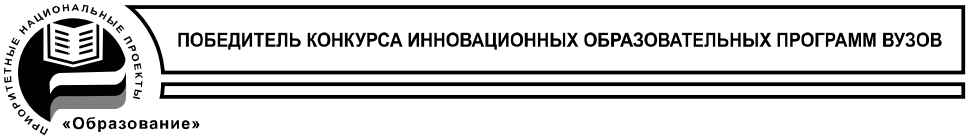
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ

САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ



Ю.А. Гатчин, Е.В. Климова

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Учебное пособие

Санкт-Петербург

2009

УДК 681.326

Гатчин Ю.А., Климова Е.В. Основы информационной безопасности: учебное пособие. – СПб: СПбГУ ИТМО, 2009. – 84 с.

Целью данного учебного пособия является ознакомление студентов с основами информационной безопасности компьютерных систем, проблемами защиты информации и подходами к их решению. В пособии рассматривается законодательная база информационной безопасности, приводится перечень возможных угроз. Отражены основные подходы к созданию систем защиты информации и представлена классификация мер по обеспечению безопасности компьютерных систем.

Пособие предназначено для студентов, специализирующихся в области информационной безопасности (специальность 090104 – Комплексная защита объектов информатизации, дисциплина «Теория информационной безопасности и методология защиты информации) и слушателей факультета повышения квалификации.

Рекомендовано к печати ученым советом факультета Компьютерных технологий и управления, 16.06.09, протокол № 11.

СПбГУ ИТМО стал победителем конкурса инновационных образовательных программ вузов России на 2007-2008 годы и успешно реализовал инновационную образовательную программу «Инновационная система подготовки специалистов нового поколения в области информационных и оптических технологий», что позволило выйти на качественно новый уровень подготовки выпускников и удовлетворять возрастающий спрос на специалистов в информационной, оптической и других высокотехнологичных отраслях науки. Реализация этой программы создала основу формирования программы дальнейшего развития вуза до 2015 года, включая внедрение современной модели образования.

ветственных задач. Кафедра стала готовить инженеров по специальности 0648. Подготовка проводилась по двум направлениям: автоматизация конструирования ЭВА и технология микроэлектронных устройств ЭВА.

Заведовали кафедрой д.т.н., проф. Новиков В В. (до 1976 г.), затем проф. Петухов Г.А.

1988 - 1997 МАП (кафедра микроэлектроники и автоматизации проектирования) Кафедра выпускала инженеров - конструкторов - технологов по микроэлектронике и автоматизации проектирования вычислительных средств (специальность 2205). Выпускники этой кафедры имеют хорошую технологическую подготовку и успешно работают как в производстве полупроводниковых интегральных микросхем, так и при их проектировании, используя современные методы автоматизации проектирования. Инженеры специальности 2205 требуются микроэлектронной промышленности и предприятиям - разработчикам вычислительных систем.

Кафедрой с 1988 г. по 1992 г. руководил проф. Арустамов С А , затем снова проф. Петухов Г.А.

С 1997 ПКС (кафедра проектирования компьютерных систем). Кафедра выпускает инженеров по специальности Проектирование и технология электронно-вычислительных средств. Область профессиональной деятельности выпускников включает в себя проектирование, конструирование и технологию электронных средств, отвечающих целям их функционирования, требованиям надежности, дизайна и условиям эксплуатации Кроме того, кафедра готовит специалистов по специальности 2206 - Организация и технология защиты информации, причем основное внимание уделяется программно-аппаратной защите информации компьютерных систем.

С 1996 г. кафедрой заведует д.т.н., профессор Гатчин Ю.А.

Юрий Арменакович Гатчин
Елена Владимировна Климова

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Учебное пособие

В авторской редакции
Дизайн Е.В. Климова
Верстка Е.В. Климова
Редакционно-издательский отдел Санкт-Петербургского государственного университета информационных технологий, механики и оптики
Зав. РИО Н.Ф. Гусарова
Лицензия ИД № 00408 от 05.11.99
Подписано к печати 17.06.09
Заказ № 2122
Тираж 100 экз.
Отпечатано на ризографе

Оглавление

Введение

На современном этапе развития общества, связанного с массовым использованием информационных технологий и созданием единого информационного пространства, в рамкам которого происходит накопление, обработка, хранение и обмен информацией, проблемы информационной безопасности приобретают первостепенное значение во всех сферах общественной и государственной деятельности. Особая острота и важность этих проблем определяется следующими факторами:

- высокими темпами роста парка средств вычислительной техники и связи, расширением областей использования ЭВМ, многообразием и повсеместным распространением информационно-управляющих систем, подлежащих защите;
- вовлечением в процесс информационного взаимодействия все большего числа людей и организаций, резким возрастанием их информационных потребностей;
- повышением уровня доверия к автоматизированным системам управления и обработки информации, использованием их в критических технологиях;
- отношением к информации, как к товару, переходом к рыночным отношениям, с присущей им конкуренцией и промышленным шпионажем, в области создания и сбыта (предоставления) информационных услуг;
- концентрацией больших объемов информации различного назначения и принадлежности на электронных носителях;
- наличием интенсивного обмена информацией между участниками этого процесса;
- количественным и качественным совершенствованием способов доступа пользователей к информационным ресурсам;
- обострением противоречий между объективно существующими потребностями общества в расширении свободного обмена информацией и чрезмерными или наоборот недостаточными ограничениями на ее распространение и использование;

- дифференциацией уровней потерь (ущерба) от уничтожения, фальсификации, разглашения или незаконного тиражирования информации (уязвимости различных затрагиваемых субъектов);
- многообразием видов угроз и возможных каналов несанкционированного доступа к информации;
- ростом числа квалифицированных пользователей вычислительной техники и возможностей по созданию ими программно-математических воздействий на систему;
- отсутствием достаточного количества квалифицированных специалистов в области защиты информации;
- развитием рыночных отношений (в области разработки, поставки, обслуживания вычислительной техники, разработки программных средств, в том числе средств защиты).

Естественно, в такой ситуации возникает потребность в защите компьютерных систем и информации от несанкционированного доступа, кражи, уничтожения и других преступных и нежелательных действий, число которых непрерывно растет. Так по оценке специалистов США, ущерб от компьютерных преступлений ежегодно составляет около 35 миллиардов долларов. В среднем ущерб от одного компьютерного преступления составляет порядка 560 тысяч долларов.

Анализ существующего положения показывает, что уровень мероприятий по защите информации, как правило, отстает от темпов автоматизации. Важнейшими аспектами при этом являются выявление, анализ и классификация возможных путей реализации угроз безопасности с целью нарушения работоспособности системы или несанкционированного доступа к информации, оценка реальности угроз безопасности и наносимого ущерба, определение основных мер противодействия угрозам безопасности, разработка критериев и механизмов безопасности, а также соответствующей нормативно-правовой базы.

Однако, необходимо отметить, что на сегодняшний день:

- не существует единой теории защищенных систем, в достаточной мере универсальной в различных предметных областях (как в государственном, так и в коммерческом секторе);
- производители средств защиты в основном предлагают отдельные компоненты для решения частных задач, оставляя решение вопросов

формирования системы защиты и совместимости этих средств своим потребителям;

- для обеспечения надежной защиты необходимо решить целый комплекс технических и организационных проблем с разработкой соответствующей документации.

В связи с этим можно выделить следующие основные принципы построения систем компьютерной безопасности, которые необходимо учитывать при их проектировании и разработке:

- системность подхода;
- комплексность решений;
- непрерывность защиты;
- разумная достаточность средств защиты;
- простота и открытость используемых механизмов защиты;
- минимум неудобств пользователям и минимум накладных расходов на функционирование механизмов защиты.

В настоящем пособии рассматриваются некоторые из основных вопросов, связанных с обеспечением информационной безопасности компьютерных систем.

1. Основные понятия, термины и определения

Широко распространенное в настоящее время понятие – информационная безопасность – подчеркивает важность информации в современном обществе и характеризует тот факт, что информационный ресурс является сегодня таким же богатством, как полезные ископаемые, производственные и людские ресурсы и также как они подлежит эащите от различного рода посягательств, злоупотреблений и преступлений.

Под *информационной безопасностью* будем понимать защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры [14].

Подход к проблемам информационной безопасности необходимо начинать с выявления субъектов, заинтересованных в обеспечении [11]:

- своевременного доступа (за приемлемое для них время) к необходимой им информации;
- конфиденциальности (сохранения в тайне) определенной части информации;
- достоверности (полноты, точности, адекватности, целостности) информации;
- защиты от навязывания им ложной (недостоверной, искаженной) информации (то есть от дезинформации);
- защиты части информации от незаконного ее тиражирования (защиты авторских прав, прав собственника информации и т.п.);
- разграничения ответственности за нарушения законных прав (интересов) других субъектов информационных отношений и установленных правил обращения с информацией;
- возможности осуществления непрерывного контроля и управления процессами обработки и передачи информации.

Очевидно, что обеспечение этих требований существенно и для государства в целом, и для отдельных общественных или коммерческих организаций, и для предприятий (юридических лиц), и для отдельных граждан (физических лиц), которые и являются субъектами информационных отношений. Поэтому введем следующие определения:

Субъект - это активный компонент информационной системы, который может стать причиной потока информации от объекта к субъекту или изменения состояния системы.

Объект - пассивный компонент системы, хранящий, принимающий или передающий информацию. Доступ к объекту означает доступ к содержащейся в нем информации.

В качестве объектов, подлежащих защите в интересах обеспечения безопасности субъектов информационных отношений, необходимо рассматривать:

- информацию и информационные ресурсы,
- носители информации,
- процессы обработки информации.

Под *информацией* обычно понимают сведения об объектах и явлениях окружающей среды, их параметрах, свойствах и состоянии, которые уменьшают имеющуюся о них степень неопределенности.

Основными потребительскими качествами информации являются: репрезентативность, содержательность, достаточность, доступность, актуальность, своевременность, точность, достоверность и устойчивость.

Информационные ресурсы определим как отдельные документы и массивы документов, представленные самостоятельно или в информационных системах (ИС) (библиотеках, архивах, фондах, базах данных, и др. ИС). Информационные ресурсы можно классифицировать:

- *по виду информации* - правовые, научно-технические, политические, финансово-экономические, статистические, метрологические, социальные, персональные, медицинские, о чрезвычайных ситуациях и т. п.;

- *по режиму доступа* – открытые, ограниченного доступа, государственная тайна, конфиденциальная информация, коммерческая тайна, профессиональная тайна, служебная тайна, личная (персональная) тайна;

- *по форме собственности* – государственные, федеральные, муниципальные, частные, коллективные;

- *по виду носителя* – на бумаге (документы, письма, медицинские карты, телефонные справочники организаций, выброшенные черновики и распечатки), на экране, в памяти ЭВМ, в канале связи, на гибких и жестких магнитных дисках и на других носителях.

Носителями информации могут являться отдельные знающие люди, которые бесспорно владеют важной информацией (эксперты), а также специально завербованные, внедренные или даже случайные информаторы – осведомители.

Осведомленность конечного пользователя о мерах безопасности должна проявляться в умении различать четыре уровня защиты компьютерных и информационных ресурсов:

- *предотвращение* – доступ к информации и технологии имеет только авторизованный персонал,

- *обнаружение* – раннее обнаружение преступлений и злоупотреблений, даже в случае обхода механизмов защиты,

- *ограничение* – уменьшение размера потерь, если преступление имело место несмотря на предпринятые меры по его предотвращению,

- *восстановление* – обеспечение эффективного восстановления информации при наличии документированных и проверенных планов проведения этой операции.

Приведем основные понятия информационной безопасности компьютерных систем [3, 11, 22]

Под *безопасностью КС* понимают ее защищенность от случайного или преднамеренного вмешательства в нормальный процесс ее функционирования, а также от попыток хищения, изменения или разрушения ее компонентов.

Природа воздействий на КС может быть самой разнообразной. Это и стихийные бедствия (землетрясения, ураганы, пожары), и выход из строя составных элементов КС, и ошибки персонала, и попытка проникновения злоумышленника.

Безопасность КС достигается принятием мер по обеспечению конфиденциальности и целостности обрабатываемой ею информации, а также доступности и целостности компонентов и ресурсов системы.

Под *доступом к информации* понимается ознакомление с информацией, ее обработка, в частности копирование, модификация или уничтожение информации.

Различают санкционированный и несанкционированный доступ к информации.

Санкционированный доступ к информации - это доступ к информации, не нарушающий установленные правила разграничения доступа.

Правила разграничения доступа служат для регламентации права доступа субъектов доступа к объектам доступа.

Несанкционированный доступ (НСД) к информации характеризуется нарушением установленных правил разграничения доступа. Лицо или процесс, осуществляющие несанкционированный доступ к информации, являются нарушителями правил разграничения доступа. Несанкционированный доступ является наиболее распространенным видом компьютерных нарушений.

Конфиденциальность данных - это статус, предоставленный данным и определяющий требуемую степень их защиты. По существу конфиденциальность информации - это свойство информации быть известной только допущенным и прошедшим проверку (авторизированным) субъектам системы

(пользователям, процессам, программам). Для остальных субъектов системы эта информация должна быть неизвестной.

Целостность информации обеспечивается в том случае, если данные в системе не отличаются в семантическом отношении от данных в исходных документах, т.е. если не произошло их случайного или преднамеренного искажения или разрушения.

Целостность компонента или ресурса системы - это свойство компонента или ресурса быть неизменными в семантическом смысле при функционировании системы в условиях случайных или преднамеренных искажений или разрушающих воздействий.

Доступность компонента или *ресурса* системы - это свойство компонента или ресурса быть доступным для авторизованных законных субъектов системы.

Под *угрозой безопасности* КС понимаются возможные воздействия на КС, которые прямо или косвенно могут нанести ущерб ее безопасности. *Ущерб безопасности* подразумевает нарушение состояния защищенности информации, содержащейся и обрабатывающейся в КС. С понятием угрозы безопасности тесно связано понятие уязвимости КС.

Уязвимость КС - это некоторое неудачное свойство системы, которое делает возможным возникновение и реализацию угрозы.

Атака на компьютерную систему - это действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости системы. Таким образом, атака - это реализация угрозы безопасности.

Противодействие угрозам безопасности является целью защиты систем обработки информации.

Безопасная или *защищенная система* - это система со средствами защиты, которые успешно и эффективно противостоят угрозам безопасности.

Комплекс средств защиты представляет собой совокупность программных и технических средств, создаваемых и поддерживаемых для обеспечения информационной безопасности КС. Комплекс создается и поддерживается в соответствии с принятой в данной организации политикой безопасности.

Политика безопасности - это совокупность норм, правил и практических рекомендаций, регламентирующих работу средств защиты КС от заданного множества угроз безопасности.

На практике важнейшими являются следующие аспекты информационной безопасности: доступность, целостность и конфиденциальность.

2. Основы государственной политики в области информационной безопасности

На официальном уровне государственная система защиты информации в России была сформирована в 1973 г. в рамках действия государственной комиссии СССР по противодействию иностранным техническим разведкам. Начиная с 1992 г., проблемы информационной безопасности в новых экономических и правовых условиях вышли из круга оборонной тематики и обусловили тем самым создание в общегосударственном масштабе более совершенной системы информационной безопасности. Создание такой системы, прежде всего, потребовало разработать необходимую нормативно-правовую базу: Концепцию национальной безопасности Российской Федерации, Доктрину информационной безопасности Российской Федерации и ряд других документов.

2.1. Стратегия национальной безопасности Российской Федерации

Указом Президента от 12 мая 2009 г. № 537 утверждена Стратегия национальной безопасности Российской Федерации (Стратегия) до 2020 года.

В связи с этим признана утратившей силу прежняя Концепция национальной безопасности Российской Федерации, утвержденная в декабре 1997 г. и модифицированная в январе 2000 г.

Стратегия национальной безопасности – это система взглядов на обеспечение в Российской Федерации безопасности личности, общества и государства от внешних и внутренних угроз в экономической, политической, социальной, международной, духовной, *информационной*, военной, оборонно-промышленной, экологической сферах, а также в сфере науки и образования.

Национальные интересы России в информационной сфере заключаются в соблюдении конституционных прав и свобод граждан в области получения информации и пользования ею, в развитии современных телекоммуникационных технологий, в защите государственных информационных ресурсов от несанкционированного доступа.

Состояние отечественной экономики, несовершенство системы организации государственной власти и гражданского общества, социально-политическая поляризация общества и криминализация общественных отношений, рост организованной преступности и увеличение масштабов терроризма,

обострение межнациональных и осложнение международных отношений создают широкий спектр внутренних и внешних угроз национальной безопасности нашей страны.

Угрозы национальной безопасности Российской Федерации в информационной сфере проявляются в стремлении ряда стран к доминированию в мировом пространстве, вытеснению с внешнего и внутреннего информационного рынка; в разработке рядом государств концепции информационных войн, предусматривающей создание средств опасного воздействия на информационные сферы других стран мира; в нарушении нормального функционирования информационных и телекоммуникационных систем, а также сохранности информационных ресурсов путем получения несанкционированного доступа к ним.

В ходе реализации настоящей Стратегии угрозы информационной безопасности предотвращаются за счет совершенствования безопасности функционирования информационных и телекоммуникационных систем критически важных объектов инфраструктуры и объектов повышенной опасности в Российской Федерации, повышения уровня защищенности корпоративных и индивидуальных информационных систем, создания единой системы информационно-телекоммуникационной поддержки нужд системы обеспечения национальной безопасности.

Важнейшими задачами в области обеспечения информационной безопасности Российской Федерации являются:

- 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 этого России потребуется:

- преодолеть технологическое отставание в важнейших областях информатизации, телекоммуникаций и связи, определяющих состояние национальной безопасности;

- разработать и внедрить технологии информационной безопасности в системах государственного и военного управления, системах управления экологически опасными производствами и критически важными объектами;

- обеспечить условия для гармонизации национальной информационной инфраструктуры с глобальными информационными сетями и системами.

Реализация Стратегии национальной безопасности Российской Федерации до 2020 года призвана стать мобилизующим фактором развития национальной экономики, улучшения качества жизни населения, обеспечения политической стабильности в обществе, укрепления национальной обороны, государственной безопасности и правопорядка, повышения конкурентоспособности и международного престижа РФ.

2.2. Доктрина информационной безопасности Российской Федерации

Доктрина информационной безопасности РФ (Доктрина) утверждена Указом № 1895 Президента РФ от 9 сентября 2000 г. Доктрина представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности и служит основой для:

- формирования государственной политики в области обеспечения информационной безопасности Российской Федерации;
- подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности Российской Федерации;
- разработки целевых программ обеспечения информационной безопасности Российской Федерации.

1. Информационная безопасность РФ (виды и источники угроз ИБ РФ, состояние ИБ РФ и основные задачи по ее обеспечению);
2. Методы обеспечения ИБ РФ (особенности обеспечения ИБ РФ в различных сферах общественной жизни, международное сотрудничество в области обеспечения ИБ);
3. Основные положения государственной политики обеспечения ИБ РФ (первоочередные мероприятия по реализации государственной политики безопасности в РФ);
4. Организационная основа обеспечения ИБ РФ (основные функции систем обеспечения ИБ РФ, основные элементы организационной основы систем обеспечения ИБ РФ).

2.3. Закон «О государственной тайне»

В основу законов, позволяющих отнести информацию к тому или иному разряду тайн, положены принципы информационного суверенитета и международные правила. Регулирование отношений, возникающих в связи с отнесени-

ем сведений к государственной тайне, их засекречиванием и рассекречиванием в интересах обеспечения безопасности Российской Федерации, осуществляется в соответствии с законом «О государственной тайне» [19].

2.3.1. Основные понятия

Государственная тайна – защищаемые государственные сведения в области военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которой 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 отражение в виде символов, образов, сигналов, технических решений и процессов.

Гриф секретности – реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него.

Степень секретности – категория, характеризующая важность такой информации, возможный ущерб в случае ее разглашения, степень ограничения доступа к ней и уровень ее охраны государством.

2.3.2. Перечень сведений, составляющих государственную тайну

Государственную тайну составляют:

1. Сведения в военной области:

- о содержании стратегических и оперативных планов и о других документах боевого управления; о подготовке и проведении военных операций, стратегическом и мобилизационном развертывании войск и об их важнейших показателях, характеризующих организацию, численность, дислокацию, боевую и мобилизационную готовность, боевую и другую военную подготовку, вооружение и материально-техническое обеспечение Вооруженных Сил, Пограничных войск и прочих воинских формирований;

- о направлении развития отдельных видов вооружения и военной техники, их количестве, тактико-технических характеристиках, организации и технологии производства, научно-исследовательских и опытно-конструкторских работах, связанных с разработкой новых образцов вооружения и военной техни-

ки, модернизации существующих образцов, а также о других работах, планируемых или осуществляемых в интересах страны;

- о силах и средствах Гражданской обороны, о готовности населенных пунктов, регионов и отдельных объектов к защите, эвакуации и рассредоточению населения, к обеспечению его жизнедеятельности и производственной деятельности объектов народного хозяйства в военное время или в условиях других чрезвычайных ситуаций;

- о геодезических, гравиметрических, картографических, гидрографических и гидрометеорологических данных и характеристиках, имеющих значение для обороны страны.

2. Сведения в области экономики, науки и техники:

- о мобилизационных планах и мощностях народного хозяйства, запасах и объемах поставок стратегических видов сырья и материалов, а также о размещении и объемах государственных мобилизационных материальных резервов;

- об использовании транспорта, связи, других отраслей и объектов инфраструктуры страны в интересах обеспечения ее безопасности;

- о содержании, объеме, финансировании и выполнении государственного оборонного заказа;

- о планах, объемах и других важнейших характеристиках добычи, производства и реализации отдельных стратегических видов сырья и продукции;

- о государственных запасах драгоценных металлов монетарной группы, драгоценных камней, валюты и других ценностей, об операциях, связанных с изготовлением денежных знаков и ценных бумаг, их хранением, охраной и защитой от подделки, обращением, обменом или изъятием, а также о других особых мерах финансовой деятельности государства.

3. Сведения в сфере внешних отношений:

- о директивах, планах, указаниях делегациям и должностным лицам по вопросам внешнеполитической и внешнеэкономической деятельности;

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

- о военном, научно-техническом и ином сотрудничестве с разными странами, если разглашение сведений об этом может нанести ущерб интересам государства;

- об экспорте и импорте вооружения, военной техники, отдельных стратегических видов сырья и продукции.

4. сведения в области государственной безопасности и охраны правопорядка:

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

- о лицах, которые сотрудничают или раньше сотрудничали на конфиденциальной основе с органами. Осуществляющими такую деятельность;

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

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

- о методах и средствах защиты секретной информации;

- об организации и о фактическом состоянии защиты государственной тайны;

- о защите Государственной границы Российской Федерации;

- о расходах федерального бюджета, связанных с обеспечением обороны, безопасности государства и правительственной деятельности в Российской Федерации;

- о разработке и использовании шифров, работе с ними, проведении научно-исследовательских работ в области криптографии;

- о подготовке кадров, раскрывающие мероприятия, проводимые в целях обеспечения безопасности государства.

Сведения могут быть отнесены к государственной тайне лишь при условии, что их разглашение будет наносить ущерб жизненно важным интересам государства. Запрещается отнесение к государственной тайне каких-либо сведений, нарушающих конституционные права человека и гражданина или наносящих вред здоровью и безопасности населения.

2.3.3. Сведения, не подлежащие отнесению к государственной тайне и засекречиванию

Не подлежит отнесению к государственной тайне и засекречиванию информация:

- о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях;

- о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;

- о привилегиях, компенсациях и льготах, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям;

- о фактах нарушения прав и свобод человека и гражданина;

- о размерах золотого запаса и государственных валютных резервах;

- о состоянии здоровья высших должностных лиц Российской Федерации;

- о фактах нарушения законности органами государственной власти и их должностными лицами.

Должностные лица, принявшие решение о засекречивании перечисленных сведений либо о включении их в этих целях в носители сведений, составляющих государственную тайну, несут уголовную, административную или дисциплинарную ответственность в зависимости от причиненного обществу, государству и гражданам материального и морального ущерба. Граждане вправе обжаловать такие решения в суд.

2.3.4. Принципы засекречивания сведений и отнесения их к государственной тайне

Отнесение сведений к государственной тайне и их засекречивание осуществляется в соответствии с принципами законности, обоснованности и своевременности.

Законность – это соответствие относимых к государственной тайне и засекречиваемых сведений положениям Закона и законодательству Российской Федерации о государственной тайне.

Обоснованность – Установление путем экспертных оценок целесообразности отнесения к государственной тайне и засекречивания конкретных сведений, вероятных экономических и иных последствий этого акта, исходя из баланса жизненно важных интересов государства, общества и граждан.

Своевременность – заключается в установлении ограничений на распространение засекречиваемых сведений с момента их получения (разработки) или заблаговременно.

2.3.5. Степени секретности сведений и грифы секретности носителей этих сведений

Степень секретности сведений, составляющих государственную тайну, должна соответствовать степени тяжести ущерба, который может быть нанесен безопасности Российской Федерации вследствие их распространения.

Устанавливаются три степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведений: «особой важности» - высший гриф секретности, «совершенно секретно» и «секретно».

Порядок определения размеров ущерба, который может быть нанесен безопасности Российской Федерации вследствие распространения сведений, составляющих государственную тайну, и правила отнесения указанных сведений к той или иной степени секретности устанавливаются Правительством Российской Федерации.

Использование перечисленных грифов секретности для засекречивания сведений, не отнесенных к государственной тайне, не допускается.

2.3.6. Порядок отнесения сведений к государственной тайне

Отнесение сведений к государственной тайне осуществляется мотивированным решением государственного эксперта по вопросам тайн. В его решении указывается: информация, представляющая государственную тайну, основания отнесения сведений к государственной тайне и, в случае ее разглашения, обоснование ущерба жизненно важным интересам государства, степень секретности, срок действия решения об отнесении сведений к государственной тайне и др.

Отнесение сведений к государственной тайне осуществляется в соответствии с Перечнем сведений, составляющих государственную тайну. В этом Перечне указываются органы государственной власти, наделяемые полномочиями по распоряжению данными сведениями. Перечень утверждается Президентом Российской Федерации, подлежит открытому опубликованию и пересматрива-

ется по мере необходимости. Органы государственной власти в соответствии с их отраслевой, ведомственной или программно-целевой принадлежностью могут создавать развернутые перечни сведений, представляющих государственную тайну. Эти перечни утверждаются соответствующими руководителями органов государственной власти. Целесообразность засекречивания таких перечней определяется их содержанием.

Информация считается государственной тайной со времени ее включения в Перечень сведений, составляющих государственную тайну.

Снижение степени секретности информации и отмена решения об отнесении ее к государственной тайне осуществляются на основании заключения государственного эксперта по вопросам тайн или, без такового заключения в связи с истечением сроков действия решений об отнесении информации к государственной тайне.

Засекречивание информации, отнесение ее к государственной тайне, осуществляется путем предоставления соответствующему документу, изделию или другому материальному носителю информации грифа секретности.

Гриф секретности является обязательным реквизитом каждого носителя информации, отнесенной к государственной тайне. Он должен содержать сведения о степени секретности данной информации, сроке засекречивания и должностном лице, предоставившем гриф.

Перечень должностных лиц, имеющих право предоставлять носителям информации гриф секретности, утверждается руководителем предприятия, учреждения или организации, осуществляющими деятельность, связанную с государственной тайной.

2.3.7. Порядок засекречивания сведений и их носителей

Основанием для засекречивания сведений, полученных (разработанных) в результате управленческой, производственной, научной и иных видов деятельности органов государственной власти, предприятий, учреждений и организаций, является их соответствие действующим в данных органах, на данных предприятиях, в данных учреждениях и организациях перечням сведений, подлежащих засекречиванию. При засекречивании этих сведений их носителям присваивается гриф секретности.

При невозможности идентификации полученных (разработанных) сведений со сведениями, содержащимися в действующем перечне, должностные ли-

ца органов государственной власти, предприятий, учреждений и организаций обязаны обеспечить предварительное засекречивание полученных (разработанных) сведений в соответствии с предполагаемой степенью секретности и в месячный срок направлять в адрес должностного лица, утвердившего указанный перечень, предложения по его дополнению (изменению).

Должностные лица, утвердившие действующий перечень, обязаны в течение трех месяцев организовать экспертную оценку поступивших предложений и принять решение по дополнению (изменению) действующего перечня или снятию предварительно присвоенного сведениям грифа секретности.

2.3.8. Реквизиты носителей сведений, составляющих государственную тайну

На носители сведений, составляющих государственную тайну, наносятся реквизиты, включающие следующие данные:

- о степени секретности содержащихся в носителе сведений со ссылкой на соответствующий пункт действующего в данном органе государственной власти, на данном предприятии, в данных учреждениях и организациях перечня сведений, подлежащих засекречиванию;
- об органе государственной власти, о предприятии, об учреждении, организации, осуществляющих засекречивание носителя;
- о регистрации носителя;
- о дате или условии рассекречивания сведений либо о событии, после наступления которого сведения будут рассекречены.

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

Если носитель содержит составные части с различными степенями секретности, каждой их них присваивается соответствующий гриф секретности, а носителю в целом присваивается гриф секретности, соответствующий тому грифу секретности, который присваивается его составной части, имеющей высшую для данного носителя степень секретности сведений.

2.3.9. Порядок рассекречивания сведений и их носителей

Рассекречивание сведений и их носителей – снятие ранее введенных в предусмотренном порядке ограничение на распространение сведений, составляющих государственную тайну, и на доступ к их носителям.

Основанием для рассекречивания требований являются:

- принятие на себя Российской Федерацией международных обязательств по открытому обмену сведениями, составляющими государственную тайну;

- изменение объективных обстоятельств, вследствие которого дальнейшая защита сведений, составляющих государственную тайну, является нецелесообразной.

Органы государственной власти, имеющие полномочия по отнесению сведений к государственной тайне, обязаны периодически, но не реже чем через каждые 5 лет, пересматривать содержание действующих в органах государственной власти, на предприятиях, в учреждениях и организациях перечней сведений, подлежащих засекречиванию, в части обоснованности их засекречивания и соответствия установленной ранее степени секретности.

Срок засекречивания сведений, составляющих государственную тайну, не должен превышать 30 лет. В исключительных случаях это срок может быть продлен по заключению межведомственной комиссии по защите государственной тайны.

Правом изменения действующих в органах государственной власти, на предприятиях, в учреждениях и организациях перечней сведений, подлежащих засекречиванию, наделяются утвердившие их руководители органов государственной власти, которые несут персональную ответственность за обоснованность принятых ими решений по рассекречиванию сведений. Решения указанных руководителей, связанные с изменением перечня сведений, отнесенных к государственной тайне, подлежат согласованию с межведомственной комиссией по защите государственной тайны, которая вправе приостанавливать и опротестовывать эти решения.

2.3.10. Допуск к государственной тайне

Понятия допуска и доступа к сведениям, составляющим государственную тайну, являются взаимосвязанными, но не тождественными (допуск всегда должен предшествовать доступу, который определяется как санкционированное

полномочными должностными лицами ознакомление конкретного лица со сведениями, составляющих государственную тайну). На практике право доступа может быть не реализовано после оформления допуска, например, в случае смены работы или отсутствия необходимости в ознакомлении с соответствующей информацией.

В соответствии с рассмотренными выше тремя степенями секретности и соответствующими им грифами секретности устанавливаются следующие формы допуска:

первая форма (ф. 1) – для граждан, допускаемых к сведениям особой важности;

вторая форма (ф. 2) – для граждан, допускаемых к совершенно секретным сведениям;

третья форма (ф. 3) – для граждан, допускаемых к секретным сведениям.

Первая форма допуска дает право на ознакомление со сведениями, составляющими государственную тайну, всех трех степеней секретности. Вторая форма допуска дает право на ознакомление со сведениями, имеющими степени секретности «совершенно секретно» и «секретно». Третья форма допуска дает право на ознакомление со сведениями, имеющими степень секретности «секретно».

В соответствии и Законом Российской Федерации «о государственной тайне» допуск должностных лиц и граждан Российской Федерации к государственной тайне осуществляется в добровольном порядке. Оформление допуска гражданину предусматривает:

- принятие им на себя обязательств перед государством по нераспространению доверенных сведений, составляющих государственную тайну;

- его согласие на частичные временные ограничения прав, связанные с проведением в отношении него проверочных мероприятий;

- письменное согласие на проведение полномочными органами проверочных мероприятий;

- ознакомление с нормами законодательства Российской Федерации о государственной тайне, предусматривающими ответственность за его нарушение;

- принятие соответствующего решения руководителем организации о допуске оформляемого лица к государственной тайне;

- определение видов, размеров и порядка предоставления льгот, предусмотренных Законом.

Таким образом, оформление допуска является осознанным и добровольным сообщением о себе гражданином установленного законом минимума информации о себе, проверка достоверности этих сведений органами государственной власти (федеральной службой безопасности – ФСБ), принятие полномочным должностным лицом (руководителем предприятия, организации, учреждения) решения о допуске и заключение с гражданином соответствующего договора с взаимными обязательствами

Решение об отказе должностному лицу или гражданину в допуске к государственной тайне принимается руководителем органа государственной власти предприятия, учреждения или организации.

Допуск лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов к государственной тайне осуществляется в порядке, установленном постановлением Правительства Российской Федерации от 22 августа 1998 года № 1003.

2.3.11. Уголовно-правовая защита информации, составляющей государственную тайну

За посягательство на государственную тайну предусмотрена уголовная ответственность независимо от того, к какой области (военной, экономической, научно- технической, внешнеполитической, внешнеэкономической, разведывательной, контрразведывательной или оперативно-розыскной деятельности) и к какой степени секретности (особой важности, совершенно секретным или секретным) относятся сведения, составляющие государственную тайну. Область государственной деятельности и степень секретности учитываются при назначении наказания за соответствующее посягательство. При назначении наказания учитываются также последствия, к которым привело конкретное посягательство на государственную тайну.

УК РФ от 13.06.1996 № 63-ФЗ предусматривает уголовную ответственность за следующие *восемь видов посягательств на государственную тайну:*

- шпионаж (ст. ст. 275, 276 УК РФ);
- выдача государственной тайны иностранному государству, иностранной организации или их представителям (ст. 275 УК РФ);
- иное оказание помощи иностранному государству, иностранной организации или их представителям (ст. 275 УК РФ);
- разглашение государственной тайны (ст. 283 УК РФ);

- утрата документов, содержащих гостайну, или предметов, сведения о которых составляют гостайну (ст. 284 УК РФ);

- уничтожение, блокирование, модификация или копирование охраняемой законом компьютерной информации (в том числе содержащей государственную тайну) в результате неправомерного доступа к ней (ст. 272 УК РФ) или нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274 УК РФ);

- поставление охраняемой законом компьютерной информации (в том числе содержащей государственную тайну) в заведомую опасность несанкционированного уничтожения, блокирования или копирования в результате создания или распространения вредоносных программ для ЭВМ (ст. 283 УК РФ);

- похищение, уничтожение, повреждение или сокрытие официальных документов (в том числе содержащих государственную тайну) (ст. 325, часть 1 УК РФ).

Рассмотрим непосредственное содержание указанных выше статей.

Статья 275. Государственная измена

Государственная измена, т. е. шпионаж, выдача государственной тайны либо иное оказание помощи иностранному государству, иностранной организации или их представителям в проведении враждебной деятельности в ущерб внешней безопасности РФ, совершенная гражданином РФ, - наказывается лишением свободы на срок от двенадцати до двадцати лет с конфискацией имущества или без таковой.

Примечание. Лицо, совершившее преступления, предусмотренные настоящей статьей, а также ст. 276 , освобождается от уголовной ответственности, если оно добровольным и своевременным сообщением органам власти или иным образом способствовало предотвращению дальнейшего интересам РФ и если в его действиях не содержится иного состава преступления.

Статья 276. Шпионаж

Передача, а равно собирание, похищение или хранение в целях передачи иностранному государству, иностранной организации или их представителям сведений, составляющих государственную тайну, а также передача или собирание по заданию иностранной разведки иных сведений для использования их в ущерб внешней безопасности РФ, если эти деяния совершены иностранным гражданином или лицом без гражданства, - наказывается лишением свободы на срок от десяти до двадцати лет.

Статья 283. Разглашение государственной тайны

1. Разглашение сведений, составляющих государственную тайну, лицом, которому она была доверена или стала известна по службе или работе, если эти сведения стали достоянием других лиц, при отсутствии признаков государственной измены – наказывается арестом на срок от четырех до шести месяцев, либо лишением свободы на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

2. То же деяние, повлекшее по неосторожности тяжкие последствия, - наказывается лишением свободы на срок от трех до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

Статья 284. Утрата документов, содержащих государственную тайну

Нарушение лицом, имеющим допуск к государственной тайне, установленных правил обращения с содержащими государственную тайну документами, а равно с предметами, сведения о которых составляют государственную тайну, если это повлекло по неосторожности их утрату и наступление тяжких последствий, - наказывается ограничением свободы на срок до трех лет, либо арестом на срок от четырех до шести месяцев, либо лишением свободы на срок до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

Кроме вышеперечисленных статей, в УК РФ включен еще ряд норм, направленных на защиту охраняемой законом информации. При этом под охраняемой законом информацией понимаются различные сведения, в число которых наряду с другими данными (содержащими личную, семейную, коммерческую, банковскую, служебную, профессиональную и другую тайну) входит и информация, составляющая государственную тайну. К эти нормам относятся следующие статьи.

Статья 272. Неправомерный доступ к компьютерной информации

1. Неправомерный доступ к охраняемой законом компьютерной информации, т. е. информации на машинном носителе, в ЭВМ, системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, - наказывается штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев, либо исправительными работами

на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой, либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, - наказывается штрафом в размере от пятисот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от пяти до восьми месяцев, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок до шести месяцев, либо лишением свободы на срок до пяти лет.

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

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами - наказывается лишением свободы на срок от двух до трех лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или заработной платы или иного дохода осужденного за период от двух до пяти месяцев.

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

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

1. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, - наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет.

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

Статья 325. Похищение или повреждение документов, штампов, печатей

Похищение, уничтожение, повреждение или сокрытие официальных документов, штампов или печатей, совершенные из корыстной или личной заинтересованности, - 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 до двух лет, либо арестом на срок до четырех месяцев, либо лишением свободы на срок до одного года.

2.4. Закон «О коммерческой тайне»

16 августа 2004 года вступил в действие Федеральный закон «О коммерческой тайне» [20], позволяющий упорядочить установление, функционирование и прекращение отношений, связанных с коммерческой тайной.

Закон регулирует отношения, связанные с отнесением информации к коммерческой тайне, передачей такой информации, охраной ее конфиденциальности в целях обеспечения баланса интересов обладателей информации, составляющей коммерческую тайну, и других участников регулируемых отношений (в том числе государства, на рынке товаров, работ, услуг и предупреждения недобросовестной конкуренции). Закон также определяет сведения, которые не могут составлять коммерческую тайну.

2.4.1. Основные понятия

Коммерческая тайна - конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Информация, составляющая коммерческую тайну, - научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в том числе составляющая секреты производства «ноу-хау»), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам. К такой информации нет свободного доступа на законном основании и в отношении нее обладателем информации введен режим коммерческой тайны.

Режим коммерческой тайны - правовые, организационные, технические и иные принимаемые обладателем информации, составляющей коммерческую тайну, меры по охране ее конфиденциальности.

Обладатель информации, составляющей коммерческую тайну, - лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании, ограничило доступ к этой информации и установило в отношении ее режим коммерческой тайны.

Доступ к информации, составляющей коммерческую тайну, - ознакомление определенных лиц с информацией, составляющей коммерческую тайну, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации.

Передача информации, составляющей коммерческую тайну, - передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем контрагенту на основании договора в объеме и на условиях, которые предусмотрены договором, включая условие о принятии контрагентом установленных договором мер по охране ее конфиденциальности.

Контрагент - сторона гражданско-правового договора, которой обладатель информации, составляющей коммерческую тайну, передал эту информацию.

Предоставление информации, составляющей коммерческую тайну, - передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем органам государственной власти, иным государственным органам, органам местного самоуправления в целях выполнения их функций.

Разглашение информации, составляющей коммерческую тайну, - действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.

2.4.2. Порядок отнесения информации к коммерческой тайне и способы ее получения

1. Право на отнесение информации к информации, составляющей коммерческую тайну, и на определение перечня и состава такой информации принадлежит обладателю информации с учетом положений данного Закона.

2. Информация, самостоятельно полученная лицом при осуществлении исследований, систематических наблюдений или иной деятельности, считается

полученной законным способом, даже если эта информация составляет коммерческую тайну и ей обладает другое лицо.

3. Информация, составляющая коммерческую тайну, считается полученной законно, если она получена от ее обладателя на основании договора.

4. Признаки информации, полученной незаконно:

полученная информация составляет коммерческую тайну и получатель умышленно преодолевал меры по ее охране;

получатель информации знал, что получает информацию от лица, не имеющего право на ее передачу получателю.

2.4.3. Сведения, которые не могут составлять коммерческую тайну

Режим коммерческой тайны не может быть установлен лицами, осуществляющими предпринимательскую деятельность, в отношении следующих сведений:

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

2) содержащихся в документах, дающих право на осуществление предпринимательской деятельности;

3) о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов;

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

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

6) о задолженности работодателей по выплате заработной платы и по иным социальным выплатам;

7) о нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений;

8) об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности;

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

10) о перечне лиц, имеющих право действовать без доверенности от имени юридического лица;

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

2.4.4. Права обладателя информации, составляющей коммерческую тайну

Права обладателя информации, составляющей коммерческую тайну, возникают с момента установления им в отношении такой информации режима коммерческой тайны. Обладатель имеет следующие права:

1) устанавливать, изменять и отменять режим коммерческой тайны;

2) использовать информацию, составляющую коммерческую тайну, для собственных нужд;

3) разрешать или запрещать доступ к информации, составляющей коммерческую тайну, определять порядок и условия доступа к этой информации;

4) вводить в гражданский оборот информацию, составляющую коммерческую тайну, на основании договоров, предусматривающих включение в них условий об охране конфиденциальности этой информации;

5) требовать от юридических и физических лиц, получивших доступ к информации, составляющей коммерческую тайну, органов государственной власти, органов местного самоуправления, которым предоставлена такая информация, соблюдения обязанностей по охране ее конфиденциальности;

6) требовать от лиц, получивших доступ к информации, составляющей коммерческую тайну, в результате действий, осуществленных случайно или по ошибке, охраны конфиденциальности этой информации;

7) защищать в установленном законом порядке свои права в случае разглашения, незаконного получения или незаконного использования третьими лицами информации, составляющей коммерческую тайну, в том числе требовать возмещения убытков, причиненных в связи с нарушением его прав.

2.4.5. Охрана коммерческой тайны

Общими мерами обеспечения соблюдения конфиденциальности информации являются следующие:

разработка перечня информации, относящейся к коммерческой тайне;

ограничение и регламентирование доступа к носителям информации;

определение круга лиц, имеющих права доступа к информации;

разработка и закрепление правил по регулированию отношений по использованию информации, составляющей коммерческую тайну, в системе трудовых договоров, договоров с контрагентами;

нанесение на документы, договора, составляющие коммерческую тайну надписи «конфиденциальная информация», при этом необходимо указывать обладателя информации (место нахождения, наименование).

После принятия вышеуказанных мер режим коммерческой тайны считается установленным.

2.4.6. Ответственность за нарушение требований Федерального закона «О коммерческой тайне»

Нарушение требований закона влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с действующим законодательством.

Статья 13.14 Кодекса об административных правонарушениях

Разглашение информации, доступ к которой ограничен ФЗ (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, влечет наложение административного штрафа.

Статья 183 УК РФ «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну»

1. Собирание сведений, составляющих коммерческую, налоговую или банковскую тайну, путем похищения документов, подкупа или угроз, а равно иным незаконным способом наказывается штрафом в размере до 80 тысяч рублей или в размере заработной платы или иного дохода осужденного за период от 1 до 6 месяцев либо лишением свободы на срок до 2-х лет.

2. Незаконные разглашение или использование сведений, составляющих коммерческую, налоговую или банковскую тайну, без согласия их владельца лицом, которому она была доверена или стала известна по службе или работе, наказываются штрафом в размере до 120 тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет либо лишением свободы на срок до 3 лет.

3. Те же деяния, причинившие крупный ущерб или совершенные из корыстной заинтересованности, наказываются штрафом в размере до 200 тысяч рублей или в размере заработной платы или иного дохода осужденного за период до 18 месяцев с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет либо лишением свободы на срок до 5 лет.

4. Деяния, предусмотренные частями 2-й или 3-ей статьи 183, повлекшие тяжкие последствия, наказываются лишением свободы на срок до 10 лет.

2.5. Закон «О персональных данных»

В январе 2007г. вступил в силу Федеральный закон от 27.07.06 № 152-ФЗ «О персональных данных» [21]. Он регулирует отношения по обработке информации, относящейся к физическим лицам (субъектам персональных данных), в государственных и муниципальных органах юридическими и физическими лицами (операторами).

В соответствии с Законом:

персональные данные (ПД) - любая информация о физическом лице (фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы и другая информация);

оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку ПД, а также определяющие цели и содержание обработки ПД;

обработка персональных данных - действия (операции) с ПД, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение ПД.

Обработка ПД может осуществляться оператором с согласия субъектов ПД с условием обеспечения их конфиденциальности.

В следующих случаях *не требуется* согласия субъекта ПД:

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

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

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

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

5) обработка ПД необходима для доставки почтовых отправлений организациями почтовой связи, для осуществления операторами электросвязи расчетов с пользователями услуг связи за оказанные услуги связи, а также для рассмотрения претензий пользователей услугами связи;

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

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

Согласие субъекта на обработку его персональных данных

На обработку своих ПД субъект должен дать согласие, причем он имеет право его отозвать в любой момент. Согласие может быть выражено в устной или письменной форме – в зависимости от категории ПД, а также характера их обработки.

Согласие субъекта ПД в письменной форме требуется в следующих случаях:

– при обработке специальных категорий ПД, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни. Обрабатывать такие сведения без письменного согласия субъекта категорически запрещено (за ис-

ключением случаев, когда они являются общедоступными). Письменное согласие на подобные действия необходимо, даже если субъекта ПД и оператора связывают договорные отношения. В общественных объединениях или религиозных организациях обработка специальных категорий ПД членов (участников) осуществляется при условии, что ПД не будут распространяться без согласия субъектов, данного в письменной форме;

– при обработке биометрических ПД – сведений, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность (сведения об особенностях строения папиллярных узоров пальцев рук человека, сетчатки глаз, о коде ДНК и т. д.). Это требование также должно соблюдаться даться независимо от наличия договорных отношений между субъектом ПД и оператором, кроме отношений, связанных с прохождением государственной гражданской службы;

– при передаче ПД субъекта оператором через Государственную границу РФ органу власти иностранного государства, физическому или юридическому лицу иностранного государства, не обеспечивающему адекватную защиту прав субъекта ПД.

В соответствии с Законом письменное согласие субъекта на обработку его персональных данных должно включать:

– фамилию, имя, отчество, адрес субъекта ПД, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

– наименование (фамилия, имя, отчество) и адрес оператора, получающего согласие субъекта ПД;

– цель обработки ПД;

– перечень ПД, на обработку которых дается согласие субъекта ПД;

– перечень действий с ПД, на совершение которых дается согласие, общее описание используемых оператором способов обработки ПД;

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

Независимо от того, в письменной или устной форме получено согласие субъекта на обработку его ПД, на оператора возлагается обязанность по доказыванию факта получения такого согласия.

Права субъекта персональных данных

Оператор обязан предоставить субъекту ПД доступ к его данным в любой момент по его просьбе. У субъекта есть право на получение следующей информации:

1) подтверждение факта обработки ПД оператором, а также цель такой обработки;

2) способы обработки ПД, применяемые оператором;

3) сведения о лицах, которые имеют доступ к ПД или которым может быть предоставлен такой доступ;

4) перечень обрабатываемых ПД и источник их получения;

5) сроки обработки ПД, в т. ч. сроки их хранения;

6) сведения о том, какие юридические последствия для субъекта ПД может повлечь за собой обработка его данных.

Если оператор осуществляет обработку ПД с нарушением требований закона, субъект вправе обжаловать его действия в Федеральную службу по надзору в сфере связи, которая является уполномоченным органом по защите прав субъектов персональных данных, или в суд.

Хранение ПД может реализовываться оператором как на материальных носителях, так и путем включения данных сведений в информационные системы ПД. Оператор при обработке подобной информации обязан принимать необходимые организационные и технические меры, в частности использовать шифровальные (криптографические) средства, для защиты ПД от неправомерного или случайного доступа к ним, от уничтожения, изменения, блокирования, копирования, распространения и т. д.

Для хранения работодателем данных о лицах, с которыми его не связывают договорные отношения, *обязательно* получение согласия на их обработку.

Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту ПД работника, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

3. Основные угрозы безопасности

Под *угрозой безопасности* понимаются потенциально возможные воздействия, события, процессы или явления, которые прямо или косвенно могут нанести ущерб интересам субъектов информационных отношений.

Ущерб безопасности подразумевает нарушение состояния защищенности информации, содержащейся и обрабатывающейся в компьютерной системе (КС). С понятием угрозы безопасности тесно связано понятие уязвимости КС.

Уязвимость КС - это некоторое наиболее ранимое свойство системы, которое делает возможным возникновение и реализацию угрозы.

Атака на компьютерную систему - это действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости системы. Таким образом, атака - это реализация угрозы безопасности.

Основная *цель защиты* КС - противодействие угрозам безопасности.

По цели воздействия различают следующие основные *типы угроз безопасности*:

- нарушение конфиденциальности (раскрытие) информации;
- нарушение целостности информации (ее полное или частичное уничтожение, искажение, фальсификация, дезинформация);
- нарушение (частичное или полное) работоспособности системы. Вывод из строя или неправомерное изменение режимов работы компонентов системы обработки информации, их модификация или подмена могут приводить к получению неверных результатов расчетов, отказам системы от потока информации (непризнанию одной из взаимодействующих сторон факта передачи или приема сообщений) и/или отказам в обслуживании конечных пользователей;
- несанкционированное тиражирование открытой информации (не являющейся конфиденциальной), например, программ, баз данных, разного рода документации, литературных произведений и т.д. в нарушение прав собственников информации, авторских прав и т.п. Информация, обладая свойствами материальных объектов, имеет такую особенность, как неисчерпаемость ресурса, что существенно затрудняет контроль за ее тиражированием.

Основными ***видами угроз безопасности*** КС и информации (угроз интересам субъектов информационных отношений) являются:

- стихийные бедствия и аварии (наводнение, ураган, землетрясение, пожар и т. п.);

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

Естественные угрозы - это угрозы, вызванные воздействиями на КС и ее элементы объективных физических процессов или стихийных природных явлений, независящих от человека.

Искусственные угрозы - это угрозы КС, вызванные деятельностью человека. Среди искусственных угроз, исходя из мотивации действий, можно выделить:

- ***непреднамеренные (неумышленные, случайные) угрозы***, вызванные ошибками в проектировании КС и ее элементов, ошибками в программном обеспечении, ошибками в действиях персонала и т.п.;
- ***преднамеренные (умышленные) угрозы***, связанные с корыстными устремлениями людей (злоумышленников).

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

3.1. Основные непреднамеренные искусственные угрозы

Основные непреднамеренные искусственные угрозы КС (действия, совершаемые людьми случайно, по незнанию, невнимательности или халатности, из любопытства, но без злого умысла) [11]:

1) неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы (неумышленная порча оборудования, удаление, искажение файлов с важной информацией или программ, в том числе системных и т.п.);

2) неправомерное отключение оборудования или изменение режимов работы устройств и программ;

3) неумышленная порча носителей информации;

4) запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или осуществляющих необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т.п.);

5) нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);

6) заражение компьютера вирусами;

7) неосторожные действия, приводящие к разглашению конфиденциальной информации, или делающие ее общедоступной;

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

9) проектирование архитектуры системы, технологии обработки данных, разработка прикладных программ, с возможностями, представляющими опасность для работоспособности системы и безопасности информации;

10) игнорирование организационных ограничений (установленных правил) при работе в системе;

11) вход в систему в обход средств защиты (загрузка посторонней операционной системы со сменных магнитных носителей и т.п.);

12) некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности;

13) пересылка данных по ошибочному адресу абонента (устройства);

14) ввод ошибочных данных;

15) неумышленное повреждение каналов связи.

3.2. Основные преднамеренные искусственные угрозы

Основные возможные пути умышленной дезорганизации работы, вывода системы из строя, проникновения в систему и несанкционированного доступа к информации:

1) физическое разрушение системы (путем взрыва, поджога и т.п.) или вывод из строя всех или отдельных наиболее важных компонентов компьютерной системы (устройств, носителей важной системной информации, лиц из числа персонала и т.п.);

2) отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т.п.);

3) действия по дезорганизации функционирования системы (изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных радиопомех на частотах работы устройств системы и т.п.);

4) внедрение агентов в число персонала системы (в том числе, возможно, и в административную группу, отвечающую за безопасность);

5) вербовка (путем подкупа, шантажа и т.п.) персонала или отдельных пользователей, имеющих определенные полномочия;

6) применение подслушивающих устройств, дистанционная фото- и видеосъемка и т.п.;

7) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи, а также наводок активных излучений на вспомогательные технические средства, непосредственно не участвующие в обработке информации (телефонные линии, сети питания, отопления и т.п.);

8) перехват данных, передаваемых по каналам связи, и их анализ с целью выяснения протоколов обмена, правил вхождения в связь и авторизации пользователя и последующих попыток их имитации для проникновения в систему;

9) хищение носителей информации (магнитных дисков, лент, микросхем памяти, запоминающих устройств и целых ПЭВМ);

10) несанкционированное копирование носителей информации;

11) хищение производственных отходов (распечаток, записей, списанных носителей информации и т.п.);

12) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;

13) чтение информации из областей оперативной памяти, используемых операционной системой (в том числе подсистемой защиты) или другими пользователями, в асинхронном режиме используя недостатки мультизадачных операционных систем и систем программирования;

14) незаконное получение паролей и других реквизитов разграничения доступа (агентурным путем, используя халатность пользователей, путем подбора, путем имитации интерфейса системы и т.д.) с последующей маскировкой под зарегистрированного пользователя ("маскарад");

15) несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики, такие как номер рабочей станции в сети, физический адрес, адрес в системе связи, аппаратный блок кодирования и т.п.;

16) вскрытие шифров криптозащиты информации;

17) внедрение аппаратных спецвложений, программных "закладок" и "вирусов" ("троянских коней" и "жучков"), то есть таких участков программ, которые не нужны для осуществления заявленных функций, но позволяющих преодолевать систему защиты, скрытно и незаконно осуществлять доступ к системным ресурсам с целью регистрации и передачи критической информации или дезорганизации функционирования системы;

18) незаконное подключение к линиям связи с целью работы "между строк", с использованием пауз в действиях законного пользователя от его имени с последующим вводом ложных сообщений или модификацией передаваемых сообщений;

19) незаконное подключение к линиям связи с целью прямой подмены законного пользователя путем его физического отключения после входа в систему и успешной аутентификации с последующим вводом дезинформации и навязыванием ложных сообщений.

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

3.3. Классификация угроз безопасности

Выше мы рассмотрели два основных класса потенциальных угроз по природе их возникновения: естественные и искусственные. Но наряду с этим угрозы можно классифицировать и по различным аспектам реализации, наиболее полно изложенным в [12, 13], и показывающим возможный спектр угроз безопасности КС.

Классификация угроз по цели:

- несанкционированное чтение информации,
- несанкционированное изменение информации,
- несанкционированное уничтожение информации,

полное или частичное разрушение КС (от кратковременного вывода из строя отдельных модулей до физического стирания системных файлов);

Классификация угроз по принципу воздействия на КС:

- использование легальных каналов получения информации (например, несанкционированное чтение из файла),
- использование скрытых каналов получения информации (например, недокументированных возможностей ОС),
- создание новых каналов получения информации (например, с помощью программных закладок).

Классификация угроз по характеру воздействия на КС:

- активное воздействие – несанкционированные действия в системе,
- пассивное воздействие – несанкционированное наблюдение за процессами в системе.

Классификация угроз по типу используемой слабости защиты:

- неадекватная политика безопасности (в том числе ошибки администратора),
- ошибки и недокументированные возможности ПО (так называемые «люки» - встроенные в систему специальные входы, предназначенные для тестирования или отладки, но случайно оставленные, что позволяет обходить систему защиты),
- ранее внедренные программные закладки.

Классификация угроз по способу воздействия на объект атаки:

- непосредственное превышение пользователем своих полномочий,
- работа от имени другого пользователя или перехват результатов его работы.

Классификация угроз по способу действий нарушителя (злоумышленника):

- в интерактивном режиме (вручную),
- в пакетном режиме (с помощью специальных программ, без участия пользователя).

Классификация угроз по используемым средствам атаки:

- штатные средства без использования дополнительного ПО,

- ПО третьих фирм (вирусы, вредоносные программы; ПО, разработанное для других целей – отладчики, сетевые мониторы и т. д.).

Классификация угроз по объекту атаки:

- аппаратные средства (оборудование),
- программное обеспечение,
- данные,
- персонал.

Возможные пути реализации угроз безопасности для перечисленных объектов атаки представлены в таблице 1 [9]:

Таблица 1. Пути реализации угроз безопасности

Объекты воздействия	Нарушение конфиденциальности информации	Нарушение целостности информации	Нарушение работоспособности системы
Аппаратные средства	НСД - подключение; использование ресурсов; хищение носителей	НСД - подключение; использование ресурсов; модификация, изменение режимов	НСД - изменение режимов; вывод из строя: разрушение
ПО	НСД - копирование; хищение; перехват	НСД, внедрение "троянского коня", "вирусов", "червей"	НСД – искажение; удаление: подмена
Данные	НСД - копирование; хищение; перехват	НСД - искажение; модификация	НСД - искажение; удаление; подмена
Персонал	Разглашение; передача сведений о защите; халатность	"Маскарад": вербовка; подкуп персонала	Уход с рабочего места: физическое устранение

3.4. Описание модели гипотетического нарушителя

Важной составляющей успешного проведения анализа риска и определения требований к составу и характеристикам системы защиты информации является подготовка гипотетической модели потенциального нарушителя. При этом необходимо учитывать, что [14]:

• квалификация нарушителя может быть на уровне разработчика данной системы;

• нарушителем может быть как постороннее лицо, так и законный пользователь системы;

• нарушителю известна информация о принципах работы системы;

• нарушитель выберет наиболее слабое звено в защите.

Кроме того, при разработке модели нарушителя необходимо:

1) определить, к какой категории лиц он может принадлежать:

- из числа внутренних субъектов – непосредственный персонал системы,

- из числа внешних (посторонних) лиц – клиенты, посетители, представители систем жизнеобеспечения, конкуренты, наемники, случайные люди;

2) выявить цели и мотивы действий нарушителя (безответственность, самоутверждение, корыстный интерес);

3) учесть возможные ограничения на действия нарушителя.

Всех нарушителей можно классифицировать следующим образом.

По уровню знаний о КС:

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

По уровню возможностей (используемым методам и средствам):

- применяющий чисто агентурные методы получения сведений;
- применяющий пассивные средства (технические средства перехвата без модификации компонентов системы);
- использующий только штатные средства и недостатки систем защиты для ее преодоления (несанкционированные действия с использованием раз-

решенных средств), а также компактные магнитные носители информации, которые могут быть скрытно пронесены через посты охраны;

- применяющий методы и средства активного воздействия (модификация и подключение дополнительных технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ).

По времени действия:

- в процессе функционирования КС (во время работы системы);
- в период неактивности компонентов системы (в нерабочее время, во время плановых перерывов в ее работе, перерывов для обслуживания и ремонта и т.п.);
- как в процессе функционирования КС, так и в период неактивности компонентов системы.

По месту действия:

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

Могут учитываться следующие ограничения и предположения о характере действий возможных нарушителей:

- работа по подбору кадров и специальные мероприятия затрудняют возможность создания коалиций нарушителей, т.е. объединения (сговора) и целенаправленных действий по преодолению подсистемы защиты двух и более нарушителей;
- нарушитель, планируя попытки НСД, скрывает свои несанкционированные действия от других сотрудников;
- НСД может быть следствием ошибок пользователей, администраторов, эксплуатирующего и обслуживающего персонала, а также недостатков принятой технологии обработки информации и т.д.

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

4. Классификация мер обеспечения безопасности компьютерных систем

Среди мер обеспечения информационной безопасности КС обычно выделяют следующие: нормативно-правовые (законодательные), морально-этические, административные, физические, программно-аппаратные [6].

4.1. Нормативно-правовые меры

К *нормативно-правовым* мерам защиты относятся действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию информации и являющиеся сдерживающим фактором для потенциальных нарушителей.

Нормативно-правовые меры направлены на решение следующих вопросов [11]:

- отнесение информации к категориям открытого и ограниченного доступа;
- определение полномочий по доступу к информации;
- права должностных лиц на установление и изменение полномочий;
- способы и процедуры доступа;
- порядок контроля, документирования и анализа действий персонала;
- ответственность за нарушение установленных требований и правил;
- проблема доказательства вины нарушителя;
- соответствующие карательные санкции.

На созданную в 1992 г. Гостехкомиссию России по защите информации были возложены обязанности по координации, организационно-методическому руководству, разработке и финансированию научно-технических программ, лицензированию деятельности предприятий и сертификации продукции.

В настоящее время защита секретной информации в автоматизированных системах осуществляется Федеральной службой по техническому и экспортному контролю (ФСТЭК), созданной по Указу Президента РФ от 09.03.2004 г. № 314 «О системе и структуре федеральных органов исполнительной власти».

В состав государственной системы ЗИ входят системы лицензирования деятельности предприятий по оказанию услуг в области защиты информации и сертификации продукции по требованиям безопасности информации.

Система лицензирования направлена на создание условий, при которых право заниматься работами по защите информации предоставляется только организациям, имеющим соответствующее разрешение (лицензию) на этот вид деятельности. А система сертификации технических и программных средств по требованиям безопасности информации направлена на защиту потребителя продукции и услуг от недобросовестной работы исполнителя. К сожалению, в этих вопросах Россия значительно отстала от развитых зарубежных стран.

Важным организационным документом системы защиты информации (СЗИ) является «Положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД в АС и СВТ». Этим документом установлен единый в стране порядок исследований, разработок, введения в действие и эксплуатации защищенных от НСД средств автоматизации.

Исходя из практических потребностей, в Положении определены различные варианты разработки защищенных средств ВТ, среди которых предусматривается:

- разработка защищенного общепрограммного обеспечения (ОПО) – ОС, СУБД, сетевого ПО;

- разработка защищенных программных средств (ПС) на базе ОПО, находящегося в эксплуатации и поставляемого вместе с незащищенными СВТ;

- разработка защищенных ПС на базе импортных программных прототипов.

В Положении изложен также порядок разработки, внедрения и эксплуатации средств криптозащиты информации.

Кроме перечисленных правовых и нормативных подзаконных актов государственной СЗИ, для нормальной деятельности в области безопасности информации необходим пакет нормативных документов технического характера – стандартов, руководящих документов, инструкций.

В США с 1984 г. сертификация СВТ по требованиям ЗИ от НСД осуществляется в соответствии с «Оранжевой книгой» - государственного стандарта «Критерии оценки надежных компьютерных систем» (Trusted Computer Systems Evaluation Criteria, TCSEC). В Европе в 1991 г. принят собственный стандарт «Критерии оценки безопасности информационных технологий – гармонизированные критерии Франции, Германии, Голландии и Великобритании», построенный на аналогичных принципах.

Отечественным аналогом «Оранжевой книги» является разработанный в 1992 г. РД «СВТ. Защита от НСД информации. Показатели защищенности от НСД к информации» [5].

Этот документ устанавливает классификацию СВТ по уровню защищенности от НСД к информации на базе перечня показателей защищенности и совокупности описывающих их требований. Он может использоваться как методический материал при разработке СЗИ, или как нормативно-методический материал при их сертификации .

Кроме того, в настоящее время в законодательной сфере РФ создана правовая основа для регулирования сбора, хранения и использования информации. В УК РФ включена отдельная глава, посвященная компьютерным преступлениям. Защита интеллектуальной собственности отражена в уголовном и гражданском кодексах.

С начала 1990-х годов действует Закон РФ «О правовой охране программ для ЭВМ и баз данных», федеральный закон «Об информации, информатизации и ЗИ», Закон РФ «Об авторском праве и смежных правах» и ряд других нормативных актов.

Важнейшие законодательные нормативно-правовые документы разработаны с учетом следующих видов тайн:

- *государственная тайна* – Закон о государственной тайне, ст. 275, 276, 283, 284 УК РФ;

- *служебная и коммерческая тайна* – ст. 139 и 727 ГК РФ, ст. 155 и 183 УК РФ;

- *банковская тайна* – ст. 25 Закона о банках и банковской деятельности в РСФСР, ст. 857 ГК, ст. 183 УК РФ;

- *личная и семейная тайна* – ст. 150 ГК, ст. 137 УК РФ;

- *тайна переписки и телефонных переговоров* – ст. 138 УК РФ;

- *тайна голосования* - ст. 142 УК РФ.

Все перечисленные выше руководящие документы не исчерпывают потребностей, возникающих в ходе практических работ в области защиты информации. Это лишь необходимая основа организационной, нормативно-технической и методической документации, без которой невозможно нормальное существование и развитие информатики, и обеспечение безопасности информационных ресурсов самих СВТ.

4.2. Морально-этические меры

К *морально-этическим* мерам противодействия угрозам безопасности относятся всевозможные нормы поведения, которые традиционно сложились или складываются в обществе по мере распространения компьютеров в стране. Эти нормы большей частью не являются обязательными, как законодательно утвержденные, но их несоблюдение обычно ведет к падению престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписаными (например, общепризнанные нормы честности, патриотизма и т.д.), так и оформленными в некий свод (кодекс) правил или предписаний. Например, "Кодекс профессионального поведения членов Ассоциации пользователей ЭВМ США" рассматривает как неэтичные действия, которые умышленно или неумышленно:

• нарушают нормальную работу компьютерных систем;

• вызывают неоправданные затраты ресурсов (машинного времени, памяти, каналов связи и т.п.);

• нарушают целостность информации (хранимой и обрабатываемой);

• нарушают интересы других законных пользователей и т.п.

Социально-психологическое обеспечение ЗИ во многом зависит также от своевременной проверки благонадежности, от расстановки работников в соответствии с их способностями и личными качествами, формирования у каждого члена коллектива осознанного понимания важности и необходимости соблюдения требований режима конфиденциальности. Идеальным считается работник, обладающий такими личными качествами, как честность, принципиальность (строгое следование основным правилам), исполнительность, дисциплинированность, эмоциональная устойчивость (самообладание), стремление к успеху и порядку в работе, самоконтроль в поступках и действиях, правильная оценка собственных возможностей и способностей, умеренная склонность к риску, осторожность, умение хранить секреты, тренированное внимание, неплохая память.

Меньше всего утечек информации наблюдается в Японии, что связано с системой «пожизненного найма», и воспитанием чувств преданности и патернализма, когда работники одной организации считают себя членами единой, большой семьи.

В целом, нормативно-правовая база и моральные устои современного общества оказались не готовы к столь быстрому скачку в развитии информационных технологий, что проявилось прежде всего при интеграции России в единое информационное пространство Европы и мира с использованием сетей типа Интернет. В настоящее время отсутствуют способы и средства контроля ценности информационных ресурсов, транслируемых через границы (происходит утечка технологий и «ноу-хау»).

Для отработки механизма взаимодействия в информационном пространстве необходимо разработать законы, регулирующие отношения в этой области.

4.3. Административные меры

Административные меры защиты - это меры организационного характера. Они регламентируют:

- процессы функционирования системы обработки данных,
- использование ее ресурсов,
- деятельность персонала,
- порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности.

Административные меры включают:

- мероприятия, осуществляемые при проектировании, строительстве и оборудовании вычислительных центров и других объектов систем обработки данных;
- мероприятия по разработке правил доступа пользователей к ресурсам системы (разработка политики безопасности);
- мероприятия, осуществляемые при подборе и подготовке персонала системы;
- организацию охраны и надежного пропускного режима;
- организацию учета, хранения, использования и уничтожения документов и носителей с информацией;
- распределение реквизитов разграничения доступа (паролей, ключей шифрования и т.п.);
- организацию явного и скрытого контроля за работой пользователей;
- мероприятия, осуществляемые при проектировании, разработке, ремонте и модификациях оборудования и программного обеспечения и т.п.

Административные меры являются той основой, которая объединяет различные меры защиты в единую систему.

Выполнение различных мероприятий по созданию и поддержанию работоспособности системы защиты должно быть возложено на специальную службу - службу компьютерной безопасности.

Обязанности должностных лиц должны быть определены таким образом, чтобы при эффективной реализации ими своих функций, обеспечивалось разделение их полномочий и ответственности.

4.4. Физические меры

Физические меры защиты основаны на применении разного рода механических, электро- или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

4.5. Технические (программно-аппаратные) меры

Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ, которые самостоятельно или в комплексе с другими средствами, реализуют следующие способы защиты:

- идентификацию (распознавание) и аутентификацию (проверку подлинности) субъектов (пользователей, процессов),
- разграничение доступа к ресурсам,
- регистрацию и анализ событий,
- криптографическое закрытие информации,
- резервирование ресурсов и компонентов систем обработки информации и др.

Взаимосвязь перечисленных мер обеспечения безопасности можно пояснить следующим образом:

1. Организационные меры обеспечивают исполнение существующих нормативных актов и строятся с учетом существующих правил поведения, принятых в стране и/или организации.

2. Воплощение организационных мер требует создания нормативных документов.

3. Для эффективного применения организационные меры должны быть поддержаны физическими и техническими средствами.

4. Применение и использование технических средств защиты требует соответствующей организационной поддержки.

Программные меры защиты основаны на использовании антивирусных средств.

На сегодняшний день известно огромное количество антивирусных программ, разработанных различными отечественными и зарубежными антивирусными лабораториями. К наиболее популярным антивирусным средствам относятся:

Антивирус Касперского 6.0 имеет четыре компонента защиты: 1. файловый антивирус, обеспечивающий безопасность файлов; 2. почтовый антивирус; 3. веб-антивирус, контролирую-

щий серфинг в Интернете; 4. проактивная защита – контроль работы макросов и блокировка опасных макрокоманд.

В версии 7.0 представлена новая концепция тройной защиты: проверка баз по сигнатурам, проактивный и эвристический механизмы.

Антивирус компании ESET – **NOD32** уже в течение 7 лет признается лучшим средством защиты от новых вирусов и атак благодаря мощному эвристическому анализатору. Основные преимущества: высокий уровень защиты, низкая ресурсоемкость, высокая скорость работы.

Российская компания «Доктор Веб» является поставщиком антивирусных продуктов **Doctor Web**, эвристический анализатор которого в сочетании с ежедневно обновляющимися вирусными базами обеспечивает защиту от вирусов и макровирусов, «троянских программ», почтового червя и других видов вредоносного программного кода.

Одним из известных иностранных антивирусов в России является **Norton Antivirus** компании Symantec. Он успешно борется с вирусами, троянскими компонентами и интернет-червями. Кроме Norton Antivirus компания разработала и другие средства для защиты от угроз, распространяемых через Интернет.

Panda Antivirus 2007. Большинство защитных продуктов полагаются на часто обновляемые локальные базы знаний. Технология Panda работает по другому принципу - большинство сигнатур злонамеренных кодов находятся в удаленной базе данных, которая обновляется в режиме реального времени. Новый антиспам Panda также полагается на механизм коллективного разума, в котором есть необходимые дефиниции для сортировки писем.

В этой версии есть также система эвристического сканирования, предотвращающая хищение персональных данных. Этот механизм особенно эффективен в борьбе с банковскими троянами.

5. Критерии оценки надежных компьютерных систем

В Оранжевой книге [18] надежная система определяется как система, использующая достаточные аппаратные и программные средства для обеспече-

ния одновременной обработки информации разной степени секретности группой пользователей без нарушения прав доступа.

Для характеристики надежности или безопасности системы используют два критерия: 1) политика безопасности и 2) гарантированность.

Политика безопасности – набор законов, правил и норм поведения, регламентирующих процессы обработки, защиты и распространения информации. Политика безопасности - это *активный компонент защиты*, включающий в себя анализ возможных угроз и выбор мер противодействия. В зависимости от сформулированной политики можно выбирать конкретные механизмы, обеспечивающие безопасность системы. Чем надежнее система, тем строже и многообразнее должна быть политика безопасности.

Гарантированность – это мера доверия, которая может быть оказана архитектуре и реализации системы. Гарантированность может проистекать как из тестирования, так и из проверки (формальной или нет) общего замысла и исполнения системы в целом и ее компонентов. Гарантированность показывает, насколько корректны механизмы, отвечающие за проведение в жизнь политики безопасности. Гарантированность можно считать *пассивным компонентом защиты*.

5.1. Основные элементы политики безопасности

Согласно Оранжевой книге, политика безопасности должна включать в себя по крайней мере следующие элементы:

- произвольное управление доступом;
- безопасность повторного использования объектов;
- метки безопасности;
- принудительное управление доступом.

Рассмотрим перечисленные элементы более подробно.

Произвольное управление доступом - это метод ограничения доступа к объектам, основанный на учете личности субъекта или группы, в которую входит субъект. Произвольность управления состоит в том, что некоторое лицо (обычно владелец объекта) может по своему усмотрению давать другим субъектам или отбирать у них права доступа к объекту.

С концептуальной точки зрения текущее состояние прав доступа при произвольном управлении описывается *матрицей доступа*, в строках которой

перечислены субъекты, а в столбцах - объекты. В ячейках, расположенных на пересечении строк и столбцов, записываются способы доступа, допустимые для данного субъекта по отношению к объекту - например: чтение, запись, выполнение, возможность передачи прав другим субъектам и т. п.

Очевидно, что прямолинейное представление подобной матрицы вследствие ее больших размеров невозможно, да и не нужно, так как она разрежена, то есть большинство клеток в ней пусты. В операционных системах более компактное представление матрицы доступа основывается или на структурировании совокупности субъектов (владелец/группа/прочие как в ОС UNIX), или на механизме списков управления доступом, когда матрица представляется по столбцам и для каждого объекта перечисляются субъекты вместе с их правами доступа. За счет использования метасимволов можно компактно описывать группы субъектов, удерживая тем самым размеры списков управления доступом в разумных пределах.

Большинство операционных систем и СУБД реализуют именно произвольное управление доступом. Главное его *достоинство* - гибкость, главные *недостатки* - рассредоточенность управления и сложность централизованного контроля, а также оторванность прав доступа от данных, что позволяет копировать секретную информацию в общедоступные файлы.

Безопасность повторного использования объектов - важное на практике дополнение средств управления доступом, предохраняющее от случайного или преднамеренного извлечения секретной информации из "мусора". Безопасность повторного использования должна гарантироваться для областей оперативной памяти (в частности, для буферов с образами экрана, расшифрованными паролями и т.п.), для дисковых блоков и магнитных носителей в целом.

Современные интеллектуальные периферийные устройства усложняют обеспечение безопасности повторного использования объектов.Например, принтер может буферизовать несколько страниц документа, которые останутся в памяти даже после окончания печати. Необходимо предпринять специальные меры, чтобы "вытолкнуть" их оттуда. Иногда организации защищаются от повторного использования слишком ревностно - путем уничтожения магнитных носителей. На практике заведомо достаточно троекратной записи случайных последовательностей бит.

Метки безопасности. Для реализации принудительного управления доступом с субъектами и объектами ассоциируются *метки безопасности*. *Метка*

субъекта описывает его благонадежность, *метка объекта* - степень закрытости содержащейся в нем информации.

Согласно "Оранжевой книге", метки безопасности состоят из двух частей - *уровня секретности* и *списка категорий*. Наиболее употребительными являются следующие уровни секретности, поддерживаемые системой:

- совершенно секретно;
- секретно;
- конфиденциально;
- несекретно.

Категории образуют неупорядоченный набор. Их назначение - описать предметную область, к которой относятся данные. В военном окружении каждая категория может соответствовать, например, определенному виду вооружений. Механизм категорий позволяет разделить информацию по отсекам, что способствует лучшей защищенности. Необходимо отметить, что субъект не может получить доступ к "чужим" категориям, даже если его уровень благонадежности "совершенно секретно". Специалист по танкам не узнает тактико-технические данные самолетов.

Главная проблема, которую необходимо решать в связи с метками, - это обеспечение их *целостности*.

Во-первых, не должно быть непомеченных субъектов и объектов, иначе в меточной безопасности появятся легко используемые бреши.

Во-вторых, при любых операциях с данными метки должны оставаться правильными. В особенности это относится к экспорту и импорту данных. Например, печатный документ должен открываться заголовком, содержащим текстовое и/или графическое представление метки безопасности. Аналогично при передаче файла по каналу связи должна передаваться и ассоциированная с ним метка, причем в таком виде, чтобы удаленная система могла ее разобрать, несмотря на возможные различия в уровнях секретности и наборе категорий.

Одним из средств обеспечения целостности меток безопасности является разделение устройств на *многоуровневые* и *одноуровневые*. На многоуровневых устройствах может храниться информация разного уровня секретности (точнее, лежащая в определенном диапазоне уровней). Одноуровневое устройство можно рассматривать как вырожденный случай многоуровневого, когда допустимый диапазон состоит из одного уровня. Зная уровень устройства, система может решить, допустимо ли записывать на него информацию с определенной

меткой. Например, попытка напечатать совершенно секретную информацию на принтере общего пользования с уровнем "несекретно" потерпит неудачу.

Принудительное управление доступом основано на сопоставлении меток безопасности субъекта и объекта.

Субъект может читать информацию из объекта, если уровень секретности субъекта не ниже, чем у объекта, а все категории, перечисленные в метке безопасности объекта, присутствуют в метке субъекта. В таком случае говорят, что метка субъекта *доминирует* над меткой объекта, то есть - читать можно только то, что положено.

Субъект может записывать информацию в объект, если метка безопасности объекта доминирует над меткой субъекта. В частности, "конфиденциальный" субъект может писать в секретные файлы, но не может - в несекретные (разумеется, должны также выполняться ограничения на набор категорий). Такое ограничение может показаться странным, но оно вполне разумно. Ни при каких операциях уровень секретности информации не должен понижаться, хотя обратный процесс вполне возможен. Посторонний человек может случайно узнать секретные сведения и сообщить их куда следует, однако лицо, допущенное к работе с секретными документами, не имеет права раскрывать их содержание всем подряд.

Описанный способ управления доступом называется принудительным, так как он не зависит от воли субъектов, на месте которых могут оказаться даже системные администраторы. После того, как зафиксированы метки безопасности субъектов и объектов, оказываются зафиксированными и права доступа. В терминах принудительного управления нельзя выразить предложение "разрешить доступ к объекту X еще и для пользователя Y". Конечно, можно изменить метку безопасности пользователя Y, но тогда он, скорее всего, получит доступ ко многим дополнительным объектам, а не только к X.

Принудительное управление доступом реализовано во многих вариантах операционных систем и СУБД, отличающихся повышенными мерами безопасности. В частности, такие варианты существуют для Sun OS и СУБД Ingres.

Независимо от практического использования принципы принудительного управления являются удобным методологическим базисом для начальной классификации информации и распределения прав доступа. Удобнее мыслить в терминах уровней секретности и категорий, чем заполнять неструктурированную матрицу доступа. Впрочем, в реальной жизни произвольное и принуди-

тельное управление доступом сочетается в рамках одной системы, что позволяет использовать сильные стороны обоих подходов.

5.2. Механизмы безопасности

Наряду с *произвольным* и *принудительным* доступом могут использоваться следующие механизмы безопасности.

Шифрование (криптозащита). Шифрование подразделяется на симметричное с секретным ключом, когда знание ключа шифрования влечет знание ключа расшифровки, и асимметричное с открытым ключом, когда знание ключа шифрования не позволяет узнать ключ расшифровки. Различают также обратимое и необратимое шифрование. Последнее может использоваться для вычисления криптографических контрольных сумм (хэш-функций, дайджестов, имитовставок).

Электронная подпись. Механизм электронной подписи включает в себя две процедуры:

- выработку подписи;
- проверку подписанной порции данных.

Процедура выработки подписи использует информацию, известную только лицу, визирующему порцию данных. Процедура проверки подписи является общедоступной, она не должна позволять найти секретный ключ подписывающего.

Механизмы контроля целостности данных. Процедура контроля целостности обычно состоит в формировании различного рода контрольных сумм, которые позволяют обнаружить модификацию информации.

Механизмы аутентификации. Аутентификация может достигаться за счет использования паролей, личных карточек или иных устройств аналогичного назначения, криптографических методов - когда демонстрируется знание секретного ключа, устройств измерения и анализа биометрических характеристик (сканирование радужной оболочки глаза или отпечатков пальцев) или их комбинация. Аутентификация бывает односторонней, когда клиент обычно доказывает свою подлинность серверу, и двусторонней, или взаимной. Пример односторонней аутентификации - процедура входа пользователя в систему.

5.3. Классы безопасности

В Оранжевой книге определяется четыре *уровня безопасности* (надежности) - D, C, B и A. Уровень D предназначен для систем, признанных неудовлетворительными. По мере перехода от уровня C к A к надежности систем предъявляются все более жесткие требования. Уровни C и B подразделяются на *классы* (C1, C2, B1, B2, B3) с постепенным возрастанием надежности. Таким образом, всего имеется шесть классов безопасности - C1, C2, B1, B2, B3, A1. При переходе к каждому следующему классу требования только добавляются.

Повышение требований к классам безопасности можно проследить по таблице 2.

Кратко опишем то новое, что появляется в каждом классе.

Уровень D. На уровне D к системе не предъявляется специальных требований и может не проводиться сертификация. Таким образом, уровень D - системы, не соответствующие более высоким классам защиты, или незащищенные. К таким системам относится, например, MS DOS.

Уровень C. ***Произвольное управление доступом.*** Надежная вычислительная система должна управлять доступом именованных пользователей к именованным объектам. Механизм управления (права для владельца/группы/прочих, списки управления доступом) должен позволять специфицировать разделение файлов между индивидами и/или группами.

Идентификация и аутентификация. Пользователи должны идентифицировать себя, прежде чем выполнять какие-либо иные действия, контролируемые надежной вычислительной системы. Для аутентификации должен использоваться какой-либо защитный механизм, например пароли. Аутентификационная информация должна быть защищена от несанкционированного доступа.

Операционная гарантированность. Надежная вычислительная система должна поддерживать область для собственного выполнения, защищенную от внешних воздействий, в частности от изменения команд и/или данных, и от по

пыток слежения за ходом работы. Ресурсы, контролируемые системой, могут составлять определенное подмножество всех субъектов и объектов системы.

Целостность системы. Должны быть в наличии аппаратные и/или программные средства, позволяющие периодически проверять корректность функционирования аппаратных и микропрограммных компонентов надежной вычислительной системы.

Таблица 2. Требования, предъявляемые к различным классам безопасности

Критерии		**Классы безопасности**					
		C1	**C2**	**B1**	**B2**	**B3**	**A1**
Требования к политике безопасности	*Добровольное управление доступом*	<	<			<	
	Повторное использование объектов		<				
	Метки безопасности			<	<		
	Целостность меток безопасности			<	<		
	Принудительное управление доступом			<	<		
Требования к подотчетности	*Идентификация и аутентификация*	<	<	<			
	Предоставление надежного пути				<	<	
	Аудит		<	<	<	<	
Требования к гарантированности	*Операционная гарантированность*	<	<	<	<	<	
	Целостность системы	<					
	Анализ тайных каналов				<	<	<
	Надежное администрирование				<	<	
	Надежное восстановление					<	
	Технологическая гарантированность	<	<	<	<	<	<
	Верификация спецификаций архитектуры			<	<	<	<
	Конфигурационное управление				<		<
	Надежное распространение						<
Требования к документации	*Руководство пользователя по безопасности*	<					
	Руководство администратора по безопасности	<	<	<	<	<	
	Тестовая документация	<			<		<
	Описание архитектуры	<		<	<	<	<

Технологическая гарантированность. Защитные механизмы должны быть протестированы на предмет соответствия их поведения системной документации. Тестирование должно подтвердить, что у неавторизованного пользователя нет очевидных способов обойти или разрушить средства защиты надежной вычислительной системы.

Руководство пользователя по безопасности. Отдельный фрагмент документации (глава, том) должен описывать защитные механизмы, предостав-

ляемые надежной вычислительной системой, и их взаимодействие между собой, содержать рекомендации по их использованию.

Руководство администратора по безопасности. Руководство должно содержать сведения о функциях и привилегиях, которыми управляет системный администратор посредством механизмов безопасности.

Тестовая документация. Разработчик системы должен представить экспертному совету документ, содержащий план тестов, процедуры их прогона и результаты тестирования.

Описание архитектуры. Должны быть описаны подход к безопасности, используемый производителем, и применение этого подхода при реализации надежной вычислительной системы. Если база состоит из нескольких модулей, должен быть описан интерфейс между ними.

Класс С2. ***Повторное использование объектов.*** При выделении хранимого объекта из пула ресурсов надежной вычислительной системы необходимо ликвидировать все следы предыдущих использований.

Аудит. Надежная вычислительная система должна создавать, поддерживать и защищать журнал регистрационной информации, относящейся к доступу к объектам, контролируемым системой. Должна быть возможность регистрации следующих событий:

•использование механизма идентификации и аутентификации;

•внесение объектов в адресное пространство пользователя, например открытие файла, запуск программы;

•удаление объектов;

•действия системных операторов, системных администраторов, администраторов безопасности;

•другие события, затрагивающие информационную безопасность.

Каждая регистрационная запись должна включать следующие поля:
•дата и время события; •идентификатор пользователя; •тип события; •результат действия (успех или неудача).

Для событий идентификации/аутентификации регистрируется также идентификатор устройства, например терминала. Для действий с объектами регистрируются имена объектов. Системный администратор может выбирать набор регистрируемых событий для каждого пользователя.

Класс В1. ***Метки безопасности.*** Надежная вычислительная система должна управлять метками безопасности, ассоциируемыми с каждым субъектом и хранимым объектом. Метки являются основой функционирования меха-

низма принудительного управления доступом. При импорте непомеченной информации соответствующий уровень секретности должен запрашиваться у авторизованного пользователя и все такие действия следует протоколировать.

Целостность меток безопасности. Метки должны адекватно отражать уровни секретности субъектов и объектов. При экспорте информации метки должны преобразовываться в точное и однозначно трактуемое внешнее представление, сопровождающее данные. Каждое устройство ввода/вывода (в том числе коммуникационный канал) должно трактоваться как одноуровневое или многоуровневое. Все изменения трактовки и ассоциированных уровней секретности должны протоколироваться.

Принудительное управление доступом. Надежная вычислительная система должна обеспечить проведение в жизнь принудительного управления доступом всех субъектов ко всем хранимым объектам. Субъектам и объектам должны быть присвоены метки безопасности, являющиеся комбинацией упорядоченных уровней секретности, а также категорий. Метки являются основой принудительного управления доступом. Надежная вычислительная система должна поддерживать по крайней мере два уровня секретности. Субъект может читать объект, если его (субъекта) метка безопасности доминирует над меткой безопасности объекта, то есть уровень секретности субъекта не меньше уровня секретности объекта и все категории объекта входят в метку безопасности субъекта. Субъект может писать в объект, если метка безопасности объекта доминирует над меткой субъекта. Надежная вычислительная база должна контролировать идентификационную и аутентификационную информацию. При создании новых субъектов, например процессов, их метки

Верификация спецификаций архитектуры. Должна существовать неформальная или формальная модель политики безопасности, поддерживаемой надежной вычислительной базой. Модель должна соответствовать основным посылкам политики безопасности на протяжении всего жизненного цикла системы.

Класс B2. ***Предоставление надежного пути.*** Надежная вычислительная система должна поддерживать надежный коммуникационный путь к себе для пользователя, выполняющего операции начальной идентификации и аутентификации. Инициатива в общении по этому пути должна исходить исключительно от пользователя.

Анализ тайных каналов. Системный архитектор должен тщательно проанализировать возможности по организации тайных каналов с памятью и оценить максимальную пропускную способность каждого выявленного канала.

Надежное администрирование. Система должна поддерживать разделение функций оператора и администратора.

Конфигурационное управление. В процессе разработки и сопровождения надежной вычислительной базы должна использоваться система конфигурационного управления, обеспечивающая контроль за изменениями в описательных спецификациях верхнего уровня, иных архитектурных данных, реализационной документации, исходных текстах, работающей версии объектного кода, тестовых данных и документации. Конфигурационное управление должно обеспечивать соответствие друг другу всех аспектов текущей версии надежной вычислительной базы. Должны предоставляться средства генерации новых версий базы по исходным текстам и средства для сравнения версий, чтобы убедиться в том, что произведены только запланированные изменения.

Класс B3. ***Надежное восстановление.*** Должны существовать процедуры и/или механизмы, позволяющие произвести восстановление после сбоя или иного нарушения работы без ослабления защиты.

Класс A1. ***Надежное распространение.*** Должна поддерживаться целостность соответствия между эталонными данными, описывающими текущую версию вычислительной базы, и эталонной копией текстов этой версии. Должны существовать процедуры, подтверждающие соответствие между поставляемыми клиентам аппаратными и программными компонентами и эталонной копией.

Литература

1. РД ГТК России. Концепция защиты СВТ от НСД к информации. Автоматизированные системы. Защита от НСД. Классификация АС и требования по защите информации. - Москва, 1992.

2. РД ГТК России. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД в АС и СВТ. - Москва, 1992.

3. ГОСТ Р 50922-96 Защита информации. Основные термины и определения. – Москва: Госстандарт, 1996.

4. РД ГТК России. Концепция защиты СВТ и АС от НСД к информации. - Москва, 1992.

5. РД ГТК России. Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации. - Москва, 1992.

6. Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и защите информации» - М., 2006.

7. Гатчин Ю.А., Климова Е.В., Ожиганов А.А. Основы информационной безопасности компьютерных систем и защиты государственной тайны: учебное пособие. ISBN 5-8064-0475-7. - СПб.: СПбГИТМО,2002. – 60 с.

8. Информационная безопасность: учебно-практическое пособие/ сост. Н.Н.Нечаева – Ульяновск: УлГТУ, 2007. – 217 с.

9. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М.: Сов. Радио, 1999. – 328 с.

10. Иванов И.Г., Кузнецов П.А.. Попов В.И. Методические основы защиты информации в банковских автоматизированных комплексах // Защита информации. 1994. №1. - С. 13-24.

11. Гайкович В.Ю. Основы безопасности информационных технологий. – М.: Инфо-М,1998.

12. Гайкович В.Ю., Першин А.Ю. Безопасность электронных банковских систем. - М.: Единая Европа, 1994. - 363 с.

13. Проскурин В.Г., Крутов С.В., Мацкевич И.В. Программно-аппаратные средства обеспечения информационной безопасности. Защита в ОС. - М.: Радио и связь, 2000. - 166 с.

14. Галатенко В.А. Основы информационной безопасности: курс лекций – М.: ИНТУИТ.ру, 2006. – 208 с.

15. Домарев В.В. Защита информации и безопасность компьютерных систем. - Киев: ДиаСофт, 1999. - 480 с.

16. Мельников В.В. Защита информации в компьютерных системах. - М.: Финансы и статистика, 1997. - 367 с.

17. Теория и практика обеспечения информационной безопасности (Серия «Защита информации») / Под ред. П.Д. Зегжды. - М.: Яхтсмен. 1996. - 192 с.

18. Department of Defense Trusted Computer System Evaluation Criteria. - DoD 5200.28-STD, 1993. (Оранжевая книга).

19. ФЗ от 21.07.1993 г. № 5485-1 «О государственной тайне» (ред. от 22.04.2004).

20. Федеральный закон РФ от 29.07.2004 г. N 98-ФЗ «О коммерческой тайне» - М.,2004

21. Федеральный закон Российской Федерации от 27.07.2006 г. N 152-ФЗ «О персональных данных».

22. Краткий учебный терминологический словарь по информатике /Сост. Е.В.Климова. – СПб.: Изд-во СПИМаш, 2009. – 64 с.

Терминологический словарь

АВТОРИЗАЦИЯ – предоставление определенных полномочий лицу (группе лиц) на выполнение некоторых действий в системе обработки данных.

АДМИНИСТРАТОР базы данных (БД) – Специальное должностное лицо (группа лиц), имеющее полное представление о БД и отвечающее за ее ведение, использование и развитие

А. защиты - субъект доступа, ответственный за защиту автоматизированной системы от НСД к информации

АККРЕДИТАЦИЯ – авторизация и санкционирование возможности обработки критичных данных в операционной среде информационной системы или сети. Решение об А. выносится после получения всеми лицами из технического персонала сертификата, подтверждающего возможность этих лиц работать с защищенными системами

АКТУАЛИЗАЦИЯ - процесс, обеспечивающий постоянное внесение текущих изменений в состояние системы, базы данных

АНАЛИЗ трафика - (рабочей нагрузки) линии связи – исследование наблюдаемых потоков данных, проходящих между пунктами по сети связи (наличие, отсутствие, объем, направление, частота)

АНТИВИРУСНЫЕ программы - программы, предотвращающие заражение компьютерным вирусом и ликвидирующие последствия заражения

АТТЕСТАЦИЯ средств защиты – удостоверение степени соответствия требованиям к данному классу средств защиты

АУТЕНТИФИКАЦИЯ – проверка принадлежности субъекта доступа предъявленного им идентификатора, подтверждение подлинности

А. пользователя – проверка соответствия пользователя предъявляемому им идентификатору

БАГ (англ. **bug** — жук) — жаргонное слово, обозначающее ошибку в программе. Термин обычно употребляется в отношении ошибок, проявляющих себя на стадии работы программы, в отличие, например, от ошибок проектирования или синтаксических ошибок.

БАГТРАК (англ. Bugtraq) — лента новостей (сайты или списки рассылки) об уязвимостях в программном обеспечении. Обновляется каждый месяц.

БАЗА ДАННЫХ (БД) – совокупность данных, организованных по определенным правилам, предусматривающим общие принципы описания, хранения и манипулирования данными, независимая от прикладных программ. Является информационной моделью предметной области. Обращение к БД осуществляется с помощью СУБД

БАРЬЕР информационный – совокупность различных препятствий, возникающих на пути распространения и использования информации

Б. психологический – возникает между пользователем и новой системой, вызывается, как правило, боязнью трудностей при переходе на новую систему, неизвестностью того, будет ли она понятна и лучше старой

БЕЗВРЕДНЫЕ вирусы - это вирусы ни как не влияющие на работу компьютера. Они не разрушают файлы, но могут переполнять оперативную и дисковую память, выводить на экран графические эффекты и т.д.

БЕЗОПАСНОСТЬ

Б. данных – свойство КС противостоять попыткам НСД к обрабатываемой и хранимой информации. Б. достигается применением аппаратных, программных и криптографических методов и средств защиты, а также комплексом организационных мероприятий. Одним из показателей Б. является безопасное время.

Б. информации – состояние защищенности информации, обрабатываемой средствами ВТ, или автоматизированной системы от внутренних или внешних угроз.

Б. компьютерных систем – свойство КС противостоять попыткам НСД к обрабатываемой и хранимой информации, вводу информации, приводящей к деструктивным действиям, и навязыванию ложной информации

Б. субъектов информационных отношений - защищенность субъектов информационных отношений от нанесения им материального, морального или иного ущерба путем воздействия на информацию и/или средства ее обработки и передачи.

БРАНДМАУЭР – сочетание программного и аппаратного обеспечения, образующее систему защиты от несанкционированного доступа к компьютеру из внешней глобальной или локальной сети

ВЕРИФИКАЦИЯ – 1/ процесс сравнения двух уровней спецификации средств ВТ или АС на надлежащее соответствие; 2/ в программировании – до-

казательство правильности программ. Различают два подхода к верификации: статический и конструктивный.

ВИРУС – программа, способная самопроизвольно создавать свои копии и модифицирующая другие программы, записанные в файлах или системных областях, для последующего получения управления и воспроизводства новой копии. Часто содержит бомбы или создает различные аудио- и видео эффекты. Переносится при копировании программ. Либо через дискеты, с которыми работали на зараженном компьютере.

ВИРУСЫ-репликаторы (черви). Распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии (от англ. Replicators - объекты, которые копируют сами себя)

ВЛАДЕЛЕЦ - в системе ЗИ и контроля доступа – пользователь, имеющий неограниченные права по отношению к файлу или другой информации.

ВРЕМЯ

Безопасное В. – математическое ожидание времени раскрытия системы защиты статистическим опробированием возможных вариантов доступа к данным. Вычисляется по формуле: $T = \sum_{i=1}^{n} p_i t_i$, где n – число проб, p_i – вероятность раскрытия при i-й пробе, t_i – время, затрачиваемое на i-ю пробу.

Среднее В. безотказной работы – среднестатистическая продолжительность нормального функционирования технического устройства между двумя последовательными отказами.

ВЫЗОВ

санкционированный В. – вызов системы, программы или данных. разрешенный данному пользователю. Как правило, реализуется путем ввода и проверки пароля.

ГАРАНТИЯ

Г. защиты – формальное разрешение на возможность использования для работы данной конкретной вычислительной машины на месте ее установки только после обеспечения защиты от НСД.

ДАМП – 1/ вывод содержимого памяти ЭВМ на устройство регистрации, из одного запоминающего устройства в другое или из одного раздела (зоны) в другой раздел (зону); 2/ данные, полученные при разгрузке памяти.

Защитный Д. (дамп контрольной точки) – копия рабочего пространства, связанного с проведением процесса, сделанная с учетом использования ее для перезапуска процесса после сбоя в системе.

ДЕЗИНФОРМАЦИЯ – Сознательное искажение передаваемых сведений с целью ложного представления у лиц, использующих эти сведения; передача ложной информации.

ДЕЯТЕЛЬНОСТЬ

Незаконная Д. В сфере ПО – непредусмотренная документами деятельность лиц, заключающаяся в копировании и распространении ПО без соответствующей лицензии.

ДОВЕРИТЕЛЬНОСТЬ – свойство соответствия безопасности некоторым критериям

ДОСТОВЕРНОСТЬ – свойство информации быть правильно воспринятой; вероятность отсутствия ошибки

ДОСТУПНОСТЬ – свойство ресурса, заключающееся в возможности его использования по требованию пользователя, имеющего соответствующие полномочия

Д. данных – свойство данных, состоящее в возможности их чтения пользователем или программой. Определяется рядом факторов: возможностью работать за терминалом, обладанием пароля, знанием языка запросов и т.д.

Д. информации - свойство системы, в которой циркулирует информация (средств и технологии ее обработки), характеризующееся способностью обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия.

ЖИВУЧЕСТЬ – свойство системы оставаться работоспособной в условиях внешних воздействий

ЖИЗНЕННО ВАЖНЫЕ ИНТЕРЕСЫ - совокупность потребностей, удовлетворение которых необходимо для надежного обеспечения существования и возможности прогрессивного развития субъекта (личности, организации, общества или государства).

ЗАКОН о защите данных 1984 г. – закон, принятый в Великобритании в соответствии с принципами Совета европейской конвенции.

ЗАКОНОДАТЕЛЬСТВО

З. о защите данных – законодательство, принятое или принимаемое во всех странах для защиты персональных данных, обрабатываемых компьютерами. Цель З. заключается в контроле и предотвращении неправильного использования информации в случае, когда персональные данные хранятся в компьютере.

ЗАЩИТА – средство для ограничения доступа или использования всей или части вычислительной системы; юридические, организационные и технические, в том числе программные, меры предотвращения НСД к аппаратуре, программам и данным.

З. криптографическая – защита информации путем осуществления ее криптографического преобразования.

З. многоуровневая - защита, обеспечивающая разграничение доступа субъектов с различными правами доступа к объектам различных уровней конфиденциальности.

З. непосредственная – меры, предусматривающие физическую защиту ресурсов от преднамеренных случайных угроз.

З. от НСД – предотвращение или существенное затруднение НСД к программам и данным путем использования аппаратных, программных и криптографических методов и средств защиты, а также проведение организационных мероприятий. Наиболее распространенным программным методом защиты является система паролей.

З. прав пользователей – совокупность правил, методов и средств, направленных на обеспечение беспрепятственного и своевременного доступа пользователей к программам и данным и защиту их информации от использования другими лицами.

З. предупредительная – организационные меры защиты от копирования. Предусматривающие суровый штраф или угрозу штрафа лицу, которое пытается несанкционированно копировать программу или файл.

ЗАЩИЩЕННОСТЬ – в вычислительной технике – способность системы противостоять НСД к программам и данным (безопасность, секретность), а также их случайному искажению или разрушению (целостность).

ЗЛОУМЫШЛЕННИК – лицо или организация, заинтересованные в получении несанкционированного доступа к программам или данным, предпринимающие попытку такого доступа или совершившие его.

ИНФАСТРУКТУРА информации – структура системы информационного обеспечения государства, представляющая собой совокупность информационно-вычислительных центров, банков данных и знаний и единой автоматизированной системы связи. Обеспечивает общие условия доступа всех потребителей и хранимой информации и предоставляет им возможность использования новых информационных технологий.

ИНФОРМАЦИЯ – совокупность знаний о фактических данных и зависимостях между ними. Является одним из видов ресурсов, используемых человеком в трудовой деятельности и в быту.

ИНФОРМАЦИЯ В КС - сведения о фактах, событиях, процессах и явлениях в некоторой предметной области, включенные в систему обработки информации, или являющиеся ее результатом в различных формах представления на различных носителях и используемые (необходимые) для оптимизации принимаемых решений в процессе управления объектами данной предметной области.

КВИТИРОВАНИЕ - подтверждение получения данных

КОМПЛЕКС средств защиты – совокупность программных и технических средств, создаваемая и поддерживаемая для обеспечения защиты СВТ и автоматизированных систем от НСД к информации.

КОМПРОМЕТАЦИЯ – утеря критичности информации или получение ее неавторизованными для этого субъектами (лицами, программами, процессами и т. д.).

КОМПЬЮТЕРНЫЕ преступления - различают: 1/финансовые кражи; 2/кражи информации; 3/кражи программного обеспечения; 4/кражи аппаратного обеспечения; 5/саботаж; 6/электронный шпионаж; 7/компьютерное хакерство

КОНТРОЛЬ – совокупность действий, позволяющих получать независимый обзор и анализ системных записей и активности системы с целью установления ее текущего состояния безопасности.

КОНФИДЕНЦИАЛЬНОСТЬ ИНФОРМАЦИИ - субъективно определяемая (приписываемая) информации характеристика (свойство), указывающая

на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемая способностью системы (среды) сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на право доступа к ней.

Объективные предпосылки подобного ограничения доступности информации заключены в необходимости защиты законных интересов некоторых субъектов информационных отношений.

КРИПТОГРАФИЯ – наука, изучающая способы тайной передачи сообщений

КРЭКЕР (англ. cracker) — человек, занимающийся взломом защиты проприетарных (частных) программных средств. Термин компьютерного жаргона. Вне профессиональной среды применяется общий термин «хакер».

ЛИЦЕНЗИЯ – разрешение на право продажи или предоставления услуг.

ЛОГИЧЕСКАЯ бомба - программа, выполняемая периодически или в определенный момент времени с целью исказить, уничтожить или модифицировать данные

МАТРИЦА ДОСТУПА – таблица, отображающая правила разграничения доступа.

МАТРИЦА ПОЛНОМОЧИЙ – таблица, элементы которой определяют права (полномочия, привилегии) определенного объекта относительно **защищаемых данных.**

МЕТКА

М. Конфиденциальности – элемент информации, характеризующий степень конфиденциальности информации, содержащейся в объекте доступа.

МОДЕЛЬ ЗАЩИТЫ – абстрактное описание комплекса программно-технических средств и организационных мер защиты от НСД.

МОДЕЛЬ НАРУШИТЕЛЯ правил разграничения доступа – абстрактное описание нарушителя правил разграничения доступа.

МОДЕЛЬ ПОЛИТИКИ БЕЗОПАСНОСТИ – выражается точным, возможно математическим образом, включающим начальное состояние системы, способы ее перехода из одного состояния в другое и определение «безопасного» состояния системы.

МОРАЛЬНО-ЭТИЧЕСКИЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ - традиционно сложившиеся в стране или обществе нормы поведения и правила обращения с информацией. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормы, однако, их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписаные (например, общепризнанные нормы честности, патриотизма и т.п.), так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний.

НАДЕЖНОСТЬ – характеристика способности функционального узла, устройства, системы выполнять при определенных условиях требуемые функции в течение определенного периода времени. Показателями Н. Является вероятность безотказной работы, среднее время наработки на отказ, среднее время восстановления.

НАРУШИТЕЛЬ – субъект, действия которого нарушают безопасность информации в рассматриваемой компьютерной системе.

НЕСАНКЦИОНИРОВАННЫЙ доступ - доступ, содержащий различные виды нарушения правил по пользованию данными

ОБЛАСТЬ

Защищенная О. – в базе данных, область, доступ к которой требует ввода пароля.

ОБМАН – намеренная попытка вынудить пользователя или ресурс системы выполнить неправомочные действия.

ОБЪЕКТ - пассивный компонент системы, единица ресурса автоматизированной системы (устройство, диск, каталог, файл и т.п.), доступ к которому регламентируется правилами разграничения доступа.

«ОРАНЖЕВАЯ КНИГА» - полное название - Department of Defense Trusted Computer System Evaluation Criteria. - DoD 5200.28-STD («Критерии оценивания безопасности КС министерства обороны»). Это американский стандарт оценивания безопасности КС, устанавливающий 4 класса – A, B, C, D – уровней доверительности (или уверенность в безопасности) для конкретных приложений, разрабатываемых и используемых в интересах правительства.

ОРГАНИЗАЦИОННЫЕ (АДМИНИСТРАТИВНЫЕ) МЕРЫ ЗАЩИТЫ - это меры, регламентирующие процессы функционирования системы об-

работки данных, использование ее ресурсов, деятельность персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности циркулирующей в ней информации.

ОЦЕНКА

О. защиты – проверка системы с целью определения степени ее соответствия установленной модели защиты, стандарту обеспечения защиты и техническим условиям.

О. риска – количественная или качественная оценка повреждения, которое может произойти, если вычислительная система не защищена от определенных угроз. Количественная оценка риска может рассчитываться на основе финансовых потерь, которые могу иметь место, если каждая конкретная угроза будет приводить в действие любой из возможных механизмов уязвимости системы.

ПАКЕТ ОШИБОК – комбинация ошибок (как правило, в двоичном сигнале), которая воспринимается как единая ошибка, если ошибочными являются ее определенные элементы («первый» и «последний»), причем промежуточные элементы не обязательно ошибочны. Отсюда следует, что знаки, предшествующие первой ошибке и следующие за последней ошибкой блока, воспринимаются как правильные.

ПАМЯТЬ С ЗАЩИТОЙ – память, имеющая специальные средства защиты от НСД к любой из ее ячеек.

ПАРОЛЬ – секретный признак, подтверждающий право доступа; обычно строка символов. Идентификатор пользователя, который является его секретом. Служит для защиты данных и программ от НСД.

П. главный – 1/ корневое слово, являющееся общим для определенного набора паролей. 2/ Пароль, предназначенный для защиты каталога паролей.

ПАССИВНАЯ УГРОЗА – возможность НСД к информации без изменения режима функционирования системы.

ПАТЕНТ – гарантия со стороны правительства, данная изобретателю или его доверенному лицу и дающая привилегию в виде исключительного права на реализацию, использование или продажу изобретения в течение определенного срока (обычно 20 лет).

ПЕРЕСТАНОВКА – криптографическая операция, связанная с изменением порядка следования отдельных битов или символов в блоке данных.

ПЕРЕХВАТ

П. сообщений – несанкционированное подключение специального терминала к линии связи, прием и использование сообщений, циркулирующих между абонентскими пунктами и ЭВМ.

ПЕРИОД ДОСТУПА – временной интервал, в течение которого действуют права доступа. В основном этот период определяется в днях или неделях.

ПОДМЕНА – поведение пользователя, пытающегося выдать себя за другого пользователя.

ПОДПИСЬ ЦИФРОВАЯ – дополнительная информация, предоставляемая источником для обеспечения аутентификации. Последовательность данных, добавляемая к блоку данных или к результату его криптографического преобразования, которая позволяет получателю данных проверить источник и целостность блока данных, а также защиту от подлога или подделки.

ПОБИТОВЫЙ ПОДСЧЕТ – метод защиты от копирования, при котором диск распознается как оригинал, если некоторый трек (или другая область) содержит определенное число битов.

ПОКАЗАТЕЛЬ ЗАЩИЩЕННОСТИ СВТ – характеристика средств вычислительной техники, отражающая защищенность и описываемая определенной группой требований, варьируемых по уровню, глубине и зависимости от класса защищенности СВТ.

ПОЛЕ ЗАЩИЩЕННОСТИ СВТ – характеристика СВТ, устанавливающая принадлежность ВТ определенному классу защищенности СВТ.

ПОЛИФАГ - антивирусная программа, распознающая известные ей вирусы по характерным участкам их кода

ПОЛНОМОЧИЯ – право пользователя (терминала, программы, системы) осуществлять те или иные процедуры над защищенными данными.

ПОМЕХИ – возмущения в канале, искажающие передаваемое сообщение.

ПОПЫТКА ДОСТУПА К ИНФОРМАЦИИ НЕАВТОРИЗОВАННАЯ – попытка получить доступ к информации за счет обхода (обмана) средств контроля доступа в сети.

ПОЧТА ЭЛЕКТРОННАЯ – система пересылки сообщений между пользователями вычислительных систем, в которой ЭВМ берет на себя все функции по хранению и пересылке сообщений. Для осуществления такой пересылки отправитель и получатель не обязательно должны одновременно находиться у терминалов и не обязательно должны быть подключены к одной ЭВМ.

ПРАВИЛО РАЗГРАНИЧЕНИЯ ДОСТУПА – совокупность правил, регламентирующих права доступа субъектов к объектам доступа.

ПРАВО – исключительное право, предоставляемое законом автору или его представителю, на воспроизведение, публикацию и копирование оригинальной работы.

ПРАВОВЫЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ - действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения, препятствующие тем самым неправомерному ее использованию и являющиеся сдерживающим фактором для потенциальных нарушителей.

ПРИВАТНОСТЬ ДАННЫХ – статус данных, состоящий в их доступности только владельцу или ограниченной группе пользователей; гарантированная системой доступность к данным со стороны определенного лица или группы лиц.

ПРИВИЛЕГИИ – права пользователя программы, состоящие в доступности определенных объектов и действий в вычислительной системе.

ПРИОРИТЕТ ПРЕРЫВАНИЙ - характеристика важности, присваиваемая программным прерываниям. Как правило, система может одновременно обслуживать только одно прерывание, однако, в некоторых случаях скорость поступления прерываний превышает скорость обслуживания. В подобной ситуации при помощи системных устройств управления можно установить такие маски прерываний, которые будут подавлять некоторые прерывания при наличии более важных прерываний.

ПРОВЕРКА КРИПТОГРАФИЧЕСКАЯ – процесс извлечения информации с помощью криптографического преобразования.

ПРОГРАММА – упорядоченная последовательность команд, подлежащая обработке; последовательность предложений языка программирования, описывающих алгоритм решения задачи.

ПРОКСИ-СЕРВЕР, брандмауэр - предназначен для решения проблем безопасности сети. Находится между компьютером и Интернетом

ПРОТИВОРЕЧИВОСТЬ ДАННЫХ – состояние базы данных, при котором дублирующие данные не равны или значения жанных не соответствуют области их определения.

ПРОХОД ЧЕРЕЗ СИСТЕМУ ЗАЩИТЫ (ОБХОДНОЙ ПУТЬ) – 1/ блок, скрытый в большой программе, который разрешает пользователю пре-

одолеть систему защиты или учета ресурсов системы в штатном режиме; 2/ блок обхода, встроенный в систему шифрования.

ПУТЬ ПРОНИКНОВЕНИЯ – проследовательность несанкционированных действий пользователя при его проникновении в защищенную вычислительную систему.

РАЗГРАНИЧЕНИЕ ДОСТУПА – совокупность методов, средств и мероприятий, обеспечивающих защиту данных от НСД пользователей.

РАЗДЕЛЕНИЕ

Р. ПРИВИЛЕГИЙ – принцип открытия механизма защиты данных, при котором для доступа к ним необходимо указать не один, а два пароля (например, двумя лицами).

Р. управляемое – предоставление используемого ресурса двум или более использующим ресурсам с помощью некоторого механизма управления доступом.

РАЗРУШЕНИЕ ИНФОРМАЦИИ – стирание информации, хранящейся в памяти ЭВМ.

РАЗРЯД ЗАЩИТЫ – один из дополнительных разрядов промежуточных результатов, обеспечивающих сохранение точности.

РЕГИСТРАЦИЯ – часть процедуры входа пользователя в систему, которая заключается в фиксации (документировании) идентификационного кода или пароля для получения доступа в вычислительную систему.

Р. открытого ключа – процесс фиксации открытых ключей, обеспечивающих достоверную информацию лицу, осуществляющему запрос, с целью предотвратить фальсификацию значения открытого ключа.

РЕЖИМ

Р. защищенный – режим, защищенной обработки базы данных, в котором все прикладные программы, работающие параллельно с программой, открывшей области базы данных в этом режиме, могут читать записи, но не могут их обновлять до тех пор, пока программа не закроет их.

Р. обеспечения безопасности – описание всех категорий допусков пользователей в привязке ко всем категориям защиты информации, которая должна храниться и обрабатываться в системе.

САНКЦИОНИРОВАННЫЙ доступ – доступ к данным или элементам сети, разрешенный уполномоченным лицом

СЕКРЕТНОСТЬ ДАННЫХ – ограничение, накладываемое автором на доступ к его информации другим лицам. Оформляется присваиванием информации определенного грифа и осуществляется закрытием ее паролем, шифрованием и другими методами.

СЕРТИФИКАТ ЗАЩИТЫ – документ, удостоверяющий соответствие СВТ или АС набору требований по защите от НСД к информации и дающий право разработчику на использование и/или распространение их как защищенных.

СЕРТИФИКАЦИЯ – официальная аттестация программы.

С. уровня защиты – процесс установления соответствия средства ВТ и АС набору определенных требований по защите.

СИГНАТУРА – уникальная характеристика системы, которая может быть проверена. Примером С. может служить признак диска, используемый в качестве идентификационной метки диска-оригинала; этот признак не должен копироваться программным способом.

СИСТЕМА

С. защиты данных – комплекс аппаратных, программных и криптографических средств, а также мероприятий, обеспечивающих защиту данных от случайного или преднамеренного разрушения, искажения или использования.

С. экспертная – комплекс программных средств, в основу которого положена интерпретация правил, аккумулирующих знания экспертов по определенной специальности.

СКРИПТКИДДИ (англ. *script kiddie* — «ребёнок, использующий скрипты») — человек, не понимающий принципов работы используемых им хакерских средств для взлома.

СТАРЕНИЕ информации – свойство информации утрачивать свою практическую ценность, обусловленное изменением состояния отображаемой ею предметной области.

СТЕЛС-ВИРУС - вирус, который оставляет в памяти компьютера модули, перехватывающие обращение программ к дискам

СТРАТЕГИЯ ЗАЩИТЫ – формальное определение критериев, особенно оперативных, которыми следует руководствоваться при обеспечении защиты системы от известных угроз.

СУБЪЕКТ - активный компонент системы (пользователь, процесс, программа), действия которого регламентируются правилами разграничения доступа.

СУБЪЕКТЫ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ - государство, государственные органы, государственные, общественные или коммерческие организации (объединения) и предприятия (юридические лица), отдельные граждане (физические лица) и иные субъекты, взаимодействующие с целью совместной обработки информации.

По отношению к информации, обрабатываемой в КС различные субъекты - участники информационных отношений могут выступать (возможно одновременно) в качестве:

- источников информации;
- пользователей (потребителей) информации;
- собственников (владельцев, распорядителей) информации;
- физических и юридических лиц, о которых собирается и обрабатывается информация;
- владельцев КС и участников процессов обработки и передачи информации и т.д.

ТЕХНИЧЕСКИЕ (АППАРАТНО-ПРОГРАММНЫЕ) СРЕДСТВА ЗАЩИТЫ - различные электронные устройства и специальные программы, входящие в состав КС, которые выполняют (самостоятельно или в комплексе с другими средствами) функции защиты информации (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

ТРОЯНСКАЯ программа (**троянский конь**) — программа, используемая злоумышленником для сбора информации, её разрушения или модификации, нарушения работоспособности компьютера или использования его ресурсов в неблаговидных целях

УГРОЗА – потенциальная возможность нарушения защиты от НСД.

УЧЕТНАЯ запись – сведения о пользователе отдельного компьютера или сети: его логин, пароль и описание прав доступа к ресурсам. Эти сведения хранятся в зашифрованном виде в специально отведенном месте

УЯЗВИМОСТЬ – свойство системы, которое может привести к нарушению ее защиты при наличии угрозы. У. может возникать случайно из-за неадекватного проектирования или неполной отладки или может быть результатом злого умысла.

УЯЗВИМОСТЬ ИНФОРМАЦИИ - подверженность информации воздействию различных дестабилизирующих факторов, которые могут привести к нарушению ее конфиденциальности, целостности, доступности, или неправомерному ее тиражированию.

УЯЗВИМОСТЬ СУБЪЕКТА ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ - потенциальная подверженность субъекта нанесению ущерба его жизненно важным интересам посредством воздействия на критичную для него информацию, ее носители и процессы обработки.

ФИЗИЧЕСКИЕ МЕРЫ ЗАЩИТЫ - это разного рода механические, электро- или электронно-механические устройства и сооружения, специально предназначенные для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам АС и защищаемой информации, а также технические средства визуального наблюдения, связи и охранной сигнализации.

ФЛАГ – часть формата элемента данных из одного или нескольких битов, которые определяют его статус.

ФРИ́КИНГ (англ. *phreaking*) — сленговое выражение, означающее взлом телефонных автоматов и сетей, обычно с целью получения бесплатных звонков.

ФРИКЕРЫ (англ. *phreaker*). **-** люди, специализирующихся на фрикинге. Это же название применяют к людям, использующим в своих неправомерных действиях телефон с целью оказать психологическое воздействие на конечного абонента.

ХАКЕР – пользователь, который пытается вносить изменения в системное ПО, не имея на это право. Этом может быть программист, который создает более или менее полезные вспомогательные программы, обычно плохо документированные и иногда вызывающие нежелательные побочные результаты.

ЦЕЛОСТНОСТЬ – состояние данных или КС, в которой данные или программы используются установленным образом, обеспечивающим устойчи-

вую работу системы, автоматическое восстановление в случае обнаружения системой потенциальной ошибки, автоматическое использование альтернативных компонентов вместо вышедших из строя.

ЦЕЛОСТНОСТЬ ИНФОРМАЦИИ - свойство информации, заключающееся в ее существовании в неизменном виде (по отношению к некоторому фиксированному ее состоянию) в условиях случайного и (или) преднамеренного искажения (разрушения).

ЦЕННОСТЬ информации – свойство информации, определяемое ее пригодностью к практическому использованию в различных областях целенаправленной деятельности человека.

ШИФР – криптографический прием, связанный с применением некоторого алгоритма преобразования символов (букв и цифр) исходного (незашифрованного) текста в зашифрованный код.

Ш. ассиметричный – шифр, в котором ключ шифрования не совпадает с ключом дешифрования.

ШИФРОВАНИЕ – криптографическое преобразование данных для получения шифрованного текста.

ЭКСПЛОЙТ – это любая программа, разработанная с целью выявления или использования уязвимостей в другом ПО.

ЭЛЕКТРОННАЯ ПОДПИСЬ – компьютерный эквивалент обычной подписи под документом, который должен обеспечить подлинность документа и защитить передаваемое сообщение от изменений

ЭЛЕКТРОННЫЙ КЛЮЧ – устройство для защиты программных продуктов от незаконного тиражирования и использования

ЭНТРОПИЯ – мера неопределенности состояния объекта или некоторой ситуации (случайной величины) с конечным числом исходов. Понятие введено Шенноном. Используется для определения количества информации в сообщении. При равновероятности всех значений сообщения $H = k*\log m$, где H – энтропия, k – число знаков в сообщении, m – число знаков в алфавите источника.

ЭХОКОНТРОЛЬ – метод контроля передачи данных, при котором принятые данные, возвращаются на передающий пункт и сравниваются с переданными данными.

ЯДРО защиты – технические программы и многопрограммные элементы комплекса средств защиты, реализующие концепцию диспетчера доступа.

СПбГУ ИТМО стал победителем конкурса инновационных образовательных программ вузов России на 2007–2008 годы и успешно реализовал инновационную образовательную программу «Инновационная система подготовки специалистов нового поколения в области информационных и оптических технологий», что позволило выйти на качественно новый уровень подготовки выпускников и удовлетворять возрастающий спрос на специалистов в информационной, оптической и других высокотехнологичных отраслях науки. Реализация этой программы создала основу формирования программы дальнейшего развития вуза до 2015 года, включая внедрение современной модели образования.

КАФЕДРА ПРОЕКТИРОВАНИЯ КОМПЬЮТЕРНЫХ СИСТЕМ

1945 - 1966 РЛПУ (кафедра радиолокационных приборов и устройств). Решением Правительства в августе 1945 г. в ЛИТМО был открыт факультет электроприборостроения. Приказом по Институту от 17 сентября 1945 г. на этом факультете была организована кафедра радиолокационных приборов и устройств, которая стала готовить инженеров, специализирующихся в новых направлениях радиоэлектронной техники, таких как радиолокация, радиоуправление, теленаведение и др. Организатором и первым заведующим кафедрой был д. т. н., профессор Зилитинкевич СИ. (до 1951 г.). Выпускникам кафедры присваивалась квалификация инженер-радиомеханик, а с 1956 г. - радиоинженер (специальность 0705).

В разные годы кафедрой заведовали доцент Мишин Б.С., доцент Захаров И.П.. доцент Иванов А Н .

1966 - 1970 КиПРЭА (кафедра конструирования и производства радиоэлектронной аппаратуры). Каждый учебный план специальности 0705 коренным образом отличался от предыдущих планов радиотехнической специальности своей четко выраженной конструкторско-технологической направленностью. Оканчивающим институт по этой специальности присваивалась квалификация инженер - конструктор - технолог РЭА.

Заведовал кафедрой доцент Иванов А Н .

1970 - 1988 КиПЭВА (кафедра конструирования и производства электронной вычислительной аппаратуры). Бурное развитие электронной вычислительной техники и внедрение ее во все отрасли народного хозяйства потребовали от отечественной радиоэлектронной промышленности решения новых от-

ветственных задач. Кафедра стала готовить инженеров по специальности 0648. Подготовка проводилась по двум направлениям: автоматизация конструирования ЭВА и технология микроэлектронных устройств ЭВА.

Заведовали кафедрой д.т.н., проф. Новиков В В . (до 1976 г.), затем проф. Петухов Г.А.

1988 - 1997 МАП (кафедра микроэлектроники и автоматизации проектирования) Кафедра выпускала инженеров - конструкторов - технологов по микроэлектронике и автоматизации проектирования вычислительных средств (специальность 2205). Выпускники этой кафедры имеют хорошую технологическую подготовку и успешно работают как в производстве полупроводниковых интегральных микросхем, так и при их проектировании, используя современные методы автоматизации проектирования. Инженеры специальности 2205 требуются микроэлектронной промышленности и предприятиям - разработчикам вычислительных систем.

Кафедрой с 1988 г. по 1992 г. руководил проф. Арустамов С А , затем снова проф. Петухов Г.А.

С 1997 ПКС (кафедра проектирования компьютерных систем). Кафедра выпускает инженеров по специальности Проектирование и технология электронно-вычислительных средств. Область профессиональной деятельности выпускников включает в себя проектирование, конструирование и технологию электронных средств, отвечающих целям их функционирования, требованиям надежности, дизайна и условиям эксплуатации Кроме того, кафедра готовит специалистов по специальности 2206 - Организация и технология защиты информации, причем основное внимание уделяется программно-аппаратной защите информации компьютерных систем.

С 1996 г. кафедрой заведует д.т.н., профессор Гатчин Ю.А.