежи, корпоративную безопасность и бесчисленное множество других важных вещей.

Криптография не является более придумкой военных, с которой не стоит связываться. Широкое распространение криптографии является одним из немногих способов защитить человека от ситуации, когда он вдруг обнаруживает, что живет в государстве, которое может контролировать каждый его шаг.

Бурное развитие криптографические системы получили в годы Первой и Второй мировых войн. Начиная с послевоенного времени и по нынешний день появление вычислительных средств ускорило разработку и совершенствование криптографических методов.

Почему проблема использования криптографических методов в информационных системах стала в настоящий момент особо актуальна?

С одной стороны, расширилось использование компьютерных сетей, в частности глобальной сети Интернет, по которым передаются большие объемы информации государственного, военного, коммерческого и частного характера, не допускающего возможности доступа к ней посторонних лиц.

С другой стороны, появление новых мощных компьютеров, технологий сетевых и нейронных вычислений сделало возможной дискредитацию криптографических систем, еще недавно считавшихся практически нераскрываемыми.

Проблемой защиты информации путем ее преобразования занимается *криптология*. Криптология разделяется на два направления – *криптографию* и *криптоанализ*. Цели этих направлений прямо противоположны.

Криптография занимается поиском и исследованием математических методов преобразования информации.

Сфера интересов *криптоанализа* – исследование возможности расшифровывания информации без знания ключей.

Современная криптография включает в себя четыре крупных раздела:

1. Симметричные криптосистемы.
2. Криптосистемы с открытым ключом.
3. Системы электронной подписи.
4. Управление ключами.

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.

Терминология

Итак, криптография дает возможность преобразовать информацию таким образом, что ее прочтение (восстановление) возможно только при знании ключа.

В качестве информации, подлежащей шифрованию и дешифрованию, будут рассматриваться тексты, построенные на некотором алфавите. Под терминами «текст» и «алфавит» понимается следующее.

Алфавит – конечное множество используемых для кодирования информации знаков.

Текст – упорядоченный набор из элементов алфавита.

В качестве примеров алфавитов, используемых в современных информационных системах, можно привести следующие:

- алфавит 233 – 33 буквы русского алфавита и пробел;
- алфавит 2256 – символы, входящие в стандартные коды;
- бинарный алфавит – 2 = {0,1};
- восьмеричный алфавит или шестнадцатеричный алфавит.

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.

Ключ – информация, необходимая для беспрепятственного шифрования и дешифрования текстов.

Криптографическая система представляет собой семейство T [T1, T2, ..., Tк] преобразований открытого текста. Члены этого семейства индексируются, или обозначаются символом к; параметр к является ключом. Пространство ключей *к* – это набор возможных значений ключа. Обычно ключ представляет собой последовательный ряд букв алфавита.

Криптосистемы разделяются на *симметричные* и *с открытым ключом*.

В *симметричных криптосистемах* и для шифрования, и для дешифрования используется один и тот же ключ.

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.

Термины *распределение ключей* и *управление ключами* относятся к процессам системы обработки информации, содержанием которых является составление и распределение ключей между пользователями.

Электронной (цифровой) подписью называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения.

Криптостойкостью называется характеристика шифра, определяющая его стойкость к дешифрованию без знания ключа (т. е. криптоанализу). Имеется несколько показателей криптостойкости, среди которых:

- количество всех возможных ключей;

• среднее время, необходимое для криптоанализа.

Преобразование T_κ определяется соответствующим алгоритмом и значением параметра κ. Эффективность шифрования с целью защиты информации зависит от сохранения тайны ключа и криптостойкости шифра.

Требования к криптосистемам

Процесс криптографического закрытия данных может осуществляться как программно, так и аппаратно. Аппаратная реализация отличается существенно большей стоимостью, однако ей присущи и преимущества: высокая производительность, простота, защищенность и т. д. Программная реализация более практична, допускает известную гибкость в использовании.

Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:

• зашифрованное сообщение должно поддаваться чтению только при наличии ключа;

• число операций, необходимых для определения использованного ключа шифрования по фрагменту шифрованного сообщения и соответствующего ему открытого текста, должно быть не меньше общего числа возможных ключей;

• число операций, необходимых для расшифровывания информации путем перебора всевозможных ключей, должно иметь строгую нижнюю оценку и выходить за пределы возможностей современных компьютеров (с учетом возможности использования сетевых вычислений);

• знание алгоритма шифрования не должно влиять на надежность защиты;

• незначительное изменение ключа должно приводить к существенному изменению вида зашифрованного сообщения даже при использовании одного и того же ключа;

• структурные элементы алгоритма шифрования должны быть неизменными;

• дополнительные биты, вводимые в сообщение в процессе шифрования, должны быть полностью и надежно скрыты в шифрованном тексте;

• длина шифрованного текста должна быть равной длине исходного текста;

• не должно быть простых и легко устанавливаемых зависимостей между ключами, последовательно используемыми в процессе шифрования;

• любой ключ из множества возможных должен обеспечивать надежную защиту информации;

• алгоритм должен допускать как программную, так и аппаратную реализацию, при этом изменение длины ключа не должно вести к качественному ухудшению алгоритма шифрования.

Основные алгоритмы шифрования

Метод шифровки-дешифровки называют шифром. Некоторые алгоритмы шифрования основаны на том, что сам метод шифрования (алгоритм) является секретным. Ныне такие методы представляют лишь исторический интерес и не имеют практического значения. Все современные алгоритмы используют ключ для управления шифровкой и дешифровкой; сообщение может быть успешно дешифровано только если известен ключ. Ключ, используемый для дешифровки, может не совпадать с ключом, используемым для шифрования, однако в большинстве алгоритмов ключи совпадают.

Алгоритмы с использованием ключа делятся на два класса: симметричные (или алгоритмы с секретным ключом) и асимметричные (или алгоритмы с открытым ключом). Разница в том, что симметричные алгоритмы используют один и тот же ключ для шифрования и для дешифрования (или же ключ для дешифровки просто вычисляется по ключу шифровки), в то время как асимметричные алгоритмы используют разные ключи, и ключ для дешифровки не может быть вычислен по ключу шифровки.

Симметричные алгоритмы подразделяют на потоковые шифры и блочные шифры. Потоковые позволяют шифровать информацию побитово, в то время как блочные работают с некоторым набором битов данных (обычно размер блока составляет 64 бита) и шифруют этот набор как единое целое.

Асимметричные шифры (также именуемые алгоритмами с открытым ключом или – в более общем плане – криптографией с открытым ключом) допускают, чтобы открытый ключ был доступен всем (скажем, опубликован в газете). Это позволяет любому зашифровать сообщение. Однако расшифровать это сообщение сможет только нужный человек (тот, кто владеет ключом дешифровки). Ключ для шифрования называют *открытым ключом*, а ключ для дешифрования – *закрытым ключом* или *секретным ключом*.

Современные алгоритмы шифровки-дешифровки достаточно сложны и их невозможно проводить вручную. Настоящие криптографические алгоритмы разработаны для пользования компьютерами или специальными

аппаратными устройствами. В большинстве приложений криптография производится программным обеспечением и имеется множество доступных криптографических пакетов.

Вообще говоря, симметричные алгоритмы работают быстрее, чем асимметричные. На практике оба типа алгоритмов часто используются вместе: алгоритм с открытым ключом используется для того, чтобы передать случайным образом сгенерированный секретный ключ, который затем используется для дешифровки сообщения.

Многие качественные криптографические алгоритмы доступны широко – в книжном магазине, библиотеке, патентном бюро или в Интернете. В России за стандарт шифрования принят ГОСТ 28147–89.

Цифровые подписи

Некоторые из асимметричных алгоритмов могут использоваться для генерирования *цифровой подписи*. Цифровой подписью называют блок данных, сгенерированный с использованием некоторого секретного ключа. При этом с помощью открытого ключа можно проверить, что данные были действительно сгенерированы с помощью этого секретного ключа. Алгоритм генерации цифровой подписи должен обеспечивать невозможность без секретного ключа создать подпись, которая при проверке окажется правильной.

Цифровые подписи используются для того, чтобы подтвердить, что сообщение пришло действительно от данного отправителя (в предположении, что лишь отправитель обладает секретным ключом, соответствующим его открытому ключу). Также подписи используются для проставления *штампа времени* на документах: сторона, которой мы доверяем, подписывает документ со штампом времени с помощью своего секретного ключа и, таким образом, подтверждает, что документ уже существовал в момент, объявленный в штампе времени.

Цифровые подписи также можно использовать для удостоверения *(сертификации)* того, что документ принадлежит определенному лицу. Это делается так: открытый ключ и информация о том, кому он принадлежит, подписываются стороной, которой доверяем. При этом доверять подписывающей стороне мы можем на основании того, что ее ключ был подписан третьей стороной. Таким образом возникает иерархия доверия. Очевидно, что некоторый ключ должен быть корнем иерархии (т. е. ему мы доверяем не потому, что он кем-то подписан, а потому, что мы верим априори, что ему можно доверять). В *централизованной инфраструктуре клю-*

чей имеется очень небольшое количество корневых ключей сети (например, облеченные полномочиями государственные агентства; их также называют *сертификационными агентствами*). В *распределенной инфраструктуре* нет необходимости иметь универсальные для всех корневые ключи, и каждая из сторон может доверять своему набору корневых ключей (скажем, своему собственному ключу и ключам, им подписанным). Эта концепция носит название *сети доверия*.

Цифровая подпись документа обычно создается так: из документа генерируется так называемый *дайджест* и к нему добавляются информация о том, кто подписывает документ, штамп времени и пр. Получившаяся строка далее зашифровывается секретным ключом подписывающего с использованием того или иного алгоритма. Получившийся зашифрованный набор битов и представляет собой подпись. К подписи обычно прикладывается открытый ключ подписывающего. Получатель сначала решает для себя, доверяет ли он тому, что открытый ключ принадлежит именно тому, кому должен принадлежать (с помощью сети доверия или априорного знания), и затем дешифрует подпись с помощью открытого ключа. Если подпись нормально дешифровалась и ее содержимое соответствует документу (дайджест и др.), то сообщение считается подтвержденным.

Свободно доступны несколько методов создания и проверки цифровых подписей (ГОСТ 34.10–94).

Криптографические хеш-функции

Криптографические хеш-функции используются обычно для генерации дайджеста сообщения при создании цифровой подписи. Хеш-функции преобразовывают сообщение в имеющее фиксированный размер *хеш-значение* таким образом, что все множество возможных сообщений распределяется равномерно по множеству хеш-значений. При этом криптографическая хеш-функция делает это так, что практически невозможно подогнать документ к заданному хеш-значению.

Криптографические хеш-функции обычно производят значения длиной в 128 и более бит. Это число значительно больше, чем количество сообщений, которые когда-либо будут существовать в мире.

Много хороших криптографических хеш-функций доступно бесплатно.

Криптографические генераторы случайных чисел

Криптографические генераторы случайных чисел производят случайные числа, которые используются в криптографических приложениях,

например для генерации ключей. Обычные генераторы случайных чисел, имеющиеся во многих языках программирования и программных средах, не подходят для нужд криптографии (они создавались с целью получить статистически случайное распределение, криптоаналитики могут предсказать поведение таких случайных генераторов).

В идеале случайные числа должны основываться на настоящем физическом источнике случайной информации, которую невозможно предсказать. Примеры таких источников включают шумящие полупроводниковые приборы, младшие биты оцифрованного звука, интервалы между прерываниями устройств или нажатиями клавиш. Полученный от физического источника шум затем «дистиллируется» криптографической хеш-функцией так, чтобы каждый бит зависел от каждого бита. Достаточно часто для хранения случайной информации используется довольно большой пул (несколько тысяч бит), и каждый бит пула делается зависимым от каждого бита шумовой информации и каждого другого бита пула криптографически надежным способом.

Когда нет настоящего физического источника шума, приходится пользоваться псевдослучайными числами. Такая ситуация нежелательна, но часто возникает на компьютерах общего назначения. Всегда нужно получить некий шум окружения, скажем, от величины задержек в устройствах, цифры статистики использования ресурсов, сетевой статистики, прерываний от клавиатуры или чего-то иного. Задачей является получить данные, непредсказуемые для внешнего наблюдателя. Для достижения этого случайный пул должен содержать как минимум 128 бит настоящей энтропии.

Криптографические генераторы псевдослучайных чисел обычно используют большой пул, содержащий случайную информацию. Биты генерируются путем выборки из пула с возможным прогоном через криптографическую хеш-функцию, чтобы спрятать содержимое пула от внешнего наблюдателя. Когда требуется новая порция битов, пул перемешивается путем шифровки со случайным ключом (его можно взять из не использованной пока части пула) так, чтобы каждый бит пула зависел от каждого другого бита. Новый шум окружения должен добавляться к пулу перед перемешиванием, дабы сделать предсказание новых значений пула еще более сложным.

Несмотря на то, что при аккуратном проектировании криптографически надежный генератор случайных чисел реализовать не так уж и труд-

но, этот вопрос часто упускают из виду. Таким образом, следует подчеркнуть важность криптографического генератора случайных чисел – если он сделан плохо, он может легко стать самым уязвимым элементом системы.

Обеспечиваемая шифром степень защиты

Хорошие криптографические системы создаются таким образом, чтобы сделать их вскрытие как можно более трудным делом. Можно построить системы, которые на практике невозможно вскрыть (хотя доказать сей факт обычно нельзя). При этом не требуется очень больших усилий для реализации. Единственное, что требуется, – это аккуратность и базовые знания. Нет прощения разработчику, если он оставил возможность для вскрытия системы. Все механизмы, которые могут использоваться для взлома системы, надо задокументировать и довести до сведения конечных пользователей.

Теоретически любой шифровальный алгоритм с использованием ключа может быть вскрыт методом перебора всех значений ключа. Если ключ подбирается *методом грубой силы*, требуемая мощность компьютера растет экспоненциально с увеличением длины ключа.

Однако длина ключа это еще не все. Многие шифры можно вскрыть и не перебирая всех возможных комбинаций. Очень трудно придумать шифр, который нельзя было бы вскрыть другим, более эффективным способом.

Вообще следует держаться в стороне от неопубликованных или секретных алгоритмов. Часто разработчик такого алгоритма не уверен в его надежности или же надежность зависит от секретности самого алгоритма. Ни один алгоритм, секретность которого зависит от секретности самого алгоритма, не является надежным. В частности, имея шифрующую программу, можно нанять программиста, который восстановит ее алгоритм методом обратной инженерии. Опыт показывает, что большинство секретных алгоритмов, ставших впоследствии достоянием общественности, оказались до смешного ненадежными.

Длины ключей, используемых в криптографии с открытым ключом, обычно значительно больше, чем в симметричных алгоритмах. Здесь проблема заключается не в подборе ключа, а в воссоздании секретного ключа по открытому.

Чтобы дать представление о степени сложности вскрытия ключа, скажем, что модули длиной 256 бит легко подбираются обычными программистами. Ключи в 384 бита могут быть вскрыты исследовательской группой университета или компании; 512-битовые ключи находятся в пре-

делах досягаемости крупных государств. Ключи длиной 768 бит, вероятно, не будут надежны продолжительное время. Ключи длиной 1024 бита могут считаться безопасными до тех пор, пока не будет существенного прогресса в алгоритме факторизации; ключи длиной 2048 бит большинство считает надежными на десятилетия.

Важно подчеркнуть, что **степень надежности криптографической системы определяется ее слабейшим звеном.** Нельзя упускать из виду ни одного аспекта разработки системы – от выбора алгоритма до политики использования и распространения ключей.

Криптоанализ и атаки на криптосистемы

Криптоанализ – это наука о дешифровке закодированных сообщений не зная ключей. Имеется много криптоаналитических подходов. Некоторые из наиболее важных для разработчиков приведены ниже.

Атака со знанием лишь шифрованного текста. Это ситуация, когда атакующий не знает ничего о содержании сообщения и ему приходится работать лишь с самим шифрованным текстом. На практике часто можно сделать правдоподобные предположения о структуре текста, поскольку многие сообщения имеют стандартные заголовки. Даже обычные письма и документы начинаются с легко предсказуемой информации. Также часто можно предположить, что некоторый блок информации содержит заданное слово.

Атака со знанием содержимого шифровки. Атакующий знает или может угадать содержимое всего или части зашифрованного текста. Задача заключается в расшифровке остального сообщения. Это можно сделать либо путем вычисления ключа шифровки, либо минуя это.

Атака с заданным текстом. Атакующий имеет возможность получить шифрованный документ для любого нужного ему текста, но не знает ключа. Задачей является нахождение ключа. Некоторые методы шифрования, и в частности K8A, весьма уязвимы для атак этого типа. При использовании таких алгоритмов надо тщательно следить, чтобы атакующий не мог зашифровать заданный им текст.

Атака с подставкой. Атака направлена на обмен шифрованными сообщениями и в особенности на протокол обмена ключами. Идея заключается в том, что, когда две стороны обмениваются ключами для секретной коммуникации (например, используя шифр Диффи-Хелмана), противник внедряется между ними на линии обмена сообщениями. Далее противник выдает каждой стороне свои ключи. В результате каждая из сторон будет

иметь разные ключи, каждый из которых известен противнику. Теперь противник будет расшифровывать каждое сообщение своим ключом и затем зашифровывать его с помощью другого ключа перед отправкой адресату. Стороны будут иметь иллюзию секретной переписки, в то время как на самом деле противник читает все сообщения.

Один из способов предотвратить атаки такого типа заключается в том, что стороны при обмене ключами вычисляют криптографическую хеш-функцию значения протокола обмена (или по меньшей мере значения ключей), подписывают ее алгоритмом цифровой подписи и посылают подпись другой стороне. Получатель проверит подпись и то, что значение хеш-функции совпадает с вычисленным значением.

Атака с помощью таймера. Этот новый тип атак основан на последовательном измерении времени, затрачиваемого на выполнение операции возведения в степень по модулю целого числа.

Имеется множество других криптографических атак и криптоаналитических подходов. Однако приведенные выше являются, по-видимому, наиболее важными для практической разработки систем. Если кто-либо собирается создавать свой алгоритм шифрования, ему необходимо понимать данные вопросы значительно глубже.

Выбор системы защиты для конкретных ИС должен быть основан на глубоком анализе слабых и сильных сторон тех или иных методов защиты. Обоснованный выбор той или иной системы защиты, в общем-то, должен опираться на какие-то критерии эффективности. К сожалению, до сих пор не разработаны подходящие методики оценки эффективности криптографических систем.

Наиболее простой критерий такой эффективности – вероятность раскрытия ключа или мощность множества ключей. По сути, это то же самое, что и криптостойкость. Для ее численной оценки можно использовать также и сложность раскрытия шифра путем перебора всех ключей.

Однако этот критерий не учитывает других важных *требований к криптосистемам:*

- невозможность раскрытия или осмысленной модификации информации на основе анализа ее структуры;
- совершенство используемых протоколов защиты;
- минимальный объем применяемой ключевой информации;
- минимальная сложность реализации (в количестве машинных операций), ее стоимость;
- высокая оперативность.

Желательно, конечно, использование некоторых интегральных показателей, учитывающих указанные факторы.

Для учета стоимости, трудоемкости и объема ключевой информации можно использовать удельные показатели – отношение указанных параметров к мощности множества ключей шифра.

Часто более эффективным при выборе и оценке криптографической системы является применение экспертных оценок и имитационное моделирование.

В любом случае выбранный комплекс криптографических методов должен сочетать как удобство, гибкость и оперативность использования, так и надежную защиту от злоумышленников циркулирующей в системах информации.

6.3. Антивирусные программы

Для обнаружения, удаления компьютерных вирусов и защиты от них разработаны специальные программы, которые позволяют обнаруживать и уничтожать вирусы. Такие программы называются антивирусными. Современные антивирусные программы представляют собой многофункциональные продукты, сочетающие в себе как превентивные, профилактические средства, так и средства лечения вирусов и восстановления данных.

Требования к антивирусным программам

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

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

2. Размеры вирусной базы программы (количество вирусов, которые правильно определяются программой). С учетом постоянного появления новых вирусов база данных должна регулярно обновляться – что толку от программы, не видящей половину новых вирусов и, как следствие, создающей ошибочное ощущение «чистоты» компьютера. Сюда же следует отнести и возможность программы определять разнообразные типы виру-

сов, и умение работать с файлами различных типов (архивы, документы). Немаловажным также является наличие резидентного монитора, осуществляющего проверку всех новых файлов «на лету» (т. е. автоматически, по мере их записи на диск).

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

4. Многоплатформенность (наличие версий программы под различные операционные системы). Конечно, если антивирус используется только дома, на одном компьютере, то этот параметр не имеет большого значения. Но вот антивирус для крупной организации просто обязан поддерживать все распространенные операционные системы. Кроме того, при работе в сети немаловажным является наличие серверных функций, предназначенных для административной работы, а также возможность работы с различными видами серверов.

Характеристика антивирусных программ

Антивирусные программы делятся следующим образом: программы-детекторы, программы-доктора, программы-ревизоры, программы-фильтры, программы-вакцины.

Программы-детекторы обеспечивают поиск и обнаружение вирусов в оперативной памяти и на внешних носителях и при обнаружении выдают соответствующее сообщение. Различают детекторы универсальные и специализированные.

Универсальные детекторы в своей работе используют проверку неизменности файлов путем подсчета и сравнения с эталоном контрольной суммы. Недостаток универсальных детекторов связан с невозможностью определения причин искажения файлов.

Специализированные детекторы выполняют поиск известных вирусов по их сигнатуре (повторяющемуся участку кода). Недостаток таких детекторов состоит в том, что они неспособны обнаруживать все известные вирусы.

Детектор, позволяющий обнаруживать несколько вирусов, называют полидетектором.

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

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

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

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

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

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

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

При попытке какой-либо программы произвести указанные действия «сторож» посылает пользователю сообщение и предлагает запретить или

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

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

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

Краткий обзор антивирусных программ

При выборе антивирусной программы необходимо учитывать не только процент обнаружения вирусов, но и способность обнаруживать новые вирусы, количество вирусов в антивирусной базе, частоту ее обновления, наличие дополнительных функций.

В настоящее время серьезный антивирус должен уметь распознавать не менее 25000 вирусов. Это не значит, что все они находятся «на воле». На самом деле большинство из них или уже прекратили свое существование, или находятся в лабораториях и не распространяются. Реально можно встретить 200–300 вирусов, а опасность представляют только несколько десятков из них.

Существует множество антивирусных программ. Рассмотрим наиболее известные из них.

Norton AntiVirus 4.0 и 5.0 (производитель «Symantec»). Один из наиболее известных и популярных антивирусов. Процент распознавания вирусов очень высокий (близок к 100 %). В программе используется механизм, который позволяет распознавать новые неизвестные вирусы.

В интерфейсе программы Norton AntiVirus имеется функция Live-Update, позволяющая щелчком по одной-единственной кнопке обновлять через Web как программу, так и набор сигнатур вирусов. Мастер по борьбе с вирусами выдает подробную информацию об обнаруженном вирусе, а также предоставляет вам возможность выбора: удалять вирус либо в автоматическом режиме, либо более осмотрительно, посредством пошаговой процедуры, которая позволяет увидеть каждое из выполняемых в процессе удаления действий.

Антивирусные базы обновляются очень часто (иногда обновления появляются несколько раз в неделю). Имеется резидентный монитор.

Недостатком данной программы является сложность настройки (хотя базовые настройки изменять практически не требуется).

Dr Solomon's AntiVirus (производитель «Dr Solomon's Software»). Считается одним из самых лучших антивирусов (Евгений Касперский как-то сказал, что это единственный конкурент его AVP). Обнаруживает практически 100 % известных и новых вирусов. Большое количество функций, сканер, монитор, эвристика и все, что необходимо, чтобы успешно противостоять вирусам.

McAfee VirusScan (производитель «McAfee Associates»). Это один из наиболее известных антивирусных пакетов. Очень хорошо удаляет вирусы, но у VirusScan хуже, чем у других пакетов, обстоят дела с обнаружением новых разновидностей файловых вирусов. Он легко и быстро устанавливается с использованием настроек по умолчанию, но его можно настроить и по собственному усмотрению. Вы можете сканировать все файлы или только программные, распространять или не распространять процедуру сканирования на сжатые файлы. Имеет много функций для работы с сетью Интернет.

Dr. Web (производитель «Диалог Наука»). Популярный отечественный антивирус. Хорошо распознает вирусы, но в его базе их гораздо меньше, чем у других антивирусных программ.

Antiviral Toolkit Pro (производитель «Лаборатория Касперского»). Этот антивирус признан во всем мире как один из самых надежных. Несмотря на простоту в использовании он обладает всем необходимым арсеналом для борьбы с вирусами. Эвристический механизм, избыточное сканирование, сканирование архивов и упакованных файлов – это далеко не полный перечень его возможностей.

Лаборатория Касперского внимательно следит за появлением новых вирусов и своевременно выпускает обновления антивирусных баз. Имеется резидентный монитор для контроля за исполняемыми файлами.

Несмотря на широкую распространенность антивирусных программ вирусы продолжают плодиться. Чтобы справиться с ними, необходимо создавать более универсальные и качественно новые антивирусные программы, которые будут включать в себя все положительные качества своих предшественников. К сожалению, на данный момент нет такой антивирусной программы, которая гарантировала бы защиту от всех разновидностей вирусов на 100 %, но некоторые фирмы на сегодняшний день достигли неплохих результатов.

Защищенность от вирусов зависит и от грамотности пользователя. Применение вкупе всех видов защит позволит достигнуть высокой безопасности компьютера и, соответственно, информации.

6.4. Профилактика компьютерных вирусов

Одним из основных методов борьбы с вирусами является, как и в медицине, своевременная профилактика. Компьютерная профилактика предполагает соблюдение небольшого числа правил, которые позволяют значительно снизить вероятность заражения вирусом и потери каких-либо данных.

Для того, чтобы определить основные правила компьютерной гигиены, необходимо выяснить основные пути проникновения вируса в компьютер и компьютерные сети.

Откуда берутся вирусы:

- глобальные сети – электронная почта;
- электронные конференции, файл-серверы ftp и BBS;
- локальные сети;
- пиратское программное обеспечение;
- персональные компьютеры «общего пользования»;
- «случайные» пользователи компьютера.

Теперь можно определить основные правила профилактики.

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

Используйте специализированные антивирусы – для проверки всех файлов, к которым происходит обращение, файлов, приходящих по электронной почте (и по Интернету в целом).

Лучше покупать дистрибутивные копии программного обеспечения у официальных продавцов, чем бесплатно или почти бесплатно копировать их из других источников либо покупать пиратские копии. При этом вероятность заражения значительно снижается, хотя известны случаи покупки инфицированных дистрибутивов.

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

Периодически сохраняйте на внешнем носителе файлы, с которыми ведется работа. Такие резервные копии носят название backup-копий. Затраты на копирование файлов, содержащих исходные тексты программ, базы данных, документацию, значительно меньше затрат на восстановление этих файлов при проявлении вирусом агрессивных свойств или при сбое компьютера.

Пользуйтесь только хорошо зарекомендовавшими себя источниками программ и прочих файлов.

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

Пользуйтесь утилитами проверки целостности информации. Такие утилиты сохраняют в специальных базах данных информацию о системных областях дисков (или целиком системные области) и информацию о файлах (контрольные суммы, размеры, атрибуты, даты последней модификации файлов и т. д.). Периодически сравнивайте информацию, хранящуюся в подобной базе данных, с реальным содержимым винчестера, так как практически любое несоответствие может служить сигналом о появлении вируса или «троянской» программы.

Ограничивайте круг лиц, допущенных к работе на конкретном компьютере. Как правило, наиболее часто подвержены заражению «многопользовательские» персональные компьютеры.

Вопросы и задания для самоконтроля

1. В чем заключаются способы и средства обеспечения безопасности информации?

2. Чем занимаются криптография и криптоанализ?

3. Охарактеризуйте разделы современной криптографии.

4. Перечислите требования к современным криптографическим системам защиты информации.

5. Какие существуют атаки на криптосистемы?

6. Какие требования предъявляются к антивирусным программам?

7. Дайте характеристику основным видам антивирусных программ.

8. Какие антивирусные программы вам еще известны?

9. Какие существуют профилактические меры против компьютерных вирусов?

Глава 7. АРХИТЕКТУРА СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

7.1. Требования к архитектуре систем защиты информации. Построение систем защиты информации

7.2. Ядро системы защиты информации. Ресурсы системы защиты информации. Организационное построение

7.1. Требования к архитектуре систем защиты информации. Построение систем защиты информации

Система защиты информации (СЗИ) в самом общем виде может быть определена как организованная совокупность всех средств, методов и мероприятий, выделяемых (предусматриваемых) на объекте обработки информации (ООИ) для решения в ней выбранных задач защиты.

Введением понятия СЗИ определяется тот факт, что все ресурсы, выделяемые для защиты информации, должны объединяться в единую, целостную систему, которая является функционально самостоятельной подсистемой любого ООИ.

Важнейшим концептуальным требованием к СЗИ является требование адаптируемости, т. е. способности к целенаправленному приспособлению при изменении структуры, технологических схем или условий функционирования ООИ. Важность требования адаптируемости обусловливается, с одной стороны, тем, что перечисленные факторы могут существенно изменяться, а с другой – тем, что процессы защиты информации относятся к слабоструктурированным, т. е. имеющим высокий уровень неопределенности. Управление же слабоструктурированными процессами может быть эффективным лишь при условии адаптируемости системы управления.

Помимо общего концептуального требования, к СЗИ предъявляется еще целый ряд более конкретных, целевых требований, которые могут быть разделены следующим образом:

- функциональные;
- эргономические;
- экономические;
- технические;
- организационные.

Сформированная к настоящему времени система включает следующий перечень общеметодологических принципов:

- концептуальное единство;
- адекватность требованиям;
- гибкость (адаптируемость);
- функциональная самостоятельность;
- удобство использования;
- минимизация предоставляемых прав;
- полнота контроля;
- адекватность реагирования;
- экономичность.

Концептуальное единство означает, что архитектура, технология, организация и обеспечение функционирования как СЗИ в целом, так и составных компонентов должны рассматриваться и реализовываться в строгом соответствии с основными положениями единой концепции защиты информации.

Адекватность требованиям означает, что СЗИ должна строиться в строгом соответствии с требованиями к защите, которые, в свою очередь, определяются категорией соответствующего объекта и значениями параметров, влияющих на защиту информации.

Гибкость (адаптируемость) системы защиты означает такое построение и такую организацию ее функционирования, при которых функции защиты осуществлялись бы достаточно эффективно при изменении в некотором диапазоне структуры объекта обработки информации, технологических схем или условий функционирования каких-либо ее компонентов.

Функциональная самостоятельность предполагает, что СЗИ должна быть самостоятельной обеспечивающей подсистемой системы обработки информации и при осуществлении функций защиты не должна зависеть от других подсистем.

Удобство использования означает, что СЗИ не должна создавать дополнительных неудобств для пользователей и персонала объекта обработки информации.

Минимизация предоставляемых прав означает, что каждому пользователю и каждому лицу из состава персонала объекта обработки информации должны предоставляться лишь те полномочия на доступ к ресурсам объекта обработки информации и находящейся в ней информации, которые ему действительно необходимы для выполнения своих функций в про-

цессе автоматизированной обработки информации. При этом предоставляемые права должны быть определены и установленным порядком утверждены заблаговременно.

Полнота контроля предполагает, что все процедуры автоматизированной обработки защищаемой информации должны контролироваться системой защиты в полном объеме, причем основные результаты контроля должны фиксироваться в специальных регистрационных журналах.

Активность реагирования означает, что СЗИ должна реагировать на любые попытки несанкционированных действий. Характер реагирования может быть различным и включает: просьбу повторить действие; отключение структурного элемента, с которого осуществлено несанкционированное действие; исключение нарушителя из числа зарегистрированных пользователей; подачу специального сигнала и др.

Экономичность СЗИ означает, что при условии соблюдения основных требований всех предыдущих принципов расходы на СЗИ должны быть минимальными.

Функциональным построением любой системы называется организованная совокупность тех функций, для регулярного осуществления которых она создается.

Под *организационным построением* понимается общая организация системы, адекватно отражающая концептуальные подходы к ее созданию. Организационно СЗИ состоит из трех механизмов:

- обеспечения защиты информации;
- управления механизмами защиты;
- общей организации работы системы.

В механизмах обеспечения защиты выделяются два вида организационных компонентов: постоянные и переменные. При этом под постоянными понимаются такие механизмы, которые встраиваются в компоненты объекта обработки информации в процессе создания СЗИ и находятся в рабочем состоянии в течение всего времени функционирования соответствующих компонентов. Переменные же механизмы являются автономными, использование их для решения задач защиты информации предполагает предварительное осуществление операций ввода в состав используемых механизмов. Встроенные и переменные механизмы могут иметь в своем составе технические, программные и организационные средства обеспечения защиты.

Соответственно составу механизмов обеспечения защиты информации, очевидно, должны быть организованы механизмы управления ими.

Механизмы общей организации работы СЗИ предназначены для системной увязки и координации работы всех компонентов СЗИ.

В понятие «организационное построение СЗИ» входит также распределение элементов этой системы по организационно-структурным элементам ООИ. Исходя из этого, в организационном построении СЗИ должны быть предусмотрены подсистемы защиты на объектах (структурных компонентах) ООИ со своими специфическими механизмами защиты и некоторое управляющее звено, которое имеет название *ядро СЗИ*.

7.2. Ядро системы защиты информации. Ресурсы системы защиты информации. Организационное построение

Ядро системы защиты предназначено для объединения всех подсистем СЗИ в единую целостную систему, организации обеспечения управления ее функционированием.

Ядро может включать организационные и технические составляющие.

Организационная составляющая включает совокупность специально выделенных для обеспечения защиты информации сотрудников, выполняющих свои функции в соответствии с разработанными правилами, а также нормативную базу, регламентирующую выполнение этих функций.

Техническая составляющая обеспечивает техническую поддержку организационной составляющей и представляет собой совокупность технических средств отображения состояний элементов СЗИ, контроля доступа к ним, управления их включением и т. д. Чаще всего эти средства объединены в соответствующий пульт управления СЗИ.

Ядро СЗИ обладает следующими функциями.

1. Включение компонентов СЗИ в работу при поступлении запросов на обработку защищаемой информации и блокирование бесконтрольного доступа к ней:

- оборудование объекта средствами охранной сигнализации;
- организация хранения носителей защищаемой информации в отдельных хранилищах (документация, шифры, магнитные носители и т. д.);
- включение блокирующих устройств, регулирующих доступ к элементам СЗИ при предъявлении соответствующих полномочий и средств сигнализации.

2. Организация и обеспечение проверок правильности функционирования СЗИ:

• аппаратных средств – по тестовым программам и организационно;

• физических средств – организационно (плановые проверки средств охранной сигнализации, сигнализации о повышении давления в кабелях и т. д.);

• программных средств – по специальным контрольным суммам (на целостность) и по другим идентифицирующим признакам.

Ресурсы системы защиты информации

Ресурсы информационно-вычислительной системы, необходимые для создания и поддержания функционирования СЗИ, как и любой другой автоматизированной системы, объединяются в техническое, математическое, программное, информационное и лингвистическое обеспечение.

1. *Техническое обеспечение* – совокупность технических средств, необходимых для технической поддержки решения всех тех задач защиты информации, решение которых может потребоваться в процессе функционирования СЗИ.

2. *Математическое обеспечение* – совокупность математических методов, моделей и алгоритмов, необходимых для оценки уровня защищенности информации и решения других задач защиты.

3. *Программное обеспечение* – совокупность программ, реализующих программные средства защиты, а также программ, необходимых для решения задач управления механизмами защиты. К ним должны быть отнесены также сервисные и вспомогательные программы СЗИ.

4. *Информационное обеспечение* – совокупность систем классификации и кодирования данных о защите информации, массивы данных СЗИ, в также входные и выходные документы СЗИ.

5. *Лингвистическое обеспечение* – совокупность языковых средств, необходимых для обеспечения взаимодействия компонентов СЗИ между собой, с компонентами объекта обработки информации и с внешней средой.

Организационное построение

Организационное построение СЗИ в самом общем случае может быть представлено совокупностью следующих рубежей защиты:

1) территории, занимаемой ООИ;

2) зданий, расположенных на территории;

3) помещений внутри здания, в которых расположены ресурсы ООИ и защищаемая информация;

4) ресурсов, используемых для обработки и хранения информации и самой защищаемой информации;

5) линий связи, проходящих в пределах одного и того же здания;

6) линий (каналов) связи, проходящих между различными зданиями, расположенными на одной и той же охраняемой территории;

7) линий (каналов) связи, соединенных с другими объектами вне охраняемой территории.

Таким образом, можно провести организационное построение системы защиты информации с помощью приведенной семирубежной модели. В наиболее общем случае необходимо в зависимости от выбранной стратегии защиты сформулировать требования к ядру СЗИ и ресурсам СЗИ, а также использовать критерии построения СЗИ, изложенные в данной главе.

Необходимо отметить, что построение СЗИ должно проводиться в соответствии с нормативно-правовой документацией, принятой в Российской Федерации. На осуществление большинства видов деятельности в сфере защиты информации необходимы лицензии. Так, для работы с государственной тайной, для работы с криптографическими средствами требуются соответствующие лицензии Федеральной службы безопасности, технические средства должны быть аттестованы Федеральной службой по техническому и экспертному контролю.

Вопросы и задания для самоконтроля

1. Дайте определение системе защиты информации.

2. Перечислите общеметодологические принципы системы защиты информации и дайте им характеристику.

3. Что такое функциональное и организационное построение системы защиты информации?

4. Что представляют собой организационные и технические составляющие ядра системы защиты информации?

5. Какими функциями обладает ядро системы защиты информации?

Заключение

Проблема обеспечения информационной безопасности широка и многогранна. За внешней тривиальностью, заключающейся в обеспечении трех составляющих информационной безопасности (доступности, целостности и конфиденциальности информации), скрывается значительный перечень мероприятий: от общих решений, принимаемых в интересах всего общества и государства, до частных решений применительно к отдельному носителю информации.

На сегодняшний день в нашей стране в целом сформирована единая политика в сфере обеспечения информационной безопасности. Для этого принят целый ряд основополагающих законов, также разработаны ключевые оценочные стандарты средств автоматизированной обработки, хранения, отображения и обмена информацией.

Наличие проблем с обеспечением защищенности информации и поддерживающей ее инфраструктуры на сегодняшний день сдерживает развитие таких перспективных экономических направлений, как электронная коммерция, электронный бизнес, безбумажный документооборот, которые могут реально повысить эффективность функционирования целых отраслей производства и сферы сервисных услуг.

В мире все более востребованными становятся услуги специалистов, занимающихся вопросами защиты информации. На этом фоне появляются крупные компании, оказывающие подобные услуги, разрабатывающие специализированные аппаратно-программные комплексы защиты информации.

В связи с этим можно отметить, что современный человек, хоть как-то связанный с информационными технологиями и средствами автоматизации обработки информации, должен представлять основные источники и угрозы информационной безопасности, а самое главное, должен знать основные приемы безопасной работы. Именно с этой точки зрения излагался материал в данном пособии. Пользователи, у которых данный материал вызвал дополнительный интерес, могут воспользоваться литературой, приведенной в конце пособия. Наиболее актуальную информацию по проблеме обеспечения информационной безопасности можно найти в периодических изданиях, а также в глобальной сети Интернет.

Список литературы

1. *Агапов А. В.* Основы федерального информационного права России [Текст] / А. В. Агапов. М.: Экономика, 1995. 345 с.

2. *Андрианов В. И.* «Шпионские штучки» и устройства для защиты объектов и информации [Текст]: справ. пособие / В. И. Андрианов. СПб.: Лань, 1996. 289 с.

3. *Андрианов В. И.* «Шпионские штучки 2», или Как сберечь свои секреты [Текст] / В. И. Андрианов, А. В. Соколов. СПб.: Полигон, 1997. 321 с.

4. *Башлы П. Н.* Информационная безопасность [Текст] / П. Н. Башлы. Ростов н/Д: Феникс, 2006. 253 с.

5. *Белов В. В.* Интеллектуальная собственность. Законодательство и практика его применения [Текст]: учеб. пособие / В. В. Белов, Г. В. Виталиев, Г. М. Денисов. М.: Юристъ, 1997. 267 с.

6. *Бержье Ж.* Промышленный шпионаж [Текст] / Ж. Бержье. М.: Междунар. отношения, 1972. 189 с.

7. *Боттом Н. Р.* Экономическая разведка и контрразведка [Текст]: практ. пособие / Н. Р. Ботом, Р. Дж. Галлати. Новосибирск: Диамант, 1994. 226 с.

8. *Вакин С. А.* Основы радиопротиводействия и радиотехнической разведки [Текст] / С. А. Вакин, Л. Н. Шустов. М.: Сов. радио, 1968. 235 с.

9. *Владимиров В.* Секреты экономической разведки [Текст] // Бизнес и безопасность. 1995. № 1. С. 24–28.

10. *Вус М. А.* Информационно-коммерческая безопасность: Защита коммерческой тайны [Текст] / М. А. Вус, В. П. Морозов. СПб.: Дом коммерч. бумаг, 1993. 368 с.

11. *Герасименко В. А.* Защита информации в автоматизированных системах обработки данных [Текст] / В. А. Герасименко. М.: Энергоатомиздат, 1994. 486 с.

12. *Герасименко В. А.* Основы защиты информации [Текст] / В. А. Герасименко, А. А. Малюк. М.: МИФИ, 1997. 195 с.

13. *Герасименко В. А.* Основы защиты коммерческой информации и интеллектуальной собственности [Текст] / В. А. Герасименко, С. П. Гришаев, Д. В. Павлов. М.: Науч.-информ. внедрен. фирма «ЮНИС», 1991. 356 с.

14. *Гоноровский И. С.* Радиотехнические цепи и сигналы [Текст] / И. С. Гоноровский. М.: Сов. радио, 1967. 167 с.

15. *Громаков Ю. А.* Стандарты и системы подвижной радиосвязи [Текст] / Ю. А. Громаков. М.: ЭКО-ТРЕНДЗ, 1997. 254 с.

16. *Грушко А. А.* Теоретические основы защиты информации [Текст] / А. А. Грушко, Е. Е. Тимонина. М.: Яхтсмен, 1996. 362 с.

17. *Жельников В.* Криптография от папируса до компьютера [Текст] / В. Жельников. М.: АВР, 1996. 283 с.

18. *Калинцев Ю. К.* Криптозащита сообщений в системах связи [Текст] / Ю. К. Капинцев. М.: МТУСИ, 2000. 265 с.

19. *Касперский Е. В.* Компьютерные вирусы: что это такое и как с ними бороться [Текст] / Е. В. Касперский. М.: СК Пресс, 1998. 325 с.

20. *Киселев А. Е.* Коммерческая безопасность [Текст] / А. Е. Киселев, В. М. Чаплыгин, М. С. Шейкин. М.: ИнфоАрт, 1993.384 с.

21. *Киселев В. Д.* Защита информации в современных системах ее передачи и обработки [Текст] / В. Д. Киселев, О. В. Есиков, А. С. Кислицин. М.: Солид, 2002. 262 с.

22. *Куприянов А. И.* Основы защиты информации [Текст]: учеб. пособие для студентов высш. учеб. заведений / А. И. Куприянов, А. В. Сахаров, В. А. Шевцов. М.: Академия, 2006. 256 с.

23. *Куприянов А. И.* Радиоэлектронные системы в информационном конфликте [Текст] / А. И. Куприянов, А. В. Сахаров. М.: Вуз. кн., 2003. 249 с.

24. *Кураков Л. П.* Информация как объект правовой защиты [Текст] / Л. П. Кураков, С. Н. Смирнов. М.: Гелиос, 1998. 236 с.

25. *Мельников В. П.* Информационная безопасность и защита информации [Текст]: учеб. пособие для студентов высш. учеб. заведений / В. П. Мельников, С. А. Клейменов, А. М. Петраков; под ред. С. А. Клейменова. 3-е изд., стер. М.: Академия, 2006. 336 с.

26. *Меньшаков Ю. К.* Защита объектов информации от технических средств разведки [Текст] / Ю. К. Меньшаков; Рос. гос. гуманит. ун-т. М., 2002. 226 с.

27. *Организация* и современные методы защиты информации [Текст] / под общ. ред. С. И. Диева, А. Г. Шаваева. М.: Концерн «Банк. Деловой Центр», 1998. 338 с.

28. *Основы* информационной безопасности [Текст]: учеб. пособие для вузов / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. М.: Горячая линия – Телеком, 2006. 544 с.

29. *Пенин П. И.* Системы передачи цифровой информации [Текст] / П. И. Пенин. М.: Сов. радио, 1976. 188 с.

30. *Помехозащищенность* радиосистем со сложными сигналами [Текст] / под ред. Г. И. Тузова. М.: Радио и связь, 1985. 224 с.

31. *Степанов Е. А.* Конфиденциальные документы и особенности защищенного документооборота [Текст] // Классификаторы и документы. 1995. № 3–4.

32. *Степанов Е. А.* Предпосылки защиты и механизм утечки конфиденциальной информации [Текст] // Секретар. дело. 1998. № 1. С. 34–39.

33. *Торокин А. А.* Основы инженерно-технической защиты информации [Текст] / А. А. Торокин. М.: Ось-89, 1998. 384 с.

34. *Хоффман Л. Дж.* Современные методы защиты информации [Текст]: пер. с англ. / Л. Дж. Хоффман. М.: Сов. радио, 1980. 462 с.

35. *Ярочкин В. И.* Информационная безопасность [Текст]: учеб. для вузов / В. И. Ярочкин. М.: Акад. Проект, 2006. 544 с.

Учебное издание

Шайдуров Андрей Александрович

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Учебное пособие

Редактор Т. А. Кузьминых
Компьютерная верстка Н. А. Ушениной

Печатается по постановлению
редакционно-издательского совета университета

Подписано в печать 29.06.10. Формат 60×84/16. Бумага для множ. аппаратов. Усл. печ. л. 7,4. Уч.-изд. л. 8,0 Тираж 100 экз. Заказ № 1203
Издательство Российского государственного профессионально-педагогического университета. Екатеринбург, ул. Машиностроителей, 11.

Отпечатано ООО "ТРИКС"
Свердловская обл., г. Верхняя Пышма, ул. Феофанова, 4