Г. А. КОСТИН, В. А. КУЛИШКИН,
С. В. МАРКОВ, С. Н. ПАНИН

# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ


САНКТ-ПЕТЕРБУРГСКИЙ УНИВЕРСИТЕТ УПРАВЛЕНИЯ И ЭКОНОМИКИ

САНКТ-ПЕТЕРБУРГСКИЙ УНИВЕРСИТЕТ
УПРАВЛЕНИЯ И ЭКОНОМИКИ

**Г. А. Костин, В. А. Кулишкин,**
**С. В. Марков, С. Н. Панин**

# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

*Учебник*

Санкт-Петербург
2011

УДК 004
ББК 32.973.202
К 72

*Рецензент:*
заведующий кафедрой информационных систем в экономике
СПбГИЭУ, д-р техн. наук, профессор
***Ирина Александровна Брусакова***

**Костин Г. А., Кулишкин В. А., Марков С. В., Панин С. Н.**

К 72 Информационная безопасность и защита информации: учебник. — СПб.: Издательство Санкт-Петербургского университета управления и экономики, 2011. — 300 с.: ил.

ISBN 978-5-94047-314-5

В учебнике рассматриваются проблемы информационной безопасности, ставшие особенно актуальными в связи с массовым переходом информационных технологий на автоматизированную основу. Авторами проведен анализ совокупности технических средств, с помощью которых может регистрироваться и передаваться информация; характеризуются направления правовой деятельности, регулирующей отношения в области обеспечения информационной безопасности; указаны основные нормативные документы, регламентирующие деятельность по обеспечению безопасности информации; представлены сведения об инженерно-механических системах обеспечения безопасности объектов, а также системах обнаружения, опознавания, регистрации и сигнализации попыток проникновения на охраняемый объект; рассмотрены основные этапы построения системы защиты информации на охраняемом объекте; приведен порядок обеспечения безопасности информации в информационных системах персональных данных.

Учебник предназначен в помощь студентам высших учебных заведений, изучающим основные образовательные программы по направлениям подготовки бакалавриата 090900.62 «Информационная безопасность» и 230700.62 «Прикладная информатика» для формирования общекультурных и профессиональных компетенций по вопросам обеспечения информационной безопасности на всех этапах разработки и эксплуатации информационных систем.



ISBN 978-5-94047-314-5

# ВВЕДЕНИЕ

Работа современного специалиста во многих областях и сферах практической деятельности связана с компьютерными информационными технологиями. Увеличение объемов информации, используемой государственными и коммерческими организациями, вызвало необходимость применения эффективных информационных систем, сетей и технологий, обеспечивающих оперативный сбор, передачу, обработку, систематизацию, выдачу данных, формирование рекомендаций по принятию управленческих решений и т. п. Однако развитие новых информационных технологий повысило уязвимость информации от действия случайных и преднамеренных угроз и вызвало необходимость принятия срочных мер по обеспечению информационной безопасности, включая установку технических и программных средств защиты и проведение специальных организационных мероприятий.

Актуальность проблемы обеспечения информационной безопасности также обусловлена важностью и значимостью информации, используемой во многих государственных и коммерческих организациях. Нарушение конфиденциальности, целостности или доступности информации ведет к крайне нежелательным последствиям. Поэтому вопросам обеспечения информационной безопасности в настоящее время уделяется особое внимание на всех этапах разработки и эксплуатации информационных систем.

Учебно-методические материалы включают десять разделов, в которых изложены основы обеспечения информационной безопасности и защиты информации.

В разделе 1 «Основные понятия и определения информационной безопасности» вводятся базовые понятия, связанные с обеспечением информационной безопасности, рассматриваются основные угрозы безопасности и основные меры противодействия им.

В разделе 2 «Характеристики угроз информационной безопасности на объекте защиты, классификация технических каналов утечки информации» проведен анализ совокупности технических средств, с помощью которых может регистрироваться и передаваться информация, а также рассмотрена физическая среда, в которой распространяется информативный сигнал.

В разделе 3 «Правовые основы обеспечения информационной безопасности» приведены направления правовой деятельности, регулирующей отношения в области обеспечения информационной безопасности; указаны основные руководящие документы, регламентирующие деятельность по обеспечению безопасности информации.

В разделе 4 «Организационные основы обеспечения информационной безопасности» рассматриваются организационные меры, связанные с сертификацией информационных систем и сетей, категорированием и аттестацией объектов вычислительной техники, приводятся основные сведения о политике безопасности.

В разделе 5 «Технические средства защиты информации» изложены сведения об активных и пассивных средствах для подавления сигналов, распространяемых в физической среде, приведены их характеристики и рекомендации по рациональному использованию.

В разделе 6 «Аппаратные и программные средства защиты информации» рассмотрены особенности современных аппаратных и программных средств защиты информации. Представлены процедуры программ внешней, внутренней защиты, а также процедуры программ ядра системы безопасности.

В разделе 7 «Физическая защита объектов информатизации» рассматриваются понятия о комплексной защите объектов, представлены сведения о инженерно-механических системах обеспечения безопасности объектов, а также системах обнаружения, опознавания, регистрации и сигнализации попыток проникновения на охраняемый объект.

В разделе 8 «Стеганографические технологии и методы защиты информации» приведены основные понятия стеганографии, отражена история ее зарождения и развития, изложены особенности технологий и методов защиты различной информации.

В разделе 9 «Антивирусная защита информации» дана характеристика и классификация компьютерных вирусов, представлены современные средства антивирусной защиты, предложены рекомендации по их применению.

В разделе 10 «Общий подход к обеспечению безопасности информационных систем» представлены основные этапы построения системы защиты информации на охраняемом объекте, приведен порядок обеспечения безопасности информации в информационных системах персональных данных.

В приложениях приведены нормативно-правовые документы, регламентирующие деятельность в области обеспечения безопасности информации.

Пособие рекомендуется для студентов, обучающихся по направлению бакалавриата 090900.62 «Информационная безопасность» и 230700.62 — «Прикладная информатика», а также может быть полезно широкому кругу специалистов в области информационных технологий.

Учебник подготовлен коллективом авторов:

Костин Геннадий Александрович — заведующий кафедрой прикладной информатики Санкт-Петербургского университета управления и экономики, доктор технических наук, доцент.

Кулишкин Виталий Александрович — начальник бюро рационализации и изобретательства Михайловской военной артиллерийской академии, кандидат военных наук, доцент.

Марков Сергей Владимирович — профессор кафедры прикладной информатики Санкт-Петербургского университета управления и экономики, кандидат технических наук, доцент.

Панин Сергей Николаевич — профессор кафедры прикладной информатики Санкт-Петербургского университета управления и экономики, кандидат технических наук, доцент.

# 1. ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Информация — это сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления. Информация может существовать в различных формах в виде совокупностей некоторых знаков (символов, сигналов и т. д.) на носителях различных типов. Она может представлять ценность для отдельных лиц или организаций.

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

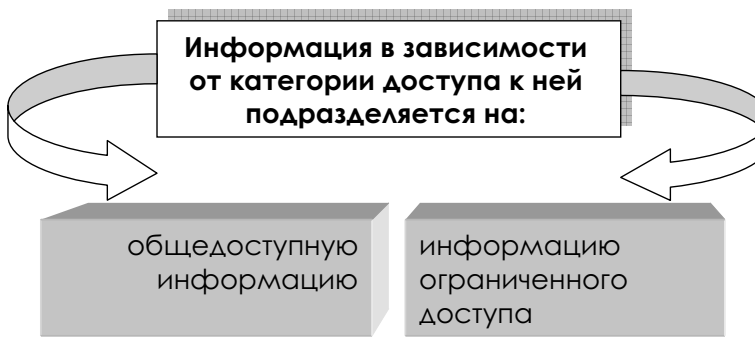


*Рис. 1.1.* Зависимость информации от категории доступа к ней

Информация, доступ к которой ограничен федеральными законами (информация ограниченного доступа), в свою очередь подразделяется на сведения, составляющие государственную тайну (ГТ) и конфиденциальную информацию (КИ).

Информация в зависимости от порядка ее предоставления или распространения подразделяется на:

- информацию, свободно распространяемую;
- информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;
- информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;

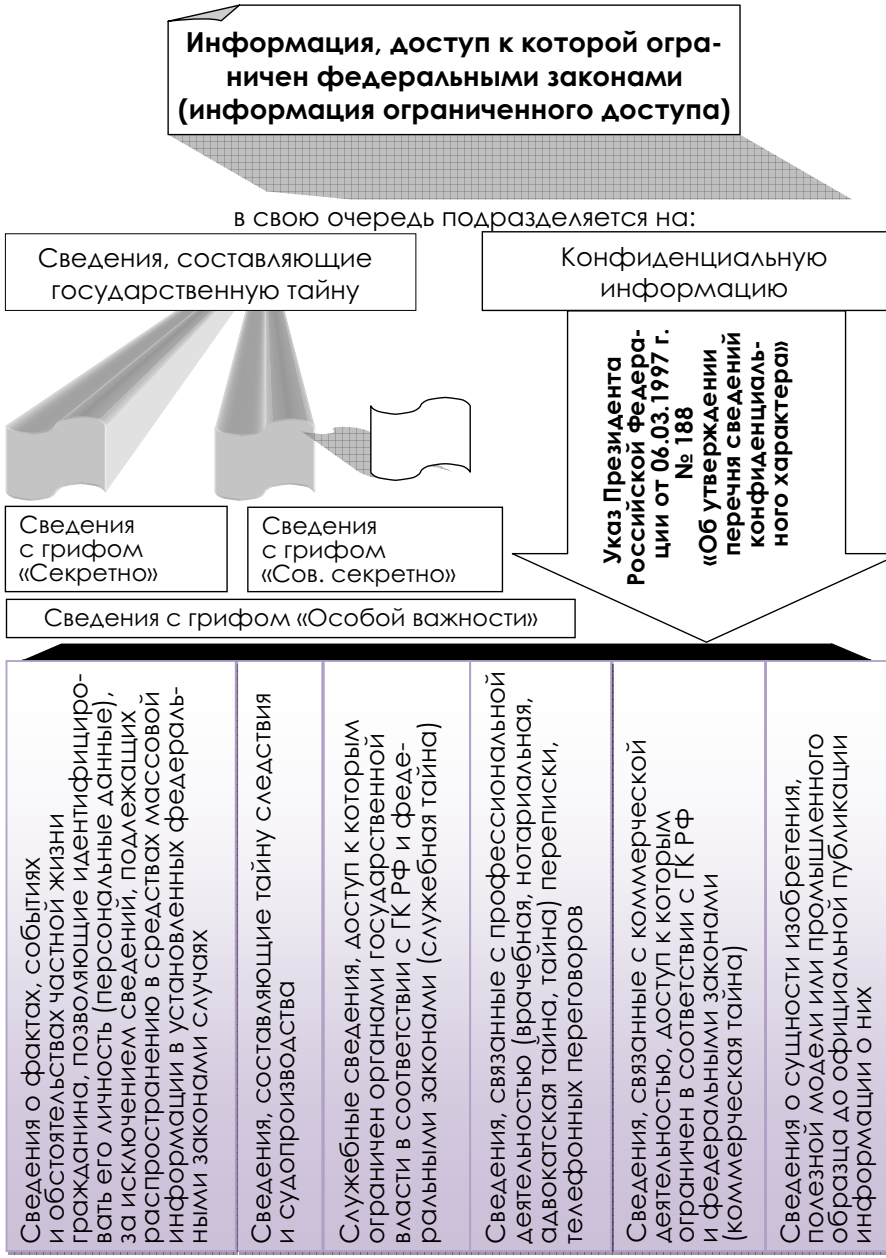


*Рис. 1.2.* Виды информации ограниченного доступа

- информацию, распространение которой в Российской Федерации ограничивается или запрещается.

Законодательством Российской Федерации установлены следующие виды информации в зависимости от ее содержания и категории доступа к ней.

Общедоступная и информация ограниченного доступа: к общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен.

Общедоступная информация может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации.

Обладатель информации, ставшей общедоступной по его решению, вправе требовать от лиц, распространяющих такую информацию, указывать себя в качестве источника такой информации.

Право на доступ к информации имеют граждане и организации.

Граждане (физические лица) и организации (юридические лица) (далее — организации) вправе осуществлять поиск и получение любой информации в любых формах и из любых источников при условии соблюдения требований, установленных настоящим Федеральным законом и другими федеральными законами.

Гражданин (физическое лицо) имеет право на получение от государственных органов, органов местного самоуправления, их должностных лиц в порядке, установленном законодательством Российской Федерации, информации, непосредственно затрагивающей его права и свободы.

Организация имеет право на получение от государственных органов, органов местного самоуправления информации, непосредственно касающейся прав и обязанностей этой организации, а также информации, необходимой в связи с взаимодействием с указанными органами при осуществлении этой организацией своей уставной деятельности.

Не может быть ограничен доступ к:

- нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления;
- информации о состоянии окружающей среды;
- информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюд-

жетных средств (за исключением сведений, составляющих государственную или служебную тайну);

- информации, накапливаемой в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией;
- иной информации, недопустимость ограничения доступа к которой установлена федеральными законами.

Государственные органы и органы местного самоуправления обязаны обеспечивать доступ к информации о своей деятельности на русском языке и государственном языке соответствующей республики в составе Российской Федерации в соответствии с федеральными законами, законами субъектов Российской Федерации и нормативными правовыми актами органов местного самоуправления. Лицо, желающее получить доступ к такой информации, не обязано обосновывать необходимость ее получения.

Решения и действия (бездействие) государственных органов и органов местного самоуправления, общественных объединений, должностных лиц, нарушающие право на доступ к информации, могут быть обжалованы в вышестоящий орган или вышестоящему должностному лицу либо в суд.

В случае если в результате неправомерного отказа в доступе к информации, несвоевременного ее предоставления, предоставления заведомо недостоверной или не соответствующей содержанию запроса информации были причинены убытки, такие убытки подлежат возмещению в соответствии с гражданским законодательством.

Предоставляется бесплатно информация:

- о деятельности государственных органов и органов местного самоуправления, размещенная такими органами в информационно-телекоммуникационных сетях;
- затрагивающая права и установленные законодательством Российской Федерации обязанности заинтересованного лица;
- иная установленная законом информация.

Установление платы за предоставление государственным органом или органом местного самоуправления информации о своей деятельности возможно только в случаях и на условиях, которые установлены федеральными законами.

Защищаемая информация — информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственниками информации. Собственниками информации могут быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

В последнее время, все большие объемы информации, в том числе и критически важной для отдельных людей, организаций или государств, хранятся, обрабатываются и передаются с использованием автоматизированных систем (АС) обработки информации. Система обработки информации — совокупность технических средств и программного обеспечения, а также методов обработки информации и действий персонала, необходимых для выполнения автоматизированной обработки информации. Объект информатизации — совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров.

Обеспечение информационной безопасности в большинстве случаев связано с комплексным решением трех задач:

– обеспечением доступности информации;
– обеспечением целостности информации;
– обеспечением конфиденциальности информации.

Именно доступность, целостность и конфиденциальность являются равнозначными и характеризуют информацию в целом (являются свойствами информации).

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

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

Роль доступности информации особенно проявляется в разного рода системах управления — производством, транспортом и т. п. Менее драматичные, но также весьма неприятные последствия — и материальные, и моральные — может иметь длительная недоступность информационных услуг, которыми пользуется большое количество

людей, например, продажа железнодорожных и авиабилетов, банковские услуги, доступ в информационную сеть Интернет и т. п.

Фактор времени в определении доступности информации в ряде случаев является очень важным, поскольку некоторые виды информации и информационных услуг имеют смысл только в определенный промежуток времени. Например, получение заранее заказанного билета на самолет после его вылета теряет всякий смысл. Точно так же получение прогноза погоды на вчерашний день не имеет никакого смысла, поскольку это событие уже наступило. В этом контексте весьма уместной является поговорка: «Дорога ложка к обеду».

Целостность информации условно подразделяется на статическую и динамическую. Статическая целостность информации предполагает неизменность информационных объектов от их исходного состояния, определяемого автором или источником информации. Динамическая целостность информации включает вопросы корректного выполнения сложных действий с информационными потоками, например, анализ потока сообщений для выявления некорректных, контроль правильности передачи сообщений, подтверждение отдельных сообщений и др.

Целостность является важнейшим аспектом информационной безопасности в тех случаях, когда информация используется для управления различными процессами, например техническими, социальными и т. д. Так, ошибка в управляющей программе приведет к остановке управляемой системы, неправильная трактовка закона может привести к его нарушениям, точно также неточный перевод инструкции по применению лекарственного препарата может нанести вред здоровью. Все эти примеры иллюстрируют нарушение целостности информации, что может привести к катастрофическим последствиям. Именно поэтому целостность информации выделяется в качестве одной из базовых составляющих информационной безопасности.

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

На втором месте по размерам ущерба (после непреднамеренных ошибок и упущений) стоят кражи и подлоги. По данным газеты *USA Today*, еще в 1992 г. в результате подобных противоправных действий с использованием персональных компьютеров американским организациям был нанесен общий ущерб в размере 882 млн долларов. Можно предположить, что реальный ущерб был намного больше, по-

скольку многие организации по понятным причинам скрывают такие инциденты; не вызывает сомнений, что в наши дни ущерб от такого рода действий вырос многократно.

В большинстве случаев виновниками оказывались штатные сотрудники организаций, отлично знакомые с режимом работы и мерами защиты. Это еще раз подтверждает опасность внутренних угроз, хотя говорят и пишут о них значительно меньше, чем о внешних.

Ранее проводилось различие между статической и динамической целостностью. С целью нарушения статической целостности злоумышленник (как правило, штатный сотрудник) может: ввести неверные данные; изменить данные.

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

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

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

Нарушение каждого из трех свойств информации (доступности, целостности, конфиденциальности) приводит к нарушению информационной безопасности в целом. Так, нарушение доступности приводит к отказу в доступе к информации, нарушение целостности приводит к фальсификации информации и, наконец, нарушение конфиденциальности приводит к раскрытию информации.

Выделение этих свойств (категорий) в качестве базовых составляющих информационной безопасности обусловлено необходимостью реализации комплексного подхода при обеспечении режима информационной безопасности.

Конфиденциальность информации — обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия её обладателя (Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»).

Взаимосвязь свойств информации представлена на рис. 1.3.

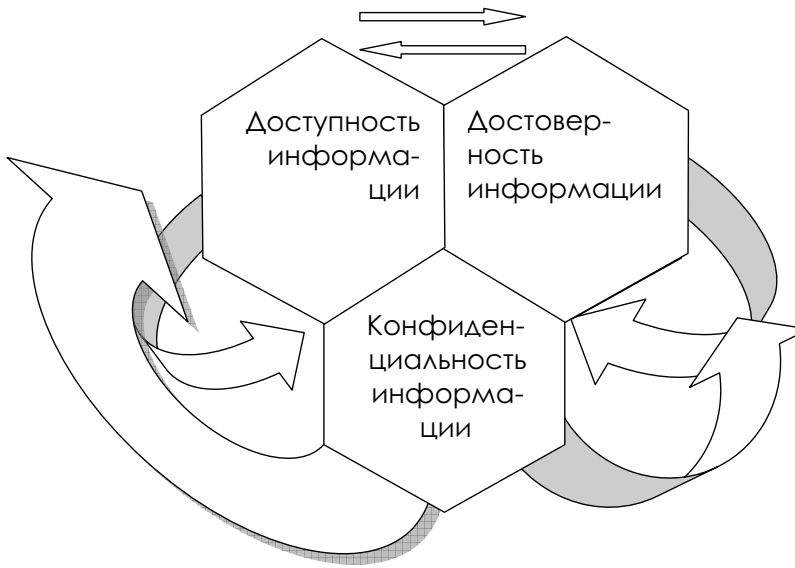


*Рис. 1.3.* Взаимосвязь свойств информации

В зависимости от конкретных условий, может решаться задача обеспечения комплексной безопасности объекта информатизации или защиты отдельных ресурсов — информационных, программных и т. д.

Информационные ресурсы (активы) — отдельные документы и отдельные массивы документов, документы и массивы документов, содержащиеся в информационных системах (библиотеках, архивах, фондах, банках данных, информационных системах других видов).

Рассматривая вопросы безопасности АС, можно говорить о наличии некоторых «желательных» состояний системы, через которые и описывается ее «защищенность» или «безопасность». Безопасность является таким же свойством системы, как надежность или производительность, и в последнее время ей уделяется все большее внимание.

Чтобы указать на причины выхода системы из безопасного состояния, вводятся понятия «угроза» и «уязвимость».

Угроза (безопасности информации) — совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Естественные угрозы — это угрозы, вызванные воздействием на АС объективных физических процессов, стихийных природных явлений, не зависящих от человека.

Естественные угрозы делятся на природные (стихийные бедствия, магнитные бури, радиоактивное излучение, осадки) и технические (отказы, сбои в работе технических средств, нарушение алгоритмов обработки информации).

Искусственные угрозы делятся на непреднамеренные (совершенные по незнанию и без злого умысла, из любопытности или халатности) и преднамеренные.

Источник угрозы безопасности информации — субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации.

Примерами угроз, связанных с деятельностью человека, могут служить удаление пользователем файла с важной информацией или пожар в здании из-за нарушения требований безопасности. В случае угроз, связанных с преднамеренными действиями человека, источник угрозы называют нарушителем или злоумышленником.

Уязвимость (информационной системы) — свойство информационной системы, обуславливающее возможность реализации угроз безопасности обрабатываемой в ней информации. Например, угроза потери информации из-за сбоя в сети электропитания реализуется, если в АС не применяются источники бесперебойного питания или средства резервного электроснабжения (это является уязвимостью).

Если говорить об информационных ресурсах, то реализация угрозы может привести к таким последствиям как получение информации людьми, которым она не предназначена, уничтожение или изменение информации, недоступность ресурсов для пользователей. Таким образом, могут быть выделены три основные угрозы безопасности.

Угроза конфиденциальности (угроза раскрытия) — это угроза, в результате реализации которой, конфиденциальная или секретная информация становится доступной лицу, группе лиц или какой-либо организации, которой она не предназначалась. Здесь необходимо по-

яснить разницу между секретной и конфиденциальной информацией. В отечественной литературе «секретной» обычно называют информацию, относящуюся к разряду государственной тайны, а «конфиденциальной» — персональные данные, коммерческую тайну и т. п.

Угроза целостности — угроза, в результате реализации которой информация становится измененной или уничтоженной. Необходимо отметить, что и в нормальном режиме работы АС данные могут изменяться и удаляться. Являются ли эти действия легальными или нет, должно определяться политикой безопасности. Политика безопасности — совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

Угроза отказа в обслуживании (угроза доступности) — угроза, реализация которой приведет к отказу в обслуживании клиентов АС, несанкционированному использованию ресурсов злоумышленниками по своему усмотрению.

Ряд авторов дополняют приведенную классификацию, вводя угрозу раскрытия параметров АС, включающей в себя подсистему защиты. Угроза считается реализованной, если злоумышленником в ходе нелегального исследования системы определены все ее уязвимости. Данную угрозу относят к разряду опосредованных: последствия ее реализации не причиняют какой-либо ущерб обрабатываемой информации, но дают возможность для реализации первичных (непосредственных) угроз.

**Таким образом, безопасность информации — это состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность. А защита информации может быть определена как деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.** Выделяются следующие направления защиты информации:

- правовая защита информации — защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением;
- техническая защита информации — защита информации, заключающаяся в обеспечении некриптографическими методами

безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств;

- криптографическая защита информации — защита информации с помощью ее криптографического преобразования;
- физическая защита информации — защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.

Защита информации осуществляется с использованием способов и средств защиты. Способ защиты информации — порядок и правила применения определенных принципов и средств защиты информации. Средство защиты информации — техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации. Отдельно выделяют:

– средства контроля эффективности защиты информации;
– средства физической защиты информации;
– криптографические средства защиты информации.

Защита информации от несанкционированного доступа — защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации.

Для защиты от несанкционированного доступа (НСД) к информации, как правило, используется идентификация, аутентификация и управление доступом. В дополнение к перечисленным, могут применяться и другие методы.

Идентификация — присвоение пользователям идентификаторов (уникальных имен или меток) под которыми система «знает» пользователя. Кроме идентификации пользователей, может проводиться идентификация групп пользователей, ресурсов АС и т. д. Идентификация нужна и для других системных задач, например, для ведения журналов событий. В большинстве случаев идентификация сопровождается аутентификацией. Аутентификация — установление подлинности — проверка принадлежности пользователю предъявленного им идентификатора. Например, в начале сеанса работы в АС пользова-

тель вводит имя и пароль. На основании этих данных система проводит идентификацию (по имени пользователя) и аутентификацию (сопоставляя имя пользователя и введенный пароль).

Управление доступом — метод защиты информации путем регулирования использования всех ресурсов системы.

Система идентификации и аутентификации является одним из ключевых элементов инфраструктуры защиты от НСД любой информационной системы. Обычно выделяют 3 группы методов аутентификации.

Аутентификация по наличию у пользователя уникального объекта заданного типа. В качестве примера можно привести аутентификацию с помощью смарт-карт или электронных 1T8B-ключей.

Аутентификация, основанная на том, что пользователю известна некоторая конфиденциальная информация. Например, аутентификация по паролю.

Аутентификация пользователя по его собственным уникальным характеристикам. Эти методы называются биометрическими. Биометрические методы аутентификации делят на статические и динамические.

Примеры аутентификации по статическим признакам — это проверка отпечатка пальца, рисунка радужной оболочки глаз, геометрии кисти руки, сравнение с фотографией и т. д. Достоинством этих методов является достаточно высокая точность. Но надо отметить, что подобные методы, как правило, требуют наличия специализированного оборудования (например, специальные сканеры) и имеют ограниченную область применения (например, при аутентификации по отпечатку пальца, из-за грязи на руке человек может не пройти аутентификацию, т. е. подобные методы неприменимы на стройках и на многих производствах).

Примеры динамической аутентификации — аутентификация по голосу (при произнесении заранее определенной фразы или произвольного текста), аутентификация по «клавиатурному почерку» (проверяются особенности работы пользователя на клавиатуре, такие как время задержки при нажатии клавиш в различных сочетаниях) и т. д.

Нередко используются комбинированные схемы аутентификации, объединяющие методы разных классов. Например, двухфакторная аутентификация — пользователь предъявляет системе смарт-карту и вводит пин-код для ее активации.

Паролями (пароль может быть использован многократно) проще реализовать и дешевле поддерживать безопасность АС, поэтому они более распространены.

Учетная запись пользователя — совокупность идентификатора, пароля и, возможно, дополнительной информации, служащей для описания пользователя. Учетные записи хранятся в базе данных парольной системы.

Парольная система — это программный или программно-аппаратный комплекс, реализующий функции идентификации и аутентификации пользователей компьютерной системы путем проверки паролей. В отдельных случаях подобная система может выполнять дополнительные функции, такие как генерация и распределение криптографических ключей и т. д. Как правило, парольная система включает в себя интерфейс пользователя, интерфейс администратора, базу учетных записей, модули сопряжения с другими компонентами подсистемы безопасности (подсистемой разграничения доступа, регистрации событий и т. д.).

Рассмотрим некоторые рекомендации по администрированию парольной системы, использующей многоразовые пароли.

Задание минимальной длины используемых в системе паролей. Это усложняет атаку путем подбора паролей. Как правило, рекомендуют устанавливать минимальную длину в 6–8 символов.

Установка требования использовать в пароле разные группы символов — большие и маленькие буквы, цифры, специальные символы. Это также усложняет подбор.

Периодическая проверка администраторами безопасности качества используемых паролей путем имитации атак, таких как подбор паролей «по словарю». При этом под компьютерной атакой понимается целенаправленное несанкционированное воздействие на информацию, на ресурс автоматизированной информационной системы или получение несанкционированного доступа к ним с применением программных или программно-аппаратных средств.

Установление максимального и минимального сроков жизни пароля, использование механизма принудительной смены старых паролей. При внедрении данной меры надо учитывать, что при невысокой квалификации пользователей, от администратора потребуются дополнительные усилия по разъяснению пользователям того, что «от них требует система».

Ограничение числа неудачных попыток ввода пароля (блокирование учетной записи после заданного числа неудачных попыток войти в систему). Данная мера позволяет защититься от атак путем подбора паролей. Но при необдуманном внедрении также может привести к дополнительным проблемам — легальные пользователи из-за ошибок ввода паролей по невнимательности могут блокировать свои учетные записи, что потребует от администратора дополнительных усилий.

Ведение журнала истории паролей, чтобы пользователи, после принудительной смены пароля, не могли вновь выбрать себе старый, возможно скомпрометированный пароль.

# 2. ХАРАКТЕРИСТИКИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОБЪЕКТЕ ЗАЩИТЫ, КЛАССИФИКАЦИЯ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

Информационная сфера играет все возрастающую роль в обеспечении жизнедеятельности общества. Через эту сферу реализуется значительная часть угроз национальной безопасности государства.

Одним из основных источников угроз безопасности информации являются деятельность иностранных разведывательных и специальных служб, преступных сообществ, организаций, групп, организаций и противозаконная деятельность отдельных лиц, направленная на сбор или хищение ценной информации, закрытой для доступа посторонних лиц. Причем в последние годы приоритет в данной сфере деятельности смещается в экономическую область.

Прежде чем рассмотреть характеристики угроз, целесообразно дать определение автоматизированной системы.

Автоматизированная система (АС) — система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

С учетом структуры АС при рассмотрении вопроса угроз необходим комплексный подход, а именно целесообразно рассматривать: уг-

розы персоналу; средствам автоматизации и информационным технологиям.


*Рис. 2.1.* Структурная схема автоматизированной системы

На рынке России представлен арсенал самых современных технических средств промышленного шпионажа, которые находят широкое применение на практике. К ним относятся: визуально-оптические, фотографические, телевизионные, тепловизионные (инфракрасные), акустические, радио, радиотехнические и некоторые другие средства разведки.

Основными направлениями технической защиты информации от утечки по техническим каналам являются:

- предотвращение утечки обрабатываемой информации за счет побочных электромагнитных излучений и наводок, создаваемых функционирующими техническими средствами, а также за счет электроакустических преобразований;
- выявление внедренных на объекты и в технические средства электронных устройств перехвата информации (закладных устройств);
- предотвращение перехвата с помощью технических средств речевой информации из помещений и объектов.

Технический канал утечки информации (ТКУИ) — совокупность объектов разведки, которые содержат информацию технических

средств разведки (ТСР), с помощью которых добывается информация, и физической среды, в которой распространяется информативный сигнал (циркулируют данные).

В связи с тем, что информационные процессы, связанные с обменом информацией, ее накоплением, хранением, модернизацией, записью, копированием и т. д. используют различные типы носителей, потенциальные угрозы безопасности информации должны рассматриваться применительно ко всем возможным классам носителей информации. Причем в качестве носителей должны рассматриваться не только физические (бумага, магнитные носители, ПЗУ, ОЗУ и др.), но и линии связи (радио — проводные, волоконно-оптические и др.) и среда распространения (твердая, водная, воздушная).

Как известно, под угрозой безопасности информации понимается возможность возникновения такого явления или события, следствием которого является нежелательное воздействие на носитель информации, частичная или полная утрата информации либо ее утечка или разглашение.

Особенностью угроз безопасности информации при утечке по техническим каналам является реализация этих угроз непосредственно через элементы ТКУИ. Угрозы не существуют отдельно от каналов (так как они зависят от характеристик и параметров канала).

Угрозы безопасности информации от утечки по техническим каналам разделяют:

1) по природе проявления:
- объективные
- субъективные.

2) по источнику угроз:
- обусловленные деятельностью людей;
- работой технических средств;
- работой заложенных в информационную систему моделей, алгоритмов, программ;
- технологическими схемами обработки информации;
- состоянием внешней среды;

3) по признаку реализации;
- преднамеренные (искусственно созданные, в том числе с применением закладных устройств);
- непреднамеренные;

4) по месту реализации по отношению к объекту информатизации:

– внешние;
– внутренние.

5) по видам используемых средств:
– применение технических средств;
– применение программных средств;
– применение программно-технических средств;

б) по виду проявления;
– приводящие к съему информации;
– приводящие к перехвату информации;
– приводящие к разглашению информации;

7) по виду нарушения безопасности информации при утечке по техническому каналу:
– приводящие к нарушению конфиденциальности информации.

Типовой объект информатизации (ОИ) характеризуются видом информации (сигналов), циркулирующей на нем и оснащением — наличием основных технических средств и систем (ОТСС), обрабатывающих эту информацию, а также вспомогательных технических средств и систем (ВТСС), находящихся в выделенном помещении либо на ОИ, обладающем характеристиками защищенности информации в силу своего конструкционного исполнения (экранированность, поглощение, затухание в пределах контролируемой зоны) во время обработки информации.

ОИ могут иметь сложную конфигурацию, но в целом их можно разделить на:

- выделенные помещения, в которых ведутся закрытые переговоры;
- выделенные помещения, в которых проводятся лекции, совещания, семинары и другие мероприятия по обсуждению информации закрытого характера;
- выделенные помещения, в которых производится обработка информации (обобщение, накопление, систематизация, модернизация) закрытого характера, в том числе с использованием технических средств;
- выделенные помещения, в которых производится обработка информации (обобщение, накопление, систематизация, модернизация, передача, прием и т. д.) закрытого характера и имеющих линии связи с выходом за пределы;
- ОИ, на которых проводится обработка информации (обобщение, накопление, систематизация, модернизация, передача,

прием и т. д.) закрытого характера и объединенные локальной вычислительной сетью;

- ОИ, на которых проводится обработка информации (обобщение, накопление, систематизация, модернизация, передача, прием и т. д.) закрытого характера и объединенные распределительной вычислительной сетью.

Угроза может быть реализована на любом из этапов жизненного цикла ОИ в процессе разработки ввода в эксплуатацию, эксплуатации по любому из возможных ТКУИ, характеризующихся присутствием соответствующих физических явлений.

Каждое техническое средство обработки информации (ТСОИ) содержит большое количество токопроводящих цепей различной протяженности и конфигурации, по которым циркулируют управляющие и информативные электрические сигналы различного вида (аналоговые, импульсные). Эти сигналы являются причиной возникновения электрических и магнитных полей рассеивания, которые зависят от:

- характеристик сигналов, циркулирующих в средствах объекта информации;
- конфигурации и излучающих свойств функциональных блоков, узлов, элементов (транзисторов, диодов, микросхем), токопроводящих цепей и их взаимного расположения;
- конфигурации и излучающих свойств токопроводящих конструкций (корпусов, панелей, крепежных конструкций и т. п.) и их взаимного расположения.

В силу этого частотно-пространственные распределения поля, величина его уровня зависят от многих факторов и имеют индивидуальный случайный характер для каждого ТСОИ. Уровни ПЭМИН ТСОИ могут принимать значения от единиц мкВ до сотни мкВ в диапазоне частот от нескольких Гц до нескольких ГГц. Критерием оценки возможности утечки информации является наличие в зоне возможного перехвата информативных сигналов с достаточным для ведения перехвата уровнем.

Паразитная генерация (возбуждение) усилителей различных диапазонов возможна за счет возникновения паразитных обратных связей на какой-либо частоте в элементах и узлах ТСОИ. Она может происходить за счет конструктивных недостатков схем, а также может быть искусственно вызвана. Излучения на частоте генерации, как правило, модулированы информативным сигналом. В таких случаях

ТСОИ является радиоретранслирующим устройством, работающим на частоте возбуждения. Диапазон частот, на котором возможна генерация, определяется частотными характеристиками элементной базы и может находиться в пределах от десятков кГц до десятков ГГц при уровне от десятков мкВ/м до сотни мкВ/м.

Некоторые элементы ТСОИ (трансформаторы, дроссели, датчики) способны изменять свои параметры (индуктивность, емкость, сопротивление) под воздействием акустического поля. При этом изменение параметров элементов приводит к возникновению переменной ЭДС (ε), т. е. наблюдается проявление микрофонного эффекта. Значение амплитуды ЭДС пропорционально зависит от силы воздействующего сигнала (p – ε), где p — это сила звука. Это приводит к появлению в цепях ТСОИ информативных электрических сигналов. Уровень таких сигналов может достигать уровня сигналов, возникающих в электродинамических или емкостных микрофонах.

Уровень и частотные характеристики наведенных сигналов определяются параметрами токопроводящих цепей и конструкций (экранирование, конфигурация, протяженность, тип проводящего и изолирующего материала, удаленность от источника ПЭМИ) и зависит от большого количества апостериорных факторов.

Информативные сигналы в цепи питания могут быть обнаружены вследствие того, что среднее значение тока в каскадах усилителей зависит от амплитуды изменения тока, потребления нагрузки, изменению информативного сигнала.

Кроме того, токи усиливаемых информативных сигналов замыкаются через источники электропитания, создавая на его внутреннем сопротивлении падение напряжения, которое может быть обнаружено в питающей линии.

Если для первого случая характерным является присутствие в цепи амплитудной огибающей информативного сигнала из-за инерционности и сглаживающих свойств узлов блоков питания, то для второго случая характерно проявление в питающей линии амплитудно-временной реализации информативного сигнала.

В системах заземления наводятся ЭДС и информативные сигналы, которые распространяясь по заземляющим проводам создают опасность утечки информации. Значение амплитуды опасного сигнала определяется возвратными токами, обусловленными сопротивлением и конфигурацией заземления, а также проводимостью почвы.

Существует возможность модуляции информационным сигналом навязываемого ВЧ сигнала с последующим распределением. (Навязывание может производится по проводным линиям.)

Не исключается возможность акустического излучения информативного речевого сигнала или сигнала, обусловленного функционированием ТСОИ.

Вибрационные сигналы, возникают посредством преобразования информативного акустического сигнала при воздействии его на строительные конструкции и инженерно-строительные коммуникации.

Технические каналы утечки информации классифицируются следующим образом.

Электромагнитные:

- перехват ПЭМИ элементов ТСОИ;
- перехват ЭМИ на частотах работы ВЧ генераторов в ТСОИ и ВТСС;
- перехват ЭМИ на частотах самовозбуждения усилителей низкой частоты ТСОИ.

Электрические:

- съем наводок ЭМИ ТСОИ с соединительных линий ВТСС и посторонних проводников;
- съем информативных сигналов с линий электропитания ТСОИ;
- съем информативных сигналов с цепи заземления ТСОИ и ВТСС;
- съем информации путем установки в ТСОИ электронных устройств перехвата информации, комплексированных с устройствами передачи информации по радиоканалам.

Параметрические:

- перехват информации путем ВЧ облучения ТСОИ.

Технические каналы утечки акустической (речевой) информации.

Под акустической понимается информация, носителем которой являются акустические сигналы. В том случае, если источником информации является человеческая речь, акустическая информация называется речевой.

Воздушные:

- перехват акустических сигналов микрофонами, комплексированными с устройствами передачи информации по радиоканалу;
- перехват акустических сигналов микрофонами, комплексированными с устройствами передачи информации по сети электропитания;

– перехват акустических сигналов микрофонами, комплексированными с устройствами передачи информации по оптическому каналу в ИК диапазоне;
– перехват акустических сигналов микрофонами, комплексированными с устройствами передачи информации по телефонным линиям;
– перехват акустических сигналов микрофонами, комплексированными с устройствами их подключения к телефонным линиям по сигналу вызова от внешнего телефонного абонента;
– перехват акустических сигналов микрофонами, комплексированными с устройствами передачи информации по трубам водоснабжения, отопления, металлоконструкциям.

Электроакустические:
– перехват акустических колебаний через ВТСС, обладающие микрофонным эффектом, путем подключения их к соединительным линиям;
– перехват акустических колебаний через ВТСС, путем ВЧ-навязывания.

Вибрационные:
– перехват акустических сигналов с помощью электронных стетоскопов;
– перехват акустических сигналов электронными стетоскопами, комплексированными с устройствами перехвата информации по радиоканалу, оптическому каналу в ИК диапазоне, по трубам водоснабжения, отопления, металлоконструкциям и т. д.

Параметрические (акустические):
– перехват акустического сигнала путем приема и детектирования ПЭМИН (на частотах ВЧ генераторов) ТСОИ и ВТСС при модуляции информативным сигналом;
– перехват акустического сигнала путем ВЧ облучения специальных полуактивных закладных устройств.

Оптико-электронный (лазерный):
– перехват акустического сигнала путем лазерного зондирования оконных стекол.

ТКУИ, передаваемой по каналам связи.

Перехват информации, передаваемой по каналам радио- и радиорелейной связи (электромагнитный канал). Перехват электромагнитных излучений на частотах работы передатчиков систем и средств связи.

Съем информации, передаваемой по кабельным линиям связи:
– электрический — съем информации, передаваемой путем контактного подключения к кабельным линиям связи;
– индукционный — бесконтактный съем информации с кабельных линий связи.

Каналы скрытого видео наблюдения и съемки.

Наблюдение за объектом (видовая информация):

1) днем:
- наблюдение за объектами с использованием оптических приборов (монокуляров, подзорных труб, биноклей, телескопов);
- наблюдение за объектами с использованием телевизионных систем, в т. ч. с устройствами передачи изображения по радиоканалу;

2) ночью:
- наблюдение за объектами с использованием приборов ночного видения; — наблюдение за объектами с использованием телевизионных систем, в т. ч. комплексированных с приборами ночного видения;
- наблюдение за объектами с использованием телевизионных систем.

Съемка объектов:

1) днем:
- съемка объектов с использованием фотоаппаратов;
- съемка объектов с использованием телевизионных систем, комплексированных с портативными устройствами видеозаписи (передачи изображения по радиоканалу);

2) ночью:
- съемка объектов с использованием фотоаппаратов, комплексированных с прибором ночного видения;
- съемка объектов с использованием телевизионных систем, в т. ч. комплексированных с прибором ночного видения и портативными устройствами видеозаписи (передачи изображения по радиоканалу);
- съемка объектов с использованием систем, комплексированных с портативными устройствами видеозаписи;
- съемка (снятие копии) документов;
- съемка документов с использованием портативных фотоаппаратов.

При организации работ по защите информации от утечки по техническим каналам на объектах ТСОИ можно выделить три этапа.

Первый этап — подготовка к реконструкции (капитальному ремонту, строительству) объекта.

Второй этап — период проведения работ по реконструкции объекта.

Третий этап — период эксплуатации объекта.

На первом этапе с привлечением соответствующих специалистов проводится оценка обстановки на объекте и вблизи от него, изучается необходимая информация.

При этом устанавливается:

– когда построен объект, какие организации привлекались для строительства, какие учреждения в нем располагались;
– условия расположения объекта и всех помещений, какие организации занимают смежные помещения, режимы их посещения.

Далее проводится оценка информации, представляющей интерес для противника, определяются помещения, а также технические системы и средства, подлежащие защите.

Для анализа возможных технических каналов утечки на объекте изучаются:

- план прилегающей к объекту местности в радиусе до 1000 м с указанием принадлежности зданий, особенно находящихся в прямой видимости из окон помещений, подлежащих защите, мест стоянок автомашин, а также расположения трансформаторной подстанции;
- поэтажные планы здания с указанием всех помещений (смежных с защищаемыми), характеристик стен, перекрытий и материалов отделки;
- план-схема инженерных коммуникаций всего объекта, включая систему вентиляции;
- план-схема системы заземления объекта, с указанием места расположения заземлителя;
- план-схема системы электропитания здания с указанием места расположения разделительного трансформатора, всех щитов и разводных коробок;
- план-схема прокладки телефонных линий связи с указанием мест расположения распределительных коробок и установки телефонных аппаратов;
- план-схема систем охранной и пожарной сигнализации с указанием мест установки и типов датчиков, а также распределительных коробок.

Целесообразно провести технический контроль по оценке реальных экранирующих свойств конструкций здания и звукоизоляции помещений с целью учета их результатов при выработке мер защиты ТСОИ и выделенных помещений.

По результатам анализа делается вывод о том, какие потенциальные каналы утечки информации существуют на объекте, и разрабатываются требования и рекомендации по защите информации, которые должны быть включены в техническое задание на разработку технического проекта.

Поиск и обнаружение закладных устройств может осуществляться визуально, а также с использованием специальной аппаратуры.

Метод поиска закладных устройств во многом определяется использованием той или иной аппаратуры контроля. К основным методам поиска закладных устройств можно отнести:

- специальное обследование выделенных помещений;
- поиск радиозакладок с использованием индикаторов поля, радиочастотомеров и интерсепторов;
- поиск радиозакладок с использованием программно-аппаратных комплексов контроля;
- поиск портативных звукозаписывающих устройств с использованием детекторов диктофонов (по наличию их побочных электромагнитных излучений генераторов подмагничивания и электродвигателей);
- поиск портативных видеозаписывающих устройств с использованием детекторов видеокамер (по наличию их побочных электромагнитных излучений генераторов подмагничивания и электродвигателей видеокамер);
- поиск закладок с использованием нелинейных локаторов;
- проверка с использованием ВЧ пробника (зонда) линий электропитания, радиотрансляции и телефонной связи;
- измерение параметров линий электропитания телефонных линий связи и т. д.;
- проведение тестового «прозвона» всех телефонных аппаратов, установленных в проверяемом помещении, с контролем прохождения всех вызванных сигналов АТС.

Простейшими и наиболее дешевыми обнаружителями радиоизлучений закладных устройств являются индикаторы электромагнитного поля, которые световым или звуковым сигналом сигнализируют о наличии в точке расположения антенны электромагнитного поля с

напряженностью выше пороговой. Более сложные из них — частотомеры — обеспечивают измерение несущей частоты наиболее «сильного «в точке приема сигнала.

Для обнаружения закладных устройств в ближней зоне могут использоваться и специальные приборы называемые интерсепторами. Интерсептор автоматически настраивается на частоту более мощного сигнала и осуществляет его детектирование. Некоторые интерсепторы позволяют не только производить ручной или автоматический захват радиосигнала, осуществлять его детектирование и прослушивать через динамик, но и определять частоту обнаруженного сигнала и вид модуляции.

Чувствительность обнаружителей поля мала, поэтому они позволяют обнаружить излучение радиозакладок в непосредственной близости от них.

Более высокую чувствительность имеют специальные радиоприемники с автоматизированным сканированием радиодиапазона (сканерные приемники или сканеры). Они обеспечивают поиск в диапазоне частот перекрывающем частоты почти всех применяемых радиозакладок — от десятков кГц до единиц ГГц. Лучшими возможностями по поиску радиозакладок обладают анализаторы спектра. Кроме перехвата излучений закладных устройств они позволяют анализировать и их характеристики.

Возможность сопряжения сканирующих приемников с переносным компьютером послужило основой для создания автоматизированных комплексов для поиска радиозакладок (так называемых программно-аппаратных комплексов контроля). Кроме программно-аппаратных комплексов, построенных на базе сканирующих приемников и переносных компьютеров, для поиска закладных устройств используются и специально разработанные многофункциональные комплексы, например, как «OSCOR-500».

Специальные комплексы и аппаратура для контроля проводных линий позволяют проводить измерение параметров (напряжений, токов, сопротивлений и т. д.) телефонных, слаботочных линий и линий электропитания, а также выявлять в них сигналы закладных устройств.

Обнаружители пустот позволяют обнаружить возможные места установки закладных устройств в пустотах стен или других деревянных или металлических конструкциях.

Большую группу образуют средства обнаружения или локализации закладных устройств по физическим свойствам элементов элек-

трической схемы или конструкции. Такими элементами являются: полупроводниковые приборы, электропроводящие металлические детали конструкций и т. д. Из этих средств наиболее достоверные результаты обеспечивают средства для обнаружения полупроводниковых элементов по их нелинейным свойствам — нелинейные радиолокаторы.

Принцип работы нелинейных радиолокаторов близок к принципу работы радиолокационных станций, широко применяемых для радиолокационной разведки объектов. Существенное отличие в том, что если приемник радиолокационной станции принимает от объекта зондирующий сигнал (эхо-сигнал) на частоте излучаемого сигнала, то приемник нелинейного локатора принимает 2-ю и 3-ю гармоники отраженного сигнала. Появление в отраженном сигнале этих гармоник обусловлено нелинейностью характеристик полупроводников.

Металлоискатели (металлодетекторы) реагируют на наличие в зоне поиска электропроводных материалов, прежде всего металлов, и позволяют обнаруживать корпуса или другие металлические элементы закладки.

Переносные рентгеновские установки применяются для просвечивания предметов, назначение которых не удается выявить без их разборки прежде всего тогда, когда она невозможна без разрушения найденного предмета.

# 3. ПРАВОВЫЕ ОСНОВЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Важнейшими для обеспечения информационной безопасности являются правовые методы. Они предусматривают разработку комплекса нормативных правовых актов, регламентирующих отношения в информационной сфере (среде), и нормативных методических документов по вопросам обеспечения информационной безопасности, т. е. создание нормативно-правового обеспечения в области информационной безопасности.

Национальная политика и нормотворческая деятельность России в сфере информационных отношений и информационной безопасности строится, исходя из провозглашенных принципов открытости общества, свобод и прав граждан на информацию. Она имеет свои особенности, связанные с уровнем развития информационных техно-

логий, со сжатыми временными отрезками на нормотворческую деятельность и другими факторами, и в то же время широко использует международный опыт.

Наиболее важными направлениями нормотворческой деятельности, регулирующей отношения в области обеспечения информационной безопасности, являются:

- формирование института тайн: государственной, служебной, коммерческой, профессиональной и личной;
- разработка механизмов реализации прав граждан и организаций на получение, распространение и использование информации;
- создание и совершенствование системы обеспечения информационной безопасности (СОИБ) Российской Федерации;
- устранение противоречий в законодательстве;
- конкретизация правовых норм, устанавливающих ответственность за правонарушения в области обеспечения информационной безопасности РФ;
- разработка и принятие нормативных правовых актов Российской Федерации, устанавливающих ответственность юридических и физических лиц за несанкционированный доступ к информации, ее противоправное копирование, искажение и противозаконное использование, преднамеренное распространение недостоверной информации, противоправное раскрытие конфиденциальной информации, использование в преступных и корыстных целях служебной информации или информации, содержащей коммерческую тайну;
- законодательное закрепление приоритета развития национальных сетей связи и отечественного производства космических спутников связи;
- определение статуса организаций, предоставляющих услуги глобальных информационно-телекоммуникационных сетей на территории РФ и правовое регулирование деятельности этих организаций.

Нормативно-правовое обеспечение России, обеспечивающее защищенность ее национальных интересов в информационной сфере, формируется в результате деятельности исполнительной и законодательной властей и включает в себя три основных компонента: нормативно-правовое обеспечение защиты прав и свобод человека и гражданина, реализуемых в информационной сфере; нормативно-право-

вое обеспечение в области развития российской информационной инфраструктуры и эффективного использования отечественных информационных ресурсов; нормативно-правовое обеспечение безопасности информационных и телекоммуникационных систем и информационных ресурсов страны.

Нормативно-правовую базу в области защиты информации и обеспечения информационной безопасности образуют: Конституция Российской Федерации; международные нормативные правовые акты в этой области, признанные Российской Федерацией; федеральные законы и кодексы Российской Федерации; указы Президента Российской Федерации; постановления и другие подзаконные нормативные правовые акты Правительства Российской Федерации; положения, стандарты, руководящие документы, инструкции, рекомендации, нормативно-технические и методические документы ФСТЭК (Гостехкомиссии) России, органов федеральной исполнительной власти: ФСБ, МВД, других министерств и ведомств.

На первом этапе деятельности по созданию нормативно-правового обеспечения работ в стране в области информатизации, зашиты информации и государственной тайны был издан ряд указов Президента Российской Федерации и приняты базовые федеральные законы. В настоящее время отношения в сфере информационной безопасности регулируются более чем 80 законами. К важной группе нормативных актов относятся руководящие и методические документы ФСТЭК (Гостехкомиссии) России, определяющие требования к классам защищенности средств вычислительной техники и автоматизированных систем от НСД к информации.

В современном мире открытых сетей нормативно-правовая база России должна быть согласована с международной практикой, т. е. отечественные стандарты и сертификационные нормативы должны быть приведены в соответствие с международным уровнем информационных технологий.

Руководствуясь перечисленными выше нормативными правовыми актами и документами в каждой отрасли разрабатываются нормативные методические документы, конкретизирующие вопросы обеспечения информационной безопасности (ИБ) ее корпоративных систем и сетей.

Нормативно-правовое обеспечение включает в себя: разработку нормативно-методической базы обеспечения информационной безопасности; проведение единой технической политики в области обеспе-


*Рис. 3.1.* Структура правовой базы защиты информации на предприятии

чения информационной безопасности; разработку комплекса мероприятий и документов по обеспечению информационной безопасности в чрезвычайных ситуациях; регламентацию проведения аттестации и сертификационных испытаний.

Схематично правовая база защиты информации на предприятии представлена на рис. 3.1.

# 4. ОРГАНИЗАЦИОННЫЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Особую роль в обеспечении информационной безопасности (ИБ) играют организационные меры. Они направлены, прежде всего, на разработку политики безопасности, т. е. совокупности документированных управленческих решений, норм и правил обеспечения информационной безопасности отрасли и ее корпоративных систем и сетей; создание и совершенствование организационной структуры системы обеспечения информационной безопасности.

К другим общим организационным мерам относятся:

- сертификация автоматизированных информационных систем и сетей, средств защиты информации и контроля за их эффективностью;
- категорирование информационных объектов по степени важности и конфиденциальности защищаемой информации;
- аттестация объектов по выполнению требований обеспечения безопасности информации при работе со сведениями, составляющими государственную тайну;
- введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования информационных средств, подлежащих защите и др.

Политика безопасности определяет стратегию отрасли в области ИБ, а также меру внимания и количество ресурсов, которое руководство считает целесообразным выделить на решение проблемы обеспечения ИБ корпоративной сети (КС). Разработка политики безопасности требует учета специфики конкретных объектов защиты.

Примером содержания политики безопасности может служить Британский стандарт B5 7799:1995, описывающий основные положения политики безопасности. Стандарт рекомендует включать в документ, характеризующий политику безопасности организации, следующие разделы:

– вводный, подтверждающий озабоченность высшего руководства проблемами информационной безопасности;
– организационный, содержащий описание подразделений, комиссий, групп и т. д., отвечающих за работу в области ИБ корпоративных систем и сетей;
– классификационный, описывающий имеющиеся в организации информационные ресурсы и необходимый уровень их защиты;
– штатный, характеризующий меры безопасности, применяемые к персоналу (организация обучения и переподготовки персонала, порядок реагирования на нарушения режима ИБ корпоративной сети и др.);
– освещающий вопросы физической защиты;
– описывающий правила разграничения доступа к защищаемой информации;
– характеризующий порядок разработки и сопровождения;
– управляющий, описывающий подходы к управлению средствами зашиты, контролю за выполнением политики безопасности, восстановлению нарушенного процесса функционирования;

– юридический, подтверждающий соответствие политики безопасности действующему законодательству.

Политика безопасности строится на основе анализа рисков. Под риском понимается произведение вероятности (возможности) активизации угрозы ИБ на величину, характеризующую возможный ущерб пользователю. Когда риски проанализированы и стратегия защиты определена, составляется программа, реализация которой должна обеспечить ИБ корпоративной сети.

В организационной структуре создаваемой системы обеспечения информационной безопасности предприятия могут выделяться следующие уровни:

- руководство, коллегия министерства;
- подразделения информационной безопасности департаментов, управлений и организаций Министерства, главный конструктор систем обеспечения информационной безопасности, головная научно-исследовательская организация;
- региональные внедренческие центры, подразделения информационной безопасности в службах связи и ИВЦ, кафедры и подразделения информационной безопасности вузов;
- подразделения (администраторы) безопасности корпоративных систем и сетей различного уровня.

Организационное обеспечение также включает в себя:

– контроль за соблюдением требований действующих и вновь вводимых руководящих документов по защите информации;
– координацию деятельности подразделений защиты информации в отрасли с департаментами, управлениями, организациями и предприятиями и другими органами.

## 5. ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Задачей технических средств защиты информации является либо ликвидация каналов утечки информации, либо снижение качества получаемой злоумышленником информации. Основным показателем качества речевой информации считается разборчивость — слоговая, словесная, фразовая и др. Чаще всего используют слоговую разборчивость, измеряемую в процентах. Принято считать, что качество аку-

стической информации достаточное, если обеспечивается около 40 % слоговой разборчивости. Если разобрать разговор практически невозможно (даже с использованием современных технических средств повышения разборчивости речи в шумах), то слоговая разборчивость соответствует около 1–2 %.

Предупреждение утечки информации по акустическим каналам сводится к пассивным и активным способам защиты. Соответственно, все приспособления защиты информации можно смело разделить на два больших класса — пассивные и активные. Пассивные — измеряют, определяют, локализуют каналы утечки, ничего не внося при этом во внешнюю среду. Активные — «зашумляют», «выжигают», «раскачивают» и уничтожают всевозможные спецсредства негласного получения информации.

Пассивное техническое средство защиты — устройство, обеспечивающее скрытие объекта защиты от технических способов разведки путем поглощения, отражения или рассеивания его излучений. К пассивным техническим средствам защиты относятся экранирующие устройства и сооружения, маски различного назначения, разделительные устройства в сетях электроснабжения, защитные фильтры и т. д. Цель пассивного способа — максимально ослабить акустический сигнал от источника звука, например, за счет отделки стен звукопоглощающими материалами.

По результатам анализа архитектурно-строительной документации формируется комплекс необходимых мер по пассивной защите тех или иных участков. Перегородки и стены по возможности должны быть слоистыми, материалы слоев — подобраны с резко отличающимися акустическими характеристиками (например, бетон-поролон). Для уменьшения мембранного переноса желательно, чтобы они были массивными. Кроме того, разумнее устанавливать двойные двери с воздушной прослойкой между ними и уплотняющими прокладками по периметру косяка. Для защиты окон от утечки информации их лучше делать с двойным остеклением, применяя звукопоглощающий материал и увеличивая расстояние между стеклами для повышения звукоизоляции, использовать шторы или жалюзи. Желательно оборудовать стекла излучающими вибродатчиками. Различные отверстия во время ведения конфиденциальных разговоров следует перекрывать звукоизолирующими заслонками.

Другим пассивным способом пресечения утечки информации является правильное устройство заземления технических средств пере-

дачи информации. Шина заземления и заземляющего контура не должна иметь петель, и ее рекомендуется выполнять в виде ветвящегося дерева. Магистрали заземления вне здания следует прокладывать на глубине около 1,5 м, а внутри здания — по стенам или специальным каналам (для возможности регулярного осмотра). В случае подключения к магистрали заземления нескольких технических средств соединять их с магистралью нужно параллельно. При устройстве заземления нельзя применять естественные заземлители (металлические конструкции зданий, имеющие соединение с землей, проложенные в земле металлические трубы, металлические оболочки подземных кабелей и т. д.).

Так как обычно разнообразные технические приборы подключены к общей сети, то в ней возникают различные наводки. Для защиты техники от внешних сетевых помех и защиты от наводок, создаваемых самой аппаратурой, необходимо использовать сетевые фильтры. Конструкция фильтра должна обеспечивать существенное снижение вероятности возникновения внутри корпуса побочной связи между входом и выходом из-за магнитных, электрических либо электромагнитных полей. При этом однофазная система распределения электроэнергии должна оснащаться трансформатором с заземленной средней точкой, трехфазная — высоковольтным понижающим трансформатором.

Экранирование помещений позволяет устранить наводки от технических средств передачи информации (переговорных комнат, серверных и т. п.). Лучшими являются экраны из листовой стали. Но применение сетки значительно упрощает вопросы вентиляции, освещения и стоимости экрана. Чтобы ослабить уровни излучения технических средств передачи информации примерно в 20 раз, можно рекомендовать экран, изготовленный из одинарной медной сетки с ячейкой около 2,5 мм либо из тонколистовой оцинкованной стали толщиной 0,51 мм и более. Листы экранов должны быть между собой электрически прочно соединены по всему периметру. Двери помещений также необходимо экранировать, с обеспечением надежного электроконтакта с дверной рамой по всему периметру не реже, чем через 10–15 мм. При наличии в помещении окон их затягивают одним или двумя слоями медной сетки с ячейкой не более 2 мм. Слои должны иметь хороший электроконтакт со стенками помещения.

Активное техническое средство защиты — устройство, обеспечивающее создание маскирующих активных помех (или имитирующих

их) для средств технической разведки или нарушающие нормальное функционирование средств негласного съема информации. Активные способы предупреждения утечки информации можно подразделить на обнаружение и нейтрализацию этих устройств.

К активным техническим средствам защиты относятся также различные имитаторы, средства постановки аэрозольных и дымовых завес, устройства электромагнитного и акустического зашумления и другие средства постановки активных помех. Активный способ предупреждения утечки информации по акустическим каналам сводится к созданию в «опасной» среде сильного помехового сигнала, который сложно отфильтровать от полезного.

Современная техника подслушивания дошла до такого уровня, что становится очень сложно обнаружить приборы считывания и прослушивания. Самыми распространенными методами выявления закладочных устройств являются: визуальный осмотр; метод нелинейной локации; металлодетектирование; рентгеновское просвечивание.

Проводить специальные меры по обнаружению каналов утечки информации и дорого, и долго. Поэтому в качестве средств защиты информации часто выгоднее использовать устройства защиты телефонных переговоров, генераторы пространственного зашумления, генераторы акустического и виброакустического зашумления, сетевые фильтры. Для предотвращения несанкционированной записи переговоров используют устройства подавления диктофонов.

Подавители диктофонов (также эффективно воздействующие и на микрофоны) применяют для защиты информации с помощью акустических и электромагнитных помех. Они могут воздействовать на сам носитель информации, на микрофоны в акустическом диапазоне, на электронные цепи звукозаписывающего устройства. Существуют стационарные и носимые варианты исполнения различных подавителей.

В условиях шума и помех порог слышимости для приема слабого звука возрастает. Такое повышение порога слышимости называют акустической маскировкой. Для формирования виброакустических помех применяются специальные генераторы на основе электровакуумных, газоразрядных и полупроводниковых радиоэлементов.

На практике наиболее широкое применение нашли генераторы шумовых колебаний. Шумогенераторы первого типа применяются для подавления непосредственно микрофонов как у радиопередающих устройств, так и у диктофонов, т. е. такой прибор банально вырабатывает некий речеподобный сигнал, передаваемый в акустические

колонки и вполне эффективно маскирующий человеческую речь. Кроме того, такие устройства применяются для борьбы с лазерными микрофонами и стетоскопическим прослушиванием. Надо отметить, что акустические шумогенераторы — едва ли не единственное средство для борьбы с проводными микрофонами. При организации акустической маскировки следует помнить, что акустический шум создает дополнительный дискомфорт для сотрудников, для участников переговоров (обычная мощность генератора шума составляет 75–90 дБ), однако в этом случае удобство должно быть принесено в жертву безопасности.

Известно, что «белый» или «розовый» шум, используемый в качестве акустической маскировки, по своей структуре имеет отличия от речевого сигнала. На знании и использовании этих отличий как раз и базируются алгоритмы шумоочистки речевых сигналов, широко используемые специалистами технической разведки. Поэтому наряду с такими шумовыми помехами в целях активной акустической маскировки сегодня применяют более эффективные генераторы «речеподобных» помех, хаотических последовательностей импульсов и т. д. Роль устройств, преобразующих электрические колебания в акустические колебания речевого диапазона частот, обычно выполняют малогабаритные широкополосные акустические колонки. Они обычно устанавливаются в помещении в местах наиболее вероятного размещения средств акустической разведки.

«Розовый» шум — сложный сигнал, уровень спектральной плотности которого убывает с повышением частоты с постоянной крутизной, равной 3–6 дБ на октаву во всем диапазоне частот. «Белым» называется шум, спектральный состав которого однороден по всему диапазону излучаемых частот. То есть такой сигнал является сложным, как и речь человека, и в нем нельзя выделить какие-то преобладающие спектральные составляющие. «Речеподобные» помехи формируются путем микширования в различных сочетаниях отрезков речевых сигналов и музыкальных фрагментов, а также шумовых помех, или из фрагментов самого скрываемого речевого сигнала при многократном наложении с различными уровнями (наиболее эффективный способ).

Системы ультразвукового подавления излучают мощные неслышимые человеческим ухом ультразвуковые колебания (около 20 кГц). Данное ультразвуковое воздействие приводит к перегрузке усилителя низкой частоты диктофона и к значительным искажениям записы-

ваемых (передаваемых) сигналов. Но опыт использования этих систем показал их несостоятельность. Интенсивность ультразвукового сигнала оказывалась выше всех допустимых медицинских норм воздействия на человека. При снижении интенсивности ультразвука невозможно надежно подавить подслушивающую аппаратуру.

Акустический и виброакустический генераторы вырабатывают шум (речеподобный, «белый» или «розовый») в полосе звуковых сигналов, регулируют уровень шумовой помехи и управляют акустическими излучателями для постановки сплошной шумовой акустической помехи. Вибрационный излучатель служит для постановки сплошной шумовой вибропомехи на ограждающие конструкции и строительные коммуникации помещения. Расширение границ частотного диапазона помеховых сигналов позволяет снизить требования к уровню помехи и снизить словесную разборчивость речи.

На практике одну и ту же поверхность приходится зашумлять несколькими виброизлучателями, работающими от разных, некоррелированных друг с другом источников помеховых сигналов, что явно не способствует снижению уровня шумов в помещении. Это связано с возможностью использования метода компенсации помех при подслушивании помещения. Данный способ заключается в установке нескольких микрофонов и двух- или трехканальном съеме смеси скрываемого сигнала с помехой в пространственно разнесенных точках с последующим вычитанием помех.

Электромагнитный генератор (генератор второго типа) наводит радиопомехи непосредственно на микрофонные усилители и входные цепи диктофона. Данная аппаратура одинаково эффективна против кинематических и цифровых диктофонов. Как правило, для этих целей применяют генераторы радиопомех с относительно узкой полосой излучения, чтобы снизить воздействие на обычную радиоэлектронную аппаратуру (они практически не оказывают воздействия на работу сотовых телефонов стандарта GSM, при условии, что связь по телефону была установлена до включения подавителя). Электромагнитную помеху генератор излучают направленно, обычно это конус 60–70°. А для расширения зоны подавления устанавливают вторую антенну генератора или даже четыре антенны.

Следует знать, что при неудачном расположении подавителей могут возникать ложные срабатывания охранной и пожарной сигнализации. Приборы с мощностью больше 5–6 Вт не проходят по медицинским нормам воздействия на человека.

# ЗАКЛЮЧЕНИЕ

Обеспечение информационной безопасности информационных систем является в настоящее время актуальной задачей. Проблемы информационной безопасности становятся все более сложными и практически значимыми в связи с массовым переходом информационных технологий на безбумажную автоматизированную основу.

Для нейтрализации потенциальных угроз требуется комплексный подход к построению системы безопасности охраняемых объектов с использованием технических, аппаратных, программных средств и организационных мероприятий защиты.

Эффективность системы безопасности существенно зависит от уровня подготовленности и выполнения руководством, сотрудниками организаций (предприятий) требований по вопросам защиты информации.

Разработанные материалы могут оказать помощь специалистам, связанным с информационными системами, а также всем, кто интересуется компьютерными информационными технологиями.

# ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АС — автоматизированная система
ВТСС — вспомогательные технические средства и системы
ВЦ — вычислительный центр
ВЧ — высокочастотный
ГТ — государственная тайна
ДКП — дискретное косинусное преобразование
ЗИ — защита информации
ИБ — информационная безопасность
ИВЦ — информационно- вычислительный центр
ИИБ — интегральная информационная безопасность
ИК — инфракрасный
ИС — информационная система
КИ — конфиденциальная информация
КС — корпоративная сеть
КСГ — контекстно-свободная грамматика
НЗБ — наименьший значащий бит
НСД — несанкционированный доступ
ОИ — объект информатизации
ОП — оперативная память
ОТСС — основные технические средства и системы
ПД — персональные данные
ПЗУ — постоянное запоминающее устройство
ПЭМИН — побочные электромагнитные излучения и наводки
СЗИ — средства защиты информации
СЗПД — система защиты персональных данных
СОИБ — система обеспечения информационной безопасности
ТКУИ — технический канал утечки информации
ТСОИ — технические средства обработки информации
ТСР — технические средства разведки
ФСТЭК — Федеральная служба по техническому и экспортному контролю
ЭДС — электродвижущая сила
ЭМИ — электромагнитный импульс

# БИБЛИОГРАФИЯ

1. Государственная тайна в Российской Федерации: учебно-методическое пособие. Изд. 2-е, перераб. и доп. / под ред. М. А. Вуса. СПб.: Изд-во Санкт-Петербургского университета, 2000. 409 с.

2. Организация и современные методы защиты информации / под общ. ред. С. А. Диева и А. Г. Шаваева. М.: Концерн «Банковский Деловой Центр», 1998. 472 с.

3. *Позняков Е. Н.* Защита объектов (рекомендации для руководящих и сотрудников служб безопасности). М.: Концерн «Банковский Деловой Центр», 1997. 224 с.

4. Рекомендации по повышению безопасности объектов. М.: ВНИИПО МВД РФ, 1995.

5. *Петраков А. В., Дорошенко П. С., Савлуков Н. В.* Охрана и защита современного предприятия. М.: Энергоатомиздат, 1999. 568 с.

6. *Волхонский В. В.* Устройства охранной сигнализации. СПб.: Экономис и культура, 1999. 272 с.

7. Вопросы обеспечения защиты коммерческой тайны при установлении внешнеэкономических и иных связей с иностранными организациями. М.: Минрадиопром, 1991.

8. *Ярочкин В. И.* Служба безопасности коммерческого предприятия. Организационные вопросы. М.: Ось-89, 1995.

9. Все о защите коммерческой информации: настольная книга для делового человека. М.: Махаон, 1992.

10. *Белов Е. Б., Лось В. П., Мещеряков Р. В., Шелупанов А. А.* Основы информационной безопасности. М.: Горячая линия — Телеком, 2006. 544 с.

11. *Яковлев В. В., Корниенко А. А.* Информационная безопасность и защита информации в корпоративных сетях железнодорожного транспорта. М., 2002.

# ПРИЛОЖЕНИЕ 1

## ПЕРЕЧЕНЬ ОСНОВНЫХ ДОКУМЕНТОВ, РЕГЛАМЕНТИРУЮЩИХ ДЕЯТЕЛЬНОСТЬ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ:

1. Федеральный закон Российской Федерации от 20 февраля 1995 г. N 24-ФЗ «Об информации, информатизации и защите информации».
2. Федеральный закон Российской Федерации от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации.
3. Закон Российской Федерации от 21 июля 1993 г. N 5485-1 «О государственной тайне».
4. Постановление Правительства Российской Федерации от 6 февраля 2010 г. N 63 «Об утверждении инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне».
4. Концепция информационной безопасности Российской Федерации.
5. Уголовный кодекс Российской Федерации (ст. 272, 273, 274, 275, 276, 283, 284).
6. Доктрина информационной безопасности Российской Федерации.

# ПРИЛОЖЕНИЕ 6

# ФЕДЕРАЛЬНЫЙ ЗАКОН ОТ 20 ФЕВРАЛЯ 1995 г. N 24-ФЗ «ОБ ИНФОРМАЦИИ, ИНФОРМАТИЗАЦИИ И ЗАЩИТЕ ИНФОРМАЦИИ»

(с изменениями от 10 января 2003 г.)

*Принят Государственной Думой 25 января 1995 г.*

## Глава 1. ОБЩИЕ ПОЛОЖЕНИЯ

Об участии России в международном информационном обмене см. Федеральный закон от 4 июля 1996 г. N 85-ФЗ

### Статья 1. Сфера действия настоящего Федерального закона

1. Настоящий Федеральный закон регулирует отношения, возникающие при:

формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителю документированной информации;

создании и использовании информационных технологий и средств их обеспечения;

защите информации, прав субъектов, участвующих в информационных процессах и информатизации.

2. Настоящий Федеральный закон не затрагивает отношений, регулируемых Законом Российской Федерации «Об авторском праве и смежных правах».

### Статья 2. Термины, используемые в настоящем Федеральном законе, их определения

В настоящем Федеральном законе используются следующие понятия:

информация — сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;

информатизация — организационный социально-экономический и научно-технический процесс создания оптимальных условий для удовлетворения информационных потребностей и реализации прав граждан, органов государственной власти, органов местного самоуправления, организаций, общественных объединений на основе формирования и использования информационных ресурсов;

документированная информация (документ) — зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать;

информационные процессы — процессы сбора, обработки, накопления, хранения, поиска и распространения информации;

информационная система — организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы;

информационные ресурсы — отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах);

информация о гражданах (персональные данные) — сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность;

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

средства обеспечения автоматизированных информационных систем и их технологий — программные, технические, лингвистические, правовые, организационные средства;

программы для электронных вычислительных машин; средства вычислительной техники и связи; словари, тезаурусы и классификаторы; инструкции и методики; положения, уставы, должностные инструкции; схемы и их описания, другая эксплуатационная и сопроводительная документация), используемые или создаваемые при проектировании информационных систем и обеспечивающие их эксплуатацию;

собственник информационных ресурсов, информационных систем, технологий и средств их обеспечения — субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения указанными объектами;

владелец информационных ресурсов, информационных систем, технологий и средств их обеспечения — субъект, осущест-

вляющий владение и пользование указанными объектами и реализующий полномочия распоряжения в пределах, установленных законом;

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

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

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

2. Основными направлениями государственной политики в сфере информатизации являются:

обеспечение условий для развития и защиты всех форм собственности на информационные ресурсы;

формирование и защита государственных информационных ресурсов;

создание и развитие федеральных и региональных информационных систем и сетей, обеспечение их совместимости и взаимодействия в едином информационном пространстве Российской Федерации;

создание условий для качественного и эффективного информационного обеспечения граждан, органов государственной власти, органов местного самоуправления, организаций и общественных объединений на основе государственных информационных ресурсов;

обеспечение национальной безопасности в сфере информатизации, а также обеспечение реализации прав граждан, организаций в условиях информатизации;

содействие формированию рынка информационных ресурсов, услуг, информационных систем, технологий, средств их обеспечения;

формирование и осуществление единой научно-технической и промышленной политики в сфере информатизации с учетом современного мирового уровня развития информационных технологий;

поддержка проектов и программ информатизации;

создание и совершенствование системы привлечения инвестиций и механизма стимулирования разработки и реализации проектов информатизации;

развитие законодательства в сфере информационных процессов, информатизации и защиты информации.

## Глава 2. ИНФОРМАЦИОННЫЕ РЕСУРСЫ

### Статья 4. Основы правового режима информационных ресурсов

1. Информационные ресурсы являются объектами отношений физических, юридических лиц, государства, составляют информационные ресурсы России и защищаются законом наряду с другими ресурсами.

2. Правовой режим информационных ресурсов определяется нормами, устанавливающими:

порядок документирования информации;

право собственности на отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах;

категорию информации по уровню доступа к ней;

порядок правовой защиты информации.

### Статья 5. Документирование информации

1. Документирование информации является обязательным условием включения информации в информационные ресурсы. Документирование информации осуществляется в порядке, устанавливаемом органами государственной власти, ответственными за организацию делопроизводства, стандартизацию документов и их массивов, безопасность Российской Федерации.

2. Документ, полученный из автоматизированной информационной системы, приобретает юридическую силу после его подписания должностным лицом в порядке, установленном законодательством Российской Федерации.

3. Юридическая сила документа, хранимого, обрабатываемого и передаваемого с помощью автоматизированных информационных и телекоммуникационных систем, может подтверждаться электронной цифровой подписью.

Юридическая сила электронной цифровой подписи признается при наличии в автоматизированной информационной системе программно-технических средств, обеспечивающих идентификацию подписи, и соблюдении установленного режима их использования.

4. Исключен.

## Статья 6. Информационные ресурсы как элемент состава имущества и объект права собственности

1. Информационные ресурсы могут быть государственными и негосударственными и как элемент состава имущества находятся в собственности граждан, органов государственной власти, органов местного самоуправления, организаций и общественных объединений. Отношения по поводу права собственности на информационные ресурсы регулируются гражданским законодательством Российской Федерации.

2. Физические и юридические лица являются собственниками тех документов, массивов документов, которые созданы за счет их средств, приобретены ими на законных основаниях, получены в порядке дарения или наследования.

3. Российская Федерация и субъекты Российской Федерации являются собственниками информационных ресурсов, создаваемых, приобретаемых, накапливаемых за счет средств федерального бюджета, бюджетов субъектов Российской Федерации, а также полученных путем иных установленных законом способов.

Государство имеет право выкупа документированной информации у физических и юридических лиц в случае отнесения этой информации к государственной тайне.

Собственник информационных ресурсов, содержащих сведения, отнесенные к государственной тайне, вправе распоряжаться этой собственностью только с разрешения соответствующих органов государственной власти.

4. Субъекты, представляющие в обязательном порядке документированную информацию в органы государственной власти и организации, не утрачивают своих прав на эти документы и на использование информации, содержащейся в них. Документированная информация, представляемая в обязательном порядке в органы государственной власти и организации юридическими лицами независимо от их организационно-правовой формы и форм собственности, а также гражданами на основании статьи 8 настоящего Федерального закона, формирует информационные ресурсы, находящиеся в совместном владении государства и субъектов, представляющих эту информацию.

5. Информационные ресурсы, являющиеся собственностью организаций, включаются в состав их имущества в соответствии с гражданским законодательством Российской Федерации.

Информационные ресурсы, являющиеся собственностью государства, находятся в ведении органов государственной власти и организаций в соответствии с их компетенцией, подлежат учету и защите в составе государственного имущества.

6. Информационные ресурсы могут быть товаром, за исключением случаев, предусмотренных законодательством Российской Федерации.

7. Собственник информационных ресурсов пользуется всеми правами, предусмотренными законодательством Российской Федерации, в том числе он имеет право:

назначить лицо, осуществляющее хозяйственное ведение информационными ресурсами или оперативное управление ими;

устанавливать в пределах своей компетенции режим и правила обработки, защиты информационных ресурсов и доступа к ним;

определять условия распоряжения документами при их копировании и распространении.

8. Право собственности на средства обработки информации не создает права собственности на информационные ресурсы, принадлежащие другим собственникам. Документы, обрабатываемые в порядке предоставления услуг или при совместном использовании этих средств обработки, принадлежат их владельцу. Принадлежность и режим производной продукции, создаваемой в этом случае, регулируются договором.

## Статья 7. Государственные информационные ресурсы

1. Государственные информационные ресурсы Российской Федерации формируются в соответствии со сферами ведения как:

федеральные информационные ресурсы;

информационные ресурсы, находящиеся в совместном ведении Российской Федерации и субъектов Российской Федерации (далее — информационные ресурсы совместного ведения);

информационные ресурсы субъектов Российской Федерации.

2. Формирование государственных информационных ресурсов в соответствии с пунктом 1 статьи 8 настоящего Федерального закона осуществляется гражданами, органами государственной власти, органами местного самоуправления, организациями и общественными объединениями.

Федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации формируют государственные информационные ресурсы, находящиеся в их ведении, и обеспечивают их использование в соответствии с установленной компетенцией.

3. Деятельность органов государственной власти и организаций по формированию федеральных информационных ресурсов, информационных ресурсов совместного ведения, информационных ресурсов субъектов Российской Федерации финансируется из федерального бюджета и бюджетов субъектов Российской Федерации по статье расходов «Информатика» («Информационное обеспечение»).

4. Исключен.

## Статья 8. Обязательное представление документированной информации для формирования государственных информационных ресурсов

1. Граждане, органы государственной власти, органы местного самоуправления, организации и общественные объединения обязаны представлять документированную информацию органам и организациям, ответственным за формирование и использование государственных информационных ресурсов.

Перечни представляемой в обязательном порядке документированной информации и перечни органов и организаций, ответственных за сбор и обработку федеральных информационных ресурсов, утверждает Правительство Российской Федерации.

2. Порядок и условия обязательного представления документированной информации доводятся до сведения граждан и организаций.

Порядок обязательного представления (получения) информации, отнесенной к государственной тайне, и конфиденциальной информации устанавливается и осуществляется в соответствии с законодательством об этих категориях информации.

3. При регистрации юридических лиц регистрационные органы обеспечивают их перечнями представляемых в обязательном порядке документов и адресами их представления. Перечень представляемой в обязательном порядке документированной информации прилагается к уставу каждого юридического лица (положению о нем).

Необеспечение регистрационными органами регистрируемых юридических лиц перечнем представляемых в обязательном порядке документов с адресами их представления не является основанием для отказа в регистрации. Должностные лица регистрационных органов, виновные в необеспечении регистрируемых юридических лиц перечнями представляемых в обязательном порядке документов с адресами их представления привлекаются к дисциплинарной ответственности вплоть до снятия с должности.

4. Документы, принадлежащие физическим и юридическим лицам, могут включаться по желанию собственника в состав государственных информационных ресурсов по правилам, установленным для включения документов в соответствующие информационные системы.

### Статья 9. Отнесение информационных ресурсов к общероссийскому национальному достоянию

1. Отдельные объекты федеральных информационных ресурсов могут быть объявлены общероссийским национальным достоянием.

2. Отнесение конкретных объектов федеральных информационных ресурсов к общероссийскому национальному достоянию и определение их правового режима устанавливаются федеральным законом.

### Статья 10. Информационные ресурсы по категориям доступа

1. Государственные информационные ресурсы Российской Федерации являются открытыми и общедоступными. Исключение составляет документированная информация, отнесенная законом к категории ограниченного доступа.

2. Документированная информация с ограниченным доступом по условиям ее правового режима подразделяется на информацию, отнесенную к государственной тайне, и конфиденциальную.

3. Запрещено относить к информации с ограниченным доступом:

законодательные и другие нормативные акты, устанавливающие правовой статус органов государственной власти, органов местного самоуправления, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации;

документы, содержащие информацию о чрезвычайных ситуациях, экологическую, метеорологическую, демографическую, санитарно-эпидемиологическую и другую информацию, необходимую для обеспечения безопасного функционирования населенных пунктов, производственных объектов, безопасности граждан и населения в целом;

документы, содержащие информацию о деятельности органов государственной власти и органов местного самоуправления, об использовании бюджетных средств и других государственных и местных ресурсов, о состоянии экономики и потреб-

ностях населения, за исключением сведений, отнесенных к государственной тайне;

документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах органов государственной власти, органов местного самоуправления, общественных объединений, организаций, представляющие общественный интерес или необходимые для реализации прав, свобод и обязанностей граждан.

4. Отнесение информации к государственной тайне осуществляется в соответствии с Законом Российской Федерации «О государственной тайне».

5. Отнесение информации к конфиденциальной осуществляется в порядке, установленном законодательством Российской Федерации, за исключением случаев, предусмотренных статьей 11 настоящего Федерального закона.

---

Федеральным законом от 10 января 2003 г. N 15-ФЗ в статью 11 настоящего Федерального закона внесены изменения.

---

### Статья 11. Информация о гражданах (персональные данные)

1. Перечни персональных данных, включаемых в состав федеральных информационных ресурсов, информационных ресурсов совместного ведения, информационных ресурсов субъектов Российской Федерации, информационных ресурсов органов местного самоуправления, а также получаемых и собираемых негосударственными организациями, должны быть закреплены на уровне федерального закона. Персональные данные относятся к категории конфиденциальной информации.

Перечень сведений конфиденциального характера утвержден Указом Президента РФ от 6 марта 1997 г. N 188.

Не допускаются сбор, хранение, использование и распространение информации о частной жизни, а равно информации, нарушающей личную тайну, семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений физического лица без его согласия, кроме как на основании судебного решения.

2. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на

основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с законодательством.

3. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

4. Неправомерность деятельности органов государственной власти и организаций по сбору персональных данных может быть установлена в судебном порядке по требованию субъектов, действующих на основании статей 14 и 15 настоящего Федерального закона и законодательства о персональных данных.

## Глава 3. ПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫМИ РЕСУРСАМИ

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

1. Пользователи — граждане, органы государственной власти, органы местного самоуправления, организации и общественные объединения — обладают равными правами на доступ к государственным информационным ресурсам и не обязаны обосновывать перед владельцами этих ресурсов необходимость получения запрашиваемой ими информации. Исключение составляет информация с ограниченным доступом.

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

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

Информация, полученная на законных основаниях из государственных информационных ресурсов гражданами и организациями, может быть использована ими для создания производ-

ной информации в целях ее коммерческого распространения с обязательной ссылкой на источник информации.

Источником прибыли в этом случае является результат вложенных труда и средств при создании производной информации, но не исходная информация, полученная из государственных ресурсов.

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

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

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

5. Порядок накопления и обработки документированной информации с ограниченным доступом, правила ее защиты и порядок доступа к ней определяются органами государственной власти, ответственными за определенные вид и массивы информации, в соответствии с их компетенцией либо непосредственно ее собственником в соответствии с законодательством.

### Статья 13. Гарантии предоставления информации

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

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

3. Комитет при Президенте Российской Федерации по политике информатизации организует регистрацию всех информационных ресурсов, информационных систем и публикацию

сведений о них для обеспечения права граждан на доступ к информации.

4. Перечень информационных услуг, предоставляемых пользователям из государственных информационных ресурсов бесплатно или за плату, не возмещающую в полном размере расходы на услуги, устанавливает Правительство Российской Федерации.

Расходы на указанные услуги компенсируются из средств федерального бюджета и бюджетов субъектов Российской Федерации.

### Статья 14. Доступ граждан и организаций к информации о них

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

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

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

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

### Статья 15. Обязанности и ответственность владельца информационных ресурсов

1. Владелец информационных ресурсов обязан обеспечить соблюдение режима обработки и правил предоставления информации пользователю, установленных законодательством Российской Федерации или собственником этих информационных ресурсов, в соответствии с законодательством.

2. Владелец информационных ресурсов несет юридическую ответственность за нарушение правил работы с информацией в порядке, предусмотренном законодательством Российской Федерации.

# Глава 4. ИНФОРМАТИЗАЦИЯ, ИНФОРМАЦИОННЫЕ СИСТЕМЫ, ТЕХНОЛОГИИ И СРЕДСТВА ИХ ОБЕСПЕЧЕНИЯ

## Статья 16. Разработка и производство информационных систем, технологий и средств их обеспечения

1. Все виды производства информационных систем и сетей, технологий и средств их обеспечения составляют специальную отрасль экономической деятельности, развитие которой определяется государственной научно-технической и промышленной политикой информатизации.

2. Государственные и негосударственные организации, а также граждане имеют равные права на разработку и производство информационных систем, технологий и средств их обеспечения.

3. Государство создает условия для проведения научно-исследовательских и опытно-конструкторских работ в области разработки и производства информационных систем, технологий и средств их обеспечения.

Правительство Российской Федерации определяет приоритетные направления развития информатизации и устанавливает порядок их финансирования.

4. Разработка и эксплуатация федеральных информационных систем финансируются из средств федерального бюджета по статье расходов «Информатика» («Информационное обеспечение»).

5. Органы государственной статистики совместно с Комитетом при Президенте Российской Федерации по политике информатизации устанавливают правила учета и анализа состояния отрасли экономической деятельности, развитие которой определяется государственной научно-технической и промышленной политикой информатизации.

## Статья 17. Право собственности на информационные системы, технологии и средства их обеспечения

1. Информационные системы, технологии и средства их обеспечения могут быть объектами собственности физических и юридических лиц, государства.

2. Собственником информационной системы, технологии и средств их обеспечения признается физическое или юридическое лицо, на средства которого эти объекты произведены, при-

обретены или получены в порядке наследования, дарения или иным законным способом.

3. Информационные системы, технологии и средства их обеспечения включаются в состав имущества субъекта, осуществляющего права собственника или владельца этих объектов. Информационные системы, технологии и средства их обеспечения выступают в качестве товара (продукции) при соблюдении исключительных прав их разработчиков.

Собственник информационной системы, технологии и средств их обеспечения определяет условия использования этой продукции.

### Статья 18. Право авторства и право собственности на информационные системы, технологии и средства их обеспечения

Право авторства и право собственности на информационные системы, технологии и средства их обеспечения могут принадлежать разным лицам.

Собственник информационной системы, технологии и средств их обеспечения обязан защищать права их автора в соответствии с законодательством Российской Федерации.

---

Федеральным законом от 10 января 2003 г. N 15-ФЗ в статью 19 настоящего Федерального закона внесены изменения

---

### Статья 19. Сертификация информационных систем, технологий, средств их обеспечения

1. Информационные системы, базы и банки данных, предназначенные для информационного обслуживания граждан и организаций, подлежат сертификации в порядке, установленном Законом Российской Федерации «О сертификации продукции и услуг».

2. Информационные системы органов государственной власти Российской Федерации и органов государственной власти субъектов Российской Федерации, других государственных органов, организаций, которые обрабатывают документированную информацию с ограниченным доступом, а также средства защиты этих систем подлежат обязательной сертификации. Порядок сертификации определяется законодательством Российской Федерации.

3. Интересы потребителя информации при использовании импортной продукции в информационных системах защищаются

таможенными органами Российской Федерации на основе международной системы сертификации.

## Глава 5. ЗАЩИТА ИНФОРМАЦИИ И ПРАВ СУБЪЕКТОВ В ОБЛАСТИ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ И ИНФОРМАТИЗАЦИИ

### Статья 20. Цели защиты

Целями защиты являются:

предотвращение утечки, хищения, утраты, искажения, подделки информации;

предотвращение угроз безопасности личности, общества, государства;

предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности;

защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;

сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;

обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

### Статья 21. Защита информации

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

Режим защиты информации устанавливается:

в отношении сведений, отнесенных к государственной тайне, — уполномоченными органами на основании Закона Российской Федерации «О государственной тайне»;

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

в отношении персональных данных — Федеральным законом.

2. Органы государственной власти и организации, ответственные за формирование и использование информационных ресурсов, подлежащих защите, а также органы и организации, разрабатывающие и применяющие информационные системы и информационные технологии для формирования и использования информационных ресурсов с ограниченным доступом, руководствуются в своей деятельности законодательством Российской Федерации.

3. Контроль за соблюдением требований к защите информации и эксплуатацией специальных программно-технических средств защиты, а также обеспечение организационных мер защиты информационных систем, обрабатывающих информацию с ограниченным доступом в негосударственных структурах, осуществляются органами государственной власти. Контроль осуществляется в порядке, определяемом Правительством Российской Федерации.

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

5. Собственник информационных ресурсов или уполномоченные им лица имеют право осуществлять контроль за выполнением требований по защите информации и запрещать или приостанавливать обработку информации в случае невыполнения этих требований.

6. Собственник или владелец документированной информации вправе обращаться в органы государственной власти для оценки правильности выполнения норм и требований по защите его информации в информационных системах. Соответствующие органы определяет Правительство Российской Федерации. Эти органы соблюдают условия конфиденциальности самой информации и результатов проверки.

### Статья 22. Права и обязанности субъектов в области защиты информации

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

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

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

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

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

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

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

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

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

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

Для рассмотрения конфликтных ситуаций и защиты прав участников в сфере формирования и использования информационных ресурсов, создания и использования информационных систем, технологий и средств их обеспечения могут создаваться временные и постоянные третейские суды.

Третейский суд рассматривает конфликты и споры сторон в порядке, установленном законодательством о третейских судах.

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

### Статья 24. Защита права на доступ к информации

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

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

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

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

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

### Статья 25. Вступление в силу настоящего Федерального закона

1. Настоящий Федеральный закон вступает в силу со дня его официального опубликования.

2. Предложить Президенту Российской Федерации привести в соответствие с настоящим Федеральным законом изданные им правовые акты.

3. Поручить Правительству Российской Федерации:

привести в соответствие с настоящим Федеральным законом изданные им правовые акты;

подготовить и внести в Государственную Думу в трехмесячный срок в установленном порядке предложения о внесении изменений и дополнений в законодательство Российской Федерации в связи с принятием настоящего Федерального закона;

принять нормативные правовые акты, обеспечивающие реализацию настоящего Федерального закона.

Президент
Российской Федерации
Б. ЕЛЬЦИН

Москва, Кремль
20 февраля 1995 г.
N 24-ФЗ

# СОДЕРЖАНИЕ

САНКТ-ПЕТЕРБУРГСКИЙ УНИВЕРСИТЕТ
УПРАВЛЕНИЯ И ЭКОНОМИКИ

***Геннадий Александрович Костин***
***Виталий Александрович Кулишкин***
***Сергей Владимирович Марков***
***Сергей Николаевич Панин***

# Информационная безопасность и защита информации

*Учебник*

Заведующий редакцией научной и учебно-методической
литературы Издательства СПбУУиЭ
*А. В. Блажко*

Подписано в печать 25.10.2011 г.
Формат 60×84 $^{1}/_{16}$. Уч.-изд. л. 14,37. Усл. печ. л. 18,75.
Тираж 600 экз. Заказ № 8597

Издательство Санкт-Петербургского университета
управления и экономики
198103, Санкт-Петербург, Лермонтовский пр. 44, лит. А
(812)448-82-50
E-mail: izdat-ime@spbume.ru, izdat-ime@yandex.ru

Отпечатано в типографии «НП-Принт»
190005, Санкт-Петербург, Измайловский пр., д. 29

В учебнике рассматриваются проблемы информационной безопасности, ставшие особенно актуальными в связи с массовым переходом информационных технологий на автоматизированную основу. Авторами проведен анализ совокупности технических средств, с помощью которых может регистрироваться и передаваться информация; характеризуются направления правовой деятельности, регулирующей отношения в области обеспечения информационной безопасности; указаны основные нормативные документы, регламентирующие деятельность по обеспечению безопасности информации; представлены сведения об инженерно-механических системах обеспечения безопасности объектов, а также системах обнаружения, опознавания, регистрации и сигнализации попыток проникновения на охраняемый объект; рассмотрены основные этапы построения системы защиты информации на охраняемом объекте; приведен порядок обеспечения безопасности информации в информационных системах персональных данных.

Учебник предназначен в помощь студентам высших учебных заведений, изучающим основные образовательные программы по направлениям подготовки бакалавриата 090900.62 «Информационная безопасность» и 230700.62 «Прикладная информатика» для формирования общекультурных и профессиональных компетенций по вопросам обеспечения информационной безопасности на всех этапах разработки и эксплуатации информационных систем.

ISBN 978-5-94047-314-5