УЧЕБНОЕ ПОСОБИЕ

ДЛЯ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ

СПЕЦИАЛЬНОСТЬ

# Основы информационной безопасности

Е. Б. Белов, В. П. Лось,
Р. В. Мещеряков, А. А. Шелупанов

Е. Б. Белов, В. Лось,
Р. В. Мещеряков, Д. А. Шелупанов

# Основы информационной безопасности

*Допущено Министерством образования и науки Российской Федерации в качестве учебного пособия для студентов высших учебных заведений, обучающихся по специальностям в области информационной безопасности*

Москва
Горячая линия - Телеком
2006

**ББК** 32.97
УДК 681.3
0-75

Рецензент: доктор физ.-мат. наук, профессор *С. С. Бондарчук*

**О-75** **Основы** информационной безопасности. Учебное пособие для вузов / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. - М.: Горячая линия - Телеком, 2006. - 544 с.: ил.

ISBN 5-93517-292-5.

Изложены вопросы теории и практики обеспечения информационной безопасности личности, общества и государства. Большое внимание уделено проблеме безопасности автоматизированных систем, включая вопросы определения модели нарушителя и требований к защите информации. Анализируются современные способы и средства защиты информации и архитектура систем защиты информации. В приложениях приведен справочный материал по ряду нормативных правовых документов и вариант рабочей программы по дисциплине «Основы информационной безопасности».

Для студентов высших учебных заведений, обучающихся по специальностям в области информационной безопасности, может быть полезной для широкого круга читателей, интересующихся вопросами обеспечения информационной безопасности.

**ББК 32.97**

*Адрес издательства в Интернет* www.techbook.ru
*e-mail:* radios_hl@mtu-net.ru

Учебное издание

**Белов** Евгений Борисович, **Лось** Владимир Павлович,
**Мещеряков** Роман Валерьевич, **Шелупанов** Александр Александрович

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

*Учебное пособие*

Редактор Е. А. Лебедев
Корректор А. Н. Иванова
Компьютерная верстка О. А. Петренко
Обложка художника В. Г. Сетина

ЛР № 071825 от 20 марта 1999 г.
Подписано в печать 16.08.05. Формат 60x88/16. Печать офсетная
Уч.-изд. л. 34. Тираж 3000 экз. Изд. № 292

ISBN 5-93517-292-5

# Предисловие

В книге рассматриваются ключевые разделы курса «Основы информационной безопасности». В него включены как теоретические, так и практические разделы, направленные на развитие навыков анализа и совершенствования информационной безопасности объектов.

Главная цель книги - познакомить обучаемых с основами информационной безопасности, определить основные направления развития этой области знаний, в рамках образовательной программы попытаться сформировать у них элементы «информационной культуры». Авторы не претендуют на собственную исключительность и глубинные научные исследования в области информационной безопасности. Не случайно, что и пособие имеет название «Основы информационной безопасности», а не, например, «Теоретические основы информационной безопасности». В этом случае нам пришлось бы основательно потрудиться над теоретическими обоснованиями многих утверждений. Наша цель куда более скромна - пробудить интерес у обучаемых к серьезному и вдумчивому изучению проблем информационной безопасности.

В настоящее время появилось много книг, посвященных рассматриваемой тематике. В ряде основополагающих работ Расторгуева С.П., Ярочкина В. И., Герасименко В. А., Малюка А. А. и других авторов достаточно точно, конкретно и правильно представлены понятия, определения и положения в области информационной безопасности. Многие из них мы использовали в учебном пособии, в частности в него практически полностью вошли разделы, связанные с информационными системами (см. источники [31, 30] ч. 2).

В пособии приведен глоссарий основных терминов. Обращаем внимание на то, что все без исключения определения и термины взяты нами из соответствующих законов РФ в области информации, защиты информации и информационной безопасности. Это освобождает авторов от необходимости использовать определения других авторов, не всегда, на наш взгляд, корректные и точные. Кроме того, приведены наиболее употребляемые термины, используемые в области информационной безопасности, на английском языке и их перевод.

В пособии представлены некоторые законодательные акты, которые могут использоваться обучаемыми студентами в качестве правовой базы обеспечения информационной безопасности.

Учебное пособие основано на опыте преподавания дисциплины «Основы информационной безопасности» в Институте криптографии, связи

и информатики Академии ФСБ России и Томском государственном университете систем управления и радиоэлектроники.

Данная дисциплина включена в государственный образовательный стандарт по специальностям: 090102 - «Компьютерная безопасность», 090105 - «Комплексное обеспечение информационной безопасности автоматизированных систем», 090106 - «Информационная безопасность телекоммуникационных систем». Рабочая программа этой дисциплины, контрольные вопросы и задания также приведена в приложениях.

Государственные образовательные стандарты (ГОС) по группе специальностей «Информационная безопасность» предусматривают изучение следующих тем: понятие национальной безопасности; виды безопасности; информационная безопасность (ИБ) в системе национальной безопасности РФ; основные понятия, общеметодологические принципы теории ИБ; анализ угроз ИБ, проблемы информационной войны; государственная информационная политика; проблемы региональной информационной безопасности; виды информации; методы и средства обеспечения ИБ; методы нарушения конфиденциальности, целостности и доступности информации; причины, виды искажения информации и каналы утечки ее.

*Авторы*

В России все - секретно,
и ничто не тайна.
*Мадам де Сталь*

# Введение

Отыскивать всему начало, как рекомендовал в свое время Козьма Прутков, довольно сложное, а порой и неблагодарное занятие. Все усложняется многократно, когда речь идет о новых областях и направлениях современных знаний. А то, что информационная безопасность - новая, бурно развивающаяся область знаний не вызывает, надеемся, ни у кого сомнений. В новых областях знаний, нет авторитетов, устоявшейся терминологии, общепризнанных понятий, категорий, принципов и т. д. Не существует и «надежной» аксиоматики, адекватно обозначающей проблему. В самом деле, занявшись подготовкой данного материала, авторы ознакомились со значительным количеством открытых литературных источников по данной проблеме и с удивлением обнаружили, что «информация» чуть ли не самое употребляемое слово. Причем каких только понятий и определений информации не давалось различными авторами. Однако многим из них и в голову не пришло заглянуть в любой учебник по теории информации, чтобы с первых страниц понять, что информация есть функция энтропии и подчиняется ряду объективных законов. Более того, знание этих законов существенно облегчает нам манипуляции с информацией. Как же так?

Столкнулись мы и с существенно «механичными» представлениями ряда авторов. Хотя достаточно внимательно присмотреться к любой биологической системе, чтобы определить присутствие в ней всех элементов информационной системы и задуматься над проблемами информационной безопасности. В самом деле, многие общеизвестные факты из функционирования живых систем заставляют по-новому взглянуть на проблему информационной безопасности.

«Вот вирус, пограничное между жизнью и неживой природой образование. Он показывает возможности нарушения чужой программы. Вирус приспособился эксплуатировать определенный вид живых клеток, «умеет» их находить, цепляться к их оболочке. Прицепившись, он проталкивает в клетку всего ОДНУ молекулу - РНК, в которой записаны команды по «производству» вирусов. И в клетке возникает тайное, теневое правительство, которое подчиняет своей воле всю жизнедеятельность огромной системы (клетка по сравнению с вирусом - это целая страна). Все ресурсы клетки направлены теперь на выполнение команд, записанных во внедренной в нее матрице. Сложные производственные системы клет-

ки ПЕРЕНАЛАЖИВАЮТСЯ на выпуск сердечников вируса и на то, чтобы одеть их в белковую оболочку, после чего истощенная клетка погибает.

Это исходный, фундаментальный вариант взаимодействия, при котором один участник жизненной драмы заставляет действовать в его интересах и по его программе так, что это не распознается жертвами и не вызывает у них сопротивления. Мы имеем случай манипуляции, проделанной путем подмены документа, в котором записана вся производственная программа.

Вообще же несть числа способам повлиять на поведение членов экологического сообщества, окружающих живое образование. Растения обрамляют свои тычинки и пестик роскошной привлекательной декорацией - цветком, выделяющим к тому же ароматный нектар. Насекомые устремляются на запах и цвет, платя за нектар работой по опылению.

Богомол притворился сухим листиком, не отличишь. Он создал невинный и скромный ложный образ, успокаивающий жертву.

Пчела-разведчица, найдя заросли медоносов, летит в улей и исполняет перед товарищами танец, точно указывая направление на цель и расстояние до нее.

Каракатица, став жертвой нападения страшного для нее хищника, выпускает чернильную жидкость, а затем вырывает и выбрасывает в темное облачко свои внутренности. Они там заманчиво шевелятся, и простодушный хищник рад: попалась, голубушка! И пока он рыщет в чернильной мути, циничная каракатица, принеся в жертву часть ради целого, уползает отращивать новые внутренности.

Иногда сигналы, посылаемые в окружающую среду, «перехватываются» хищником или паразитом и становятся губительными для их отправителя. Грибок стрига наносит огромный урон урожаям пшеницы в Азии и Африке. Его споры, дремлющие в земле, оживают лишь на четвертый день после того, как пшеничное зерно после посева пустит корень - на свежем ростке корня паразитирует гриб. Как же определяет грибок момент своей активизации и нападения? Сигналом служит одно из веществ, выделяемых корнем (его недавно выделили из засеянной земли, очистили, изучили строение и назвали стригол). Достаточно попадания в спору грибка всего одной молекулы стригола, чтобы были запущены бурные процессы жизнедеятельности. На беду себе семя пшеницы «утечкой информации» программирует поведение своего паразита.

В других случаях, наоборот, паразит своей «химической информацией» (какими-то выделениями) программирует поведение эксплуатируемых им существ. Иногда эффективность этого программирования бывает так высока, что впору говорить о гипнотическом воздействии. Это особенно поражает, когда по программе действуют большие массы организ-

мов, например у «социальных», живущих большими колониями насекомых. Так, например, устроились в муравейниках крошечные жучки - жуки Ломехуза.

Своими манерами и движениями жучки Ломехуза очень напоминают муравьев и хорошо владеют их языком жестов. Солидарные и трудолюбивые муравьи по первой же просьбе дают корм собрату. Муравей выражает эту просьбу, определенным образом постукивая товарища. Жучки «освоили» эти жесты и легко выманивают пищу. Но они прожорливы и обязывают целые отряды муравьев переключиться на их кормежку. На теле у жучков есть пучки золотистых волосков, на которых скапливаются выделения. Рабочие муравьи слизывают эти выделения и утрачивают всякий здравый смысл. Они начинают выкармливать жучков и их личинок с таким рвением, что оставляют без корма и собратьев, и даже собственные личинки. Возлюбив пришельцев, сами они впадают в полное уничтожение, вплоть до того, что скармливают жучкам муравьиные яйца, оставаясь без потомства. А если муравейнику грозит опасность, они спасают личинок жука, бросая своих.

Ясно, что своими наркотическими выделениями жучки Ломехуза посылают муравьям сигнал, блокирующий важную программу поведения, заложенную в организм муравья, ту программу, которая в норме побуждает муравья совершать действия, направленные на жизнеобеспечение муравейника и продолжение рода. И видимо, переданная жучками информация не только блокирует «нормальную» программу, но перекодирует ее, активизируя те действия муравьев, которые выгодны паразиту [31]. Причем так, что муравьи просто счастливы выполнять эти действия».

Согласитесь, весьма увлекательно и поучительно. Конечно, здесь можно продолжить ряд примеров биологических систем, однако и без того понятно: анализ биологических, или «живых», систем позволяет выйти на многие аналогии систем информационных и их безопасности. Посмотрите, как хитро переплетены вопросы защиты информации и защиты от информации, информационные атаки и попытки (не всегда удачные) противостояния этим атакам. Отсюда можно сделать вывод довольно очевидный: многообразие живой природы дает нам достаточно оснований смотреть на проблему информационной безопасности как на сложный, интегрированный комплекс мероприятий.

Средства массовой информации (СМИ) муссируют не только и не столько различного рода рекламу товаров и услуг, хотя одного этого достаточно для того, чтобы испытать недовольство или откровенное раздражение. Гораздо тоньше и опаснее СМИ проводят порой информаци-

онные атаки, буквально «зомбируя» население городов, регионов и стран. «Кстати, само понятие «зомбирование» стало так часто употребляться направо и налево, что полезно уделить немного места и определить, что это такое. Среди суеверий, распространенных на Гаити, интерес ученых давно привлекала вера в зомби. Это оживший мертвец, которого злые колдуны освобождают из могилы и заставляют служить в качестве раба. Для этой веры есть материальные основания: колдуны, используя очень сильный нейротоксин (тетродоксин), могут снижать видимую жизнедеятельность организма вплоть до полной видимости смерти - с полным параличом. Если колдуну удавалось точно подобрать дозу, этот «умерший» человек оживал в гробу и вытаскивался колдуном из могилы. Колдун давал своему рабу съесть «огурец зомби» - снадобье, содержащее сильное психоактивное растение Datura stramonium L., от которого тот впадал в транс. Антропологи выяснили и социокультурное значение зомбирования - это санкции, накладываемые жрецами племени с целью поддерживать порядок и подтверждать свою власть. Вера в зомбирование и силу зомби разделялась всеми слоями гаитянского общества - страшные тонтон-макуты диктатора Дювалье считались его зомби, чего он, конечно, не отрицал» [31].

Значит, можно сделать вывод о том, что очень важно знать теоретические и практические основы информационной безопасности, хотя бы для того, чтобы избежать «дозированных информационных инъекций».

*Теория защиты информации* определяется как система основных идей, относящихся к защите информации, дающая целостное представление о сущности проблемы защиты, закономерностях ее развития и существенных связях с другими отраслями знания, формирующаяся на основе опыта практического решения задач защиты и определяющая основные ориентиры в направлении совершенствования практики защиты информации.

Составными частями теории являются:

- полные и систематизированные сведения о происхождении, сущности и содержании проблемы защиты;
- систематизированные результаты анализа развития теоретических исследований и разработок, а также опыта практического решения задач защиты;
- научно обоснованная постановка задачи защиты информации в современных системах ее обработки, полно и адекватно учитывающая текущие и перспективные концепции построения систем и техноло-

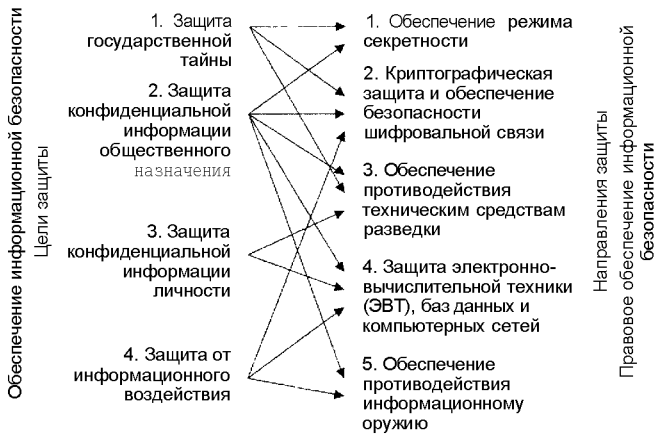
гий обработки, потребности в защите информации и объективные предпосылки их удовлетворения;

- общие стратегические установки на организацию защиты информации, учитывающие все многообразие потенциально возможных условий защиты;
- методы, необходимые для адекватного и наиболее эффективного решения всех задач защиты и содержащие как общеметодологические подходы к решению, так и конкретные прикладные методы решения;
- методологическая и инструментальная база, содержащая необходимые методы и инструментальные средства для решения любой совокупности задач защиты в рамках любой выбранной стратегической установки;
- научно обоснованные предложения по организации и обеспечению работ по защите информации;
- научно обоснованный прогноз перспективных направлений развития теории и практики защиты информации.

*Информационная безопасность* определяется способностью государства, общества, личности:

- обеспечивать с определенной вероятностью достаточные и защищенные информационные ресурсы и информационные потоки для поддержания своей жизнедеятельности и жизнеспособности, устойчивого функционирования и развития;
- противостоять информационным опасностям и угрозам, негативным информационным воздействиям на индивидуальное и общественное сознание и психику людей, а также на компьютерные сети и другие технические источники информации;
- вырабатывать личностные и групповые навыки и умения безопасного поведения;
- поддерживать постоянную готовность к адекватным мерам в информационном противоборстве, кем бы оно ни было навязано.

*Информационная война* - действия, принимаемые для достижения информационного превосходства в интересах национальной военной стратегии, осуществляемые путем влияния на информацию и информационные системы противника при одновременной защите собственной информации своих информационных систем. На следующем рисунке представлены направления и цели защиты информации и их взаимосвязь.




Основная цель защиты любой конфиденциальной информации состоит в том, чтобы предотвратить незаконное овладение ею конкурентами или злоумышленниками.

Зарубежный опыт в области защиты интеллектуальной собственности и отечественный опыт в защите государственных секретов показывает, что эффективной может быть только комплексная защита, сочетающая в себе такие направления защиты, как правовая, организационная и инженерно-техническая.

Комплексный характер защиты информации проистекает из комплексных действий злоумышленников, стремящихся любыми средствами добыть важную для конкурентной борьбы информацию. Здесь правомерно утверждение, что оружие защиты должно быть адекватно оружию нападения.

Читатель, видимо, уже сделал для себя вывод, что информационная безопасность - достаточно сложная и многогранная проблема, решение которой под силу хорошо организованным и подготовленным структурам.

Что касается подходов к реализации защитных мероприятий по обеспечению безопасности информационных систем, то сложилась трехстадийная (трехэтапная) разработка таких мер.

Первая стадия - выработка требований - включает:

- определение состава средств информационной системы (ИС);
- анализ уязвимых элементов ИС;

- оценка угроз (выявление проблем, которые могут возникнуть из-за наличия уязвимых элементов);
- анализ риска (прогнозирование возможных последствий, которые могут вызвать эти проблемы).

Вторая стадия - определение способов защиты - включает ответы на следующие вопросы:

- какие угрозы должны быть устранены и в какой мере?
- какие ресурсы системы должны быть защищаемы и в какой степени?
- с помощью каких средств должна быть реализована защита?
- какова должна быть полная стоимость реализации защиты и затраты на эксплуатацию с учетом потенциальных угроз?

Третья стадия - определение функций, процедур и средств безопасности, реализуемых в виде некоторых механизмов защиты.

# Часть 1

# ОСНОВЫ ГОСУДАРСТВЕННОЙ ИНФОРМАЦИОННОЙ ПОЛИТИКИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

## 1. Понятие национальной безопасности

### 1.1. Интересы и угрозы в области национальной безопасности

В Концепции национальной безопасности РФ, утвержденной Указом Президента РФ от 17.12.1997 г. № 1300 (в редакции Указа Президента РФ от 10.01.2000 г. №24) [1], дается следующее определение национальной безопасности.

Под национальной безопасностью РФ понимается безопасность ее многонационального народа как носителя суверенитета и единственного источника власти в РФ.

Национальные интересы России - это совокупность сбалансированных интересов личности, общества и государства в различных сферах жизнедеятельности: экономической, внутриполитической, социальной, международной, информационной, военной, пограничной, экологической и других. В теории национальной безопасности используется понятие «жизненно важные интересы». Жизненно важные интересы - это совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства [3]. В контексте данной книги понятия «национальные интересы» и «жизненно важные интересы» являются идентичными.

Национальные интересы носят долгосрочный характер. В области внутренней и внешней политики государства этими интересами определяются:

- основные цели этой политики;
- стратегические и текущие задачи.

Национальные интересы обеспечиваются институтами государственной власти, осуществляющими свои функции, в том числе во взаимодействии с действующими на основе Конституции РФ и законодательства РФ общественными организациями.

Интересы личности состоят в реализации конституционных прав и свобод [2], в обеспечении личной безопасности, в повышении качества и уровня жизни, в физическом, духовном и интеллектуальном развитии человека и гражданина.

Интересы общества состоят в упрочении демократии, в создании правового, социального государства, в достижении и поддержании общественного согласия, в духовном обновлении России.

Интересы государства состоят в незыблемости конституционного строя, суверенитета и территориальной целостности России, в политической, экономической и социальной стабильности, в безусловном обеспечении законности и поддержании правопорядка, в развитии равноправного и взаимовыгодного международного сотрудничества.

Реализация национальных интересов России возможна только на основе устойчивого развития экономики. Поэтому национальные интересы России в этой сфере являются ключевыми.

Во **внутриполитической** сфере национальные интересы России состоят в сохранении стабильности конституционного строя, институтов государственной власти, в обеспечении гражданского мира и национального согласия, территориальной целостности, единства правового пространства, правопорядка и в завершении процесса становления демократического общества, а также в нейтрализации причин и условий, способствующих возникновению политического и религиозного экстремизма, этносепаратизма и их последствий - социальных, межэтнических и религиозных конфликтов, терроризма.

Национальные интересы России в **социальной** сфере заключаются в обеспечении высокого уровня жизни народа.

Национальные интересы в **духовной** сфере состоят в сохранении и укреплении нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.

Национальные интересы России в **международной** сфере заключаются в обеспечении суверенитета, упрочении позиций России как великой державы - одного из влиятельных центров многополярного мира, в развитии равноправных и взаимовыгодных отношений со всеми странами и интеграционными объединениями, прежде всего с государствами-участниками Содружества Независимых Государств и традиционными партнерами России, в повсеместном соблюдении прав и свобод человека и недопустимости применения при этом двойных стандартов.

Национальные интересы России в **информационной** сфере заключаются в соблюдении конституционных прав и свобод граждан в области получения информации и пользования ею, в развитии современных теле-

коммуникационных технологий, в защите государственных информационных ресурсов от несанкционированного доступа.

Национальные интересы России в **военной** сфере заключаются в защите ее независимости, суверенитета, государственной и территориальной целостности, в предотвращении военной агрессии против России и ее союзников, в обеспечении условий для мирного, демократического развития государства.

Национальные интересы России в **пограничной** сфере заключаются в создании политических, правовых, организационных и других условий для обеспечения надежной охраны государственной границы РФ, в соблюдении установленных законодательством РФ порядка и правил осуществления экономической и иных видов деятельности в пограничном пространстве РФ.

Национальные интересы России в экологической сфере заключаются в сохранении и оздоровлении окружающей среды.

Важнейшими составляющими национальных интересов России являются защита личности, общества и государства от терроризма, в том числе международного, а также от чрезвычайных ситуаций природного и техногенного характера и их последствий, а в военное время - от опасностей, возникающих при ведении военных действий или вследствие этих действий.

Достижению национальных интересов препятствуют те или иные угрозы. Угроза - это совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства [3], это возможная опасность [4].

Состояние отечественной экономики, несовершенство системы организации государственной власти и гражданского общества, социально-политическая поляризация российского общества и криминализация общественных отношений, рост организованной преступности и увеличение масштабов терроризма, обострение межнациональных и осложнение международных отношений создают широкий спектр внутренних и внешних угроз национальной безопасности страны.

В сфере экономики угрозы имеют комплексный характер и обусловлены прежде всего существенным сокращением внутреннего валового продукта, снижением инвестиционной, инновационной активности и научно-технического потенциала, стагнацией аграрного сектора, разбалансированием банковской системы, ростом внешнего и внутреннего государственного долга, тенденцией к преобладанию в экспортных поставках топливно-сырьевой и энергетической составляющих, а в импортных поставках - продовольствия и предметов потребления, включая предметы первой необходимости.

Ослабление научно-технического и технологического потенциала страны, сокращение исследований на стратегически важных направлениях научно-технического развития, отток за рубеж специалистов и интеллектуальной собственности угрожают России утратой передовых позиций в мире, деградацией наукоемких производств, усилением внешней технологической зависимости и подрывом обороноспособности России.

Негативные процессы в экономике могут иметь своими последствиями сепаратистские устремления ряда субъектов РФ. Это может привести к усилению политической нестабильности, ослаблению единого экономического пространства России и его важнейших составляющих - производственно-технологических и транспортных связей, финансово-банковской, кредитной и налоговой систем.

Экономическая дезинтеграция, социальная дифференциация общества, девальвация духовных ценностей способствуют усилению напряженности во взаимоотношениях регионов и центра, представляя собой угрозу федеративному устройству и социально-экономическому укладу РФ.

Этноэгоизм, этноцентризм и шовинизм, проявляющиеся в деятельности ряда общественных объединений, а также неконтролируемая миграция способствуют усилению национализма, политического и религиозного экстремизма, этносепаратизма и создают условия для возникновения конфликтов.

Единое правовое пространство страны размывается вследствие несоблюдения принципа приоритета норм Конституции РФ над иными правовыми нормами, федеральных правовых норм над нормами субъектов РФ, недостаточной отлаженности государственного управления на различных уровнях.

Угроза криминализации общественных отношений, складывающихся в процессе реформирования социально-политического устройства и экономической деятельности, приобретает особую остроту. Серьезные просчеты, допущенные на начальном этапе проведения реформ в экономической, военной, правоохранительной и иных областях государственной деятельности, ослабление системы государственного регулирования и контроля, несовершенство правовой базы и отсутствие сильной государственной политики в социальной сфере, снижение духовно-нравственного потенциала общества являются основными факторами, способствующими росту преступности, особенно ее организованных форм, а также коррупции.

Последствия этих просчетов проявляются в ослаблении правового контроля за ситуацией в стране, в сращивании отдельных элементов исполнительной и законодательной власти с криминальными структурами, проникновении их в сферу управления банковским бизнесом, крупными

производствами, торговыми организациями и товаропроводящими сетями. В связи с этим борьба с организованной преступностью и коррупцией имеет не только правовой, но и политический характер.

Масштабы терроризма и организованной преступности возрастают вследствие зачастую сопровождающегося конфликтами изменения форм собственности, обострения борьбы за власть на основе групповых и этнонационалистических интересов. Отсутствие эффективной системы социальной профилактики правонарушений, недостаточная правовая и материально-техническая обеспеченность деятельности по предупреждению терроризма и организованной преступности, правовой нигилизм, отток из органов обеспечения правопорядка квалифицированных кадров увеличивают степень воздействия этой угрозы на личность, общество и государство.

Угрозу национальной безопасности России в социальной сфере создают глубокое расслоение общества на узкий круг богатых и преобладающую массу малообеспеченных граждан, увеличение удельного веса населения, живущего за чертой бедности, рост безработицы.

Угрозой физическому здоровью нации являются кризис систем здравоохранения и социальной защиты населения, рост потребления алкоголя и наркотических веществ.

Последствиями глубокого социального кризиса являются резкое сокращение рождаемости и средней продолжительности жизни в стране, деформация демографического и социального состава общества, подрыв трудовых ресурсов как основы развития производства, ослабление фундаментальной ячейки общества - семьи, снижение духовного, нравственного и творческого потенциала населения.

Углубление кризиса во внутриполитической, социальной и духовной сферах может привести к утрате демократических завоеваний.

Основные угрозы в международной сфере обусловлены такими факторами, как:

- стремление отдельных государств и межгосударственных объединений принизить роль существующих механизмов обеспечения международной безопасности, прежде всего ООН и ОБСЕ;
- опасность ослабления политического, экономического и военного влияния России в мире;
- укрепление военно-политических блоков и союзов, прежде всего расширение НАТО на восток;
- возможность появления в непосредственной близости от российских границ иностранных военных баз и крупных воинских контингентов;

распространение оружия массового уничтожения и средств его доставки; ослабление интеграционных процессов в Содружестве Независимых Государств;

- возникновение и эскалация конфликтов вблизи государственной границы РФ и внешних границ государств-участников Содружества Независимых Государств;
- притязания на территорию РФ.

Угрозы национальной безопасности РФ в международной сфере проявляются в попытках других государств противодействовать укреплению России как одного из центров влияния в многополярном мире, помешать реализации национальных интересов и ослабить ее позиции в Европе, на Ближнем Востоке, в Закавказье, Центральной Азии и Азиатско-Тихоокеанском регионе.

Серьезную угрозу национальной безопасности РФ представляет терроризм. Международным терроризмом развязана открытая кампания в целях дестабилизации ситуации в России.

Усиливаются угрозы национальной безопасности РФ в информационной сфере. Серьезную опасность представляют собой стремление ряда стран к доминированию в мировом информационном пространстве, вытеснению России с внешнего и внутреннего информационного рынка; разработка рядом государств концепции информационных войн, предусматривающей создание средств опасного воздействия на информационные сферы других стран мира; нарушение нормального функционирования информационных и телекоммуникационных систем, а также сохранности информационных ресурсов, получение несанкционированного доступа к ним.

Возрастают уровень и масштабы угроз в военной сфере.

Возведенный в ранг стратегической доктрины переход НАТО к практике силовых (военных) действий вне зоны ответственности блока и без санкции Совета Безопасности ООН чреват угрозой дестабилизации всей стратегической обстановки в мире.

Увеличивающийся технологический отрыв ряда ведущих держав и наращивание их возможностей по созданию вооружений и военной техники нового поколения создают предпосылки качественно нового этапа гонки вооружений, коренного изменения форм и способов ведения военных действий.

Активизируется деятельность на территории РФ иностранных специальных служб и используемых ими организаций.

Усилению негативных тенденций в военной сфере способствуют затянувшийся процесс реформирования военной организации и оборонного

промышленного комплекса РФ, недостаточное финансирование национальной обороны и несовершенство нормативной правовой базы. На современном этапе это проявляется в критически низком уровне оперативной и боевой подготовки Вооруженных сил РФ, других войск, воинских формирований и органов, в недопустимом снижении укомплектованности войск (сил) современным вооружением, военной и специальной техникой, в крайней остроте социальных проблем и приводит к ослаблению военной безопасности РФ в целом.

Угрозы национальной безопасности и интересам РФ в пограничной сфере обусловлены:

- экономической, демографической и культурно-религиозной экспансией сопредельных государств на российскую территорию;
- активизацией деятельности трансграничной организованной преступности, а также зарубежных террористических организаций.

Угроза ухудшения экологической ситуации в стране и истощения ее природных ресурсов находится в прямой зависимости от состояния экономики и готовности общества осознать глобальность и важность этих проблем. Для России эта угроза особенно велика из-за преимущественного развития топливно-энергетических отраслей промышленности, неразвитости законодательной основы природоохранной деятельности, отсутствия или ограниченного использования природосберегающих технологий, низкой экологической культуры. Имеет место тенденция к использованию территории России в качестве места переработки и захоронения опасных для окружающей среды материалов и веществ. В этих условиях ослабление государственного надзора, недостаточная эффективность правовых и экономических механизмов предупреждения и ликвидации чрезвычайных ситуаций увеличивают риск катастроф техногенного характера во всех сферах хозяйственной деятельности.

Обеспечение национальной безопасности РФ во многом определяется состоянием информационной безопасности.

Важнейшими задачами обеспечения информационной безопасности РФ являются:

- реализация конституционных прав и свобод граждан РФ в сфере информационной деятельности;
- совершенствование и защита отечественной информационной инфраструктуры, интеграция России в мировое информационное пространство;
- противодействие угрозе развязывания противоборства в информационной сфере.

Основу системы обеспечения национальной безопасности РФ составляют органы, силы и средства обеспечения национальной безопасности, осуществляющие меры политического, правового, организационного, экономического, военного и иного характера, направленные на обеспечение безопасности личности, общества и государства.

Полномочия органов и сил обеспечения национальной безопасности РФ, их состав, принципы и порядок действий определяются соответствующими законодательными актами РФ.

## 1.2. Влияние процессов информатизации общества на составляющие национальной безопасности и их содержание

Процесс информатизации затронул практически все стороны жизни общества. В соответствии с Федеральным законом от 20.02.1995 г. № 24-ФЗ «Об информации, информатизации и защите информации» под **информатизацией** понимается 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.

В настоящее время невозможно себе представить деятельность крупных банков, промышленных и торговых предприятий, транспортных организаций, правоохранительных органов без соответствующих баз данных и высокопроизводительной вычислительной техники.

Условно можно выделить следующие составляющие национальной безопасности: экономическую, внутриполитическую, социальную, духовную, международную, информационную, военную, пограничную, экологическую.

Содержание каждой из перечисленных составляющих отражено в соответствующих нормативных правовых актах.

Информатизация является характерной чертой жизни современного общества. Новые информационные технологии активно внедряются во все сферы народного хозяйства. Компьютеры управляют космическими кораблями и самолетами, контролируют работу атомных электростанций, распределяют электроэнергию и обслуживают банковские системы. Компьютеры являются основой множества автоматизированных систем обработки информации (АСОИ), осуществляющих хранение и обработку информации, предоставление ее потребителям, реализуя тем самым современные информационные технологии.

По мере развития и усложнения средств, методов и форм автоматизации процессов обработки информации повышается зависимость общества от степени безопасности используемых им информационных технологий, от которых порой зависит благополучие, а иногда и жизнь многих людей.

Актуальность и важность проблемы обеспечения безопасности информационных технологий обусловлены такими причинами, как:

- резкое увеличение вычислительной мощности современных компьютеров при одновременном упрощении их эксплуатации;
- резкое увеличение объемов информации, накапливаемой, хранимой и обрабатываемой с помощью компьютеров и других средств автоматизации;
- сосредоточение в единых базах данных информации различного назначения и различной принадлежности;
- высокие темпы роста парка персональных компьютеров, находящихся в эксплуатации в самых разных сферах деятельности;
- резкое расширение круга пользователей, имеющих непосредственный доступ к вычислительным ресурсам и массивам данных;
- бурное развитие программных средств, не удовлетворяющих даже минимальным требованиям безопасности;
- повсеместное распространение сетевых технологий и объединение локальных сетей в глобальные;
- развитие глобальной сети Интернет, практически не препятствующей нарушениям безопасности систем обработки информации во всем мире.

# 2. Информационная безопасность в системе национальной безопасности Российской Федерации

## 2.1. Основные понятия, общеметодологические принципы обеспечения информационной безопасности

К основным понятиям в области обеспечения информационной безопасности относятся понятия «информация», «информационная сфера» и «информационная безопасность».

Приведем здесь два подхода к определению понятия «информация» [8, 9].

Первый подход сводится к следующему. В философской литературе «информация» раскрывается как «одно из наиболее общих понятий науки, обозначающее некоторые сведения, совокупность каких-либо данных, знаний и т. п.» [6]. При этом отмечается, что «само понятие «информация» обычно предполагает наличие по крайней мере трех объектов: источника информации, потребителя информации и передающей среды. Информация не может быть передана, принята или хранима в чистом виде. Носителем информации является сообщение.

Отсюда следует, что понятие «информация» включает два основных элемента: сведения и сообщения.

Сведения выполняют несколько основных функций [8]:

- познание окружающего мира (гносеологическая), включающее формирование представлений о структуре окружающей среды, накопление знаний о закономерностях изменения объектов среды и протекающих в ней процессов; оценку состояния этих процессов;
- социальная коммуникация (коммуникативная), включающая формирование представлений о способах удовлетворения базовых и вторичных потребностей, формирование представлений о правилах поведения в обществе, взаимодействия с другими людьми, о нравственных ценностях, формирование личностных шкал ценности материальных и духовных благ, которые могут быть использованы для удовлетворения его потребностей, а также допустимости использования для овладения ими известных средств и т. д.;
- удовлетворение потребностей (прагматическая), включающее целеполагание, т. е. формирование, оценку и выбор целей, достижение которых способствует удовлетворению базовых и вторичных потребностей человека, и целедостижение как управление своей деятельностью по достижению выбранных целей.

Все множество накопленных человеком сведений может быть представлено в виде некоторой «базы знаний», в которой располагаются образы, возникающие в результате осознания полученных сообщений, ощущения, вызванные этими образами, эмоциональные и прагматические оценки этих образов. Между «объектами» «базы» могут быть установлены определенные ассоциативные отношения. Совокупность сохраняющихся у человека образов, ощущений, оценок с установившимися ассоциативными отношениями между ними образует знания.

Данная «база» составляет основное содержание информационной модели человека.

Мышление может быть представлено в виде процесса формирования на основе имеющихся у человека сведений и знаний новых ассоциативных связей между объектами, расположенными в его «базе».

Объем информации, имеющейся у человека в форме сведений, может быть измерен количеством накопленных им ощущений, образов, оценок и ассоциативных отношений между ними. Чем больше этих ощущений, образов и оценок, тем большим объемом информации располагает человек. Соответственно количество информации, поступающей к человеку посредством сообщения, может быть измерено количеством новых объектов «базы» (ощущений, образов, оценок, отношений между элементами «базы»), проявляющихся в результате осознания сообщения.

Ценность информации, проявляющейся в форме сведений, определяется субъективной важностью задачи, для решения которой данные сведения могут быть использованы, а также тем влиянием, которое оказали сведения на решение задачи. Это влияние может выражаться в изменении концептуальной модели задачи, в изменении приоритетов между возможными вариантами ее решения, в оценке целесообразности решения задачи вообще.

Информация, поступающая к человеку в форме сведений, обладает рядом свойств:

- *идеальностью* - существованием только в сознании человека и вследствие этого невозможностью восприятия органами чувств;
- *субъективностью* - зависимостью количества и ценности сведений от информационной модели субъекта, получающего сведения;
- *информационной неуничтожаемостью* - невозможностью уничтожения сведений другими сведениями, полученными человеком;
- *динамичностью* - возможностью изменения ценности имеющихся сведений и знаний под воздействием времени, других поступающих сведений;
- *накапливаемостью* - возможностью практически неограниченного накопления сведений в информационной модели человека.

Способность получать, накапливать и использовать для обеспечения жизнедеятельности информацию в форме сведений является свойством всех живых объектов, однако объем и содержание выполняемых с их использованием функций у различных классов этих объектов существенно отличаются. Так, можно предположить, что функцию целеполагания выполняет только человек.

Информация в форме сведения вследствие идеального характера достаточно редко выступает в качестве объекта научных исследований.

К числу изучающих ее отраслей науки можно отнести психологию и медицину.

2. Понятие «сообщение» часто определяется как «кодированный эквивалент события, зафиксированный источником информации и выраженный с помощью последовательности условных физических символов (алфавита), образующих некоторую упорядоченную совокупность» [7].

С интересующей нас точки зрения сообщения используются, прежде всего, для передачи сведений другим людям и составляют существо представительной стороны информации, или ее представительной формы. Информация в форме сообщения появляется как реализация способности человека описывать сведения на некотором языке, представляющем собой совокупность лексики и грамматики.

Человек, формируя сообщение, выделяет часть своей информационной модели, которую хочет передать, устанавливает отношения между ее элементами и известными ему понятиями. С помощью языка в некотором алфавите он осуществляет кодирование понятий, получая в результате систематизированный набор знаков, который может быть передан другим людям, т. е. происходит объективизация содержательной стороны информации и соответствующие сведения как бы становятся доступны для восприятия органами чувств.

Воспринимая сообщение, человек устанавливает отношения между составляющим его набором букв и знаков и известными ему понятиями, а затем - образами, ощущениями, оценками, ассоциативными отношениями, т. е. преобразовывает представительную форму информации в ее содержательную форму.

Исходя из этого, сообщение может быть представлено как совокупность набора передаваемых сведений и порядка (алгоритмов) их кодирования в набор знаков сообщения и декодирования в сведения. Без алгоритма кодирования сообщение превращается просто в набор знаков.

Человек как источник информации может обмениваться с технической системой сообщениями только в том случае, если в ней заложен определенный алгоритм декодирования передаваемого набора знаков, их последующей обработки, а также алгоритм кодирования для передачи человеку-потребителю ответного сообщения.

Преобразование информации из сведений в сообщения и из сообщений в сведения составляет существо общего закона обращения информации.

Информация в форме сообщения обладает рядом свойств, к числу которых следует отнести:

- *материальность* - способность воздействовать на органы чувств;

- *измеримость* - возможность количественной оценки параметров сообщения (количество знаков, составляющих сообщение);
- *сложность* - наличие набора знаков и алгоритмов их кодирования и декодирования;
- *проблемная ориентированность* - содержание сведений, относящихся к одной их задач человеческой деятельности.

Информация в форме сообщений наиболее часто исследуется с технической, семантической и прагматической точек зрения.

С технической точки зрения сообщения представляют интерес как объект передачи по каналам связи. При этом изучаются вопросы надежности, устойчивости, оперативности, дальности, помехозащищенности передачи сообщений, в некоторых случаях - скрытности передачи, а также принципы и методы проектирования систем передачи сообщений, средств их защиты от несанкционированного доступа.

К числу наиболее выдающихся результатов, полученных в этой области, обычно относят создание теории информации и кибернетики.

Представляется, что количество информации по Шеннону может интерпретироваться как количество новых объектов «информационной модели» человека, которые должны возникнуть после его получения при условии, что человек, получающий сообщение, не имел никаких сведений как о существовании объекта информирования, так и о его свойствах.

С семантической точки зрения сообщения представляют интерес как средство передачи сведений, т. е. совокупность набора знаков, полученного в результате кодирования и требующего декодирования для использования в практической деятельности. Данные свойства сообщения изучаются, например, в криптографии, искусствоведении и филологии.

С прагматической точки зрения сообщения исследуются как средство воздействия на информационную модель человека, детерминирования его поведения. Учитывая, что сообщение служит средством передачи сведений, ему могут быть приписаны те или иные свойства данных сведений, после чего оно, сообщение, может рассматриваться в качестве некоторого их аналога, обладающего ценностью, достоверностью, своевременностью и т. д. С этой точки зрения информация изучается в педагогике, юриспруденции, социологии, политологии, технических науках.

Второй подход к определению понятия «информация» состоит в следующем [9]. Термин «информация» в настоящее время исключительно популярен. Если не пытаться дать ему четкое определение, а применять в общепринятом бытовом смысле, мы действительно входим в «информационную эпоху».

Есть некоторая историческая аналогия «информационной эпохи» XX в. и «эпохи электричества» в XIX в. Еще многое было непонятно в природе явления, с термином «электричество» связывались зачастую наивные и фантастические представления, но он был столь же популярен. Сегодня физика достаточно полно объясняет крайне сложные электромагнитные процессы, обеспечивает базу для создания разнообразнейших электрических устройств и систем, проникающих во все области жизни, но надо признать, что сам факт существования электрического заряда мы воспринимаем на том же уровне древних, мы знаем только, что он - заряд - есть. При этом мы уже осознали, что задолго до появления не только знания об электричестве, но и человека как такового электромагнитные явления (начиная от энергии света) определяли развитие жизни, т. е. «эпоха электричества» изначальна.

Информационные процессы, целенаправленно формируемые человеком, уже сегодня во многом поддаются описанию в понятиях математической теории информации. Однако с первых шагов формирования этой области науки отмечалось противоречие между конкретным, весьма ограниченным предметом научного описания и исключительно широким общепринятым пониманием термина «информация».

Один из признанных основоположников современной теории информации - Р. В. Л. Хартли, определяя предмет своего исследования, отмечал в 1928 г.: «В обычном понимании термин «информация» слишком эластичен; необходимо прежде всего установить для него специфический смысл...» [10]. Специфика смысла для Хартли определялась процессом передачи сигналов. При этом, подчеркивая необходимость исключения психологических факторов, он ни в коей мере не ставил под сомнение существование двух разумных операторов: формирующего и воспринимающего сигнал. В таком смысле термин «информация» получает совершенно конкретное узкое значение. Например, он не может быть применен для описания процесса наблюдения за пассивным объектом. Крайнее несоответствие узкого значения термина «информация» его общепринятому интуитивному содержанию отмечалось многими исследователями. Так, К. Черри отмечает: «В определенном смысле вызывает сожаление то обстоятельство, что математическое понятие, введенное Хартли, стало вообще называться информацией» [11].

Отметим, что в отличие от электричества роль информации в жизни человека была интуитивно осознана с древнейших времен. «Вначале было слово...» - мысль, пронизывающая сознание человека во все времена. Материалистическое направление в философии отказалось от идей субъекта - носителя основополагающей информации, но никак не от ее существования, приняв за факт «законы природы». Состояние науки в XIX в.

давало основание полагать, что модель мира сведется к крайне ограниченному комплекту частиц вещества и не менее ограниченному количеству «законов». Носитель «закона» выводился из рассмотрения (аналогично «заряду» - он есть, существует по определению). В середине XX в. развитие теории и практики заставило изменить подход. Теоретическая физика пришла к осознанию несводимости модели мира к нескольким простейшим законам. С другой стороны, развитие автоматических систем уже в 50-е гг. привело к пониманию исключительной информационной сложности даже простейших самоуправляемых систем. В конце концов в советской школе материалистической философии сформировалось представление об информации как некоей третьей (вместе с веществом и энергией) форме проявления материального мира, отражающей изменчивость материи. Не углубляясь во внутрифилософские проблемы, воспользуемся таким подходом, не очень отличающимся от подходов других школ (не слишком экстремистских).

Становление кибернетики потребовало анализа с позиций точной науки процессов в самоуправляющихся системах, анализа процессов формирования модели внешнего мира, формирования знания. Возможно, из-за естественной связи кибернетики с математической теорией информации произошло распространение термина «информация» на приращение знания субъекта. По Винеру, «информация - это обозначение содержания, черпаемого нами из внешнего мира в процессе нашего приспособления к нему и приведения в соответствие с ним нашего мышления» [12].

Таким образом, в сложившемся применении термина «информация» можно выделить три направления. Основная мысль заключается в том, что эти три направления соответствуют трем совершенно различным сущностям, между которыми существует связь; в конкретных случаях может быть установлено какое-то частное соотношение, но природа их различна, и не может быть речи о какой-либо эквивалентности, взаимном преобразовании или превращении.

То, что при описании этих сущностей, особенно в русскоязычной речи, применяется одно заимствованное, иноязычное слово - «информация», - весьма печальное обстоятельство, приводящее ко многим недоразумениям. Представляется, что, поскольку «информационная эпоха» действительно наступает, назрела необходимость уточнить содержание понятия «информация» и найти разные определения для различных сущностей.

Автор статьи [9] не претендует, по его признанию, на оригинальность в постановке этого вопроса. По существу, именно на его решение были направлены попытки создания «качественной», семантической и т. п.

теории информации, которые, несмотря на участие в них крупнейших специалистов, пока не дали существенных завершенных результатов. На решение этой проблемы - одной из центральных в понимании информационных процессов - авторы также ни в коей мере не претендуют. Ниже излагается только ряд соображений, направленных на более четкое определение информации в задачах информационной безопасности.

Прежде всего, несколько уточним определения трех вышеупомянутых предметов рассмотрения.

Информация «в философском смысле». Назовем ее ***автономной информацией.*** Автономная - в смысле объективно существующая, независимо от какого-либо субъекта. Эта информация - особое проявление материи, противостоящее хаосу, - определяет процессы изменения материального мира, но в рамках представлений современной точной науки непосредственно человеком не воспринимается.

Информация «по Винеру». Это - приращение знания, изменение модели окружающего мира, возникающее в процессе взаимодействия самоуправляющейся системы с окружающей средой. Назовем ее ***информацией воздействия***.

Самоуправляющаяся система - субъект - всегда включает в себя в какой-то форме модель внешнего мира - «знание». Физические процессы воздействия внешней среды на самоуправляющуюся систему могут приводить к изменению модели - к приращению знания. Субъектом может быть человек, коллектив, организация, государство, в пределе - все человечество. Рассмотрение в качестве субъекта какого-либо искусственного устройства в принципе не исключается, но при существующем состоянии работ в области искусственного интеллекта несколько преждевременно. Будем считать понятие «информация воздействия» как некоторую характеристику процесса формирования модели внешнего мира. Информация воздействия не может быть определена через отдельно взятые свойства внешней среды или физического процесса взаимодействия внешней среды и субъекта или свойства модели. Для возникновения приращения знания воздействие должно частично, но не исчерпывающе описываться существующей моделью, причем соответствующая область модели должна быть активизирована. В противном случае воздействие воспринимается без развития модели, т. е. оно может быть информативным или неинформативным.

Информация воздействия - совокупная характеристика среды, процесса взаимодействия, субъекта, статического и динамического состояния его модели мира.

Для любого другого субъекта - внешнего наблюдателя - оценка информации воздействия возможна только в виде гипотезы, подтверждае-

мой или опровергаемой последующими действиями наблюдаемого субъекта, испытавшего воздействие внешней среды.

Информация «по Хартли». Назовем ее ***информацией взаимодействия.***

Частным случаем воздействия является воздействие другого субъекта, имеющее целью согласование в некотором смысле моделей внешней среды двух субъектов или коллектива. При этом предполагается существование предварительно согласованных областей моделей - соглашение о языке общения. Отметим, что понятие «согласование моделей» не обязательно подразумевает согласование целей субъектов. При их противоборстве «согласование» может иметь целью искажение модели внешней среды у противника.

Отметим также, что процесс взаимодействия внутренне достаточно сложен. Субъект, инициирующий воздействие, - передатчик - формирует на основе некоторой области своей модели физический процесс - сообщение. При этом привлекаемую часть модели субъекта-передатчика можно было бы характеризовать «информацией передатчика», а сообщение - «информацией сообщения». Сообщение, воздействуя с воспринимающего субъекта, может при условии его статической и динамической готовности сформировать некоторую информацию воздействия - «информацию приемника». В этом процессе наблюдаемым элементом является только сообщение и в этом смысле информация взаимодействия совпадает с информацией сообщения. В данном контексте «взаимодействие» - более подходящий термин, так как в явном виде подразумевает наличие нескольких участников процесса.

Таким образом:

автономная информация существует ***независимо от наличия субъекта,*** в рамках современных представлений точной науки ***непосредственно не воспринимается;***

информация воздействия может рассматриваться ***только в системе, включающей активного субъекта*** с учетом состояния его модели внешнего мира, другими субъектами непосредственно не воспринимается и ***может вероятностно оцениваться*** по предыдущему и последующему поведению субъекта, испытывающего воздействие;

информация взаимодействия существует *в системе* ***нескольких субъектов,*** связана с целенаправленно формируемым физическим процессом и в этом виде ***полностью воспринимается.***

В то же время сам процесс взаимодействия включает три составляющие:

- информационную базу передатчика, определяемую как часть знания, используемую при формировании сообщения;

- информацию сообщения, определяемую как соглашение о языке общения, - собственно информацию взаимодействия;
- информацию приемника, определяемую как информацию воздействия воспринимающего субъекта.

Эти три компонента несводимы к одному качественному или количественному описанию.

Информационная база передатчика и информация приемника значимы содержательно, но по содержанию неэквивалентны. При получении сообщения группой приемников каждый из них воспринимает свою информацию воздействия, и эти информации приемников также неэквивалентны по содержанию.

Информация сообщения характеризует физический процесс в плане соглашения о языке общения и может рассматриваться каждым субъектом, освоившим язык общения, изолированно от других субъектов-участников процесса общения и в отрыве от содержания.

Рассмотрим ситуацию с точки зрения информационной безопасности. Выделим 4 компонента, в той или иной мере присутствующие во всех подходах к понятию информационной безопасности:

- обеспечение для субъекта доступа к достаточно полной и достоверной информации, необходимой для реализации его прав и обязанностей в обществе;
- защиту субъекта от деструктивных информационных воздействий;
- защиту от несанкционированного воздействия на информацию, принадлежащую субъекту;
- защиту информационной инфраструктуры группы субъектов (организации, государства...) от разрушительных воздействий.

Первые три компонента связаны с безопасностью знаний, т. е. для защищаемого объекта значима именно информация воздействия.

Основным предметом информационного нападения, целью, всегда является информация воздействия, т. е. то, что воспринимает субъект-нападающая сторона в случае попытки несанкционированного получения информации или объект нападения в случае попытки дезинформации, искажения информации, введения отвлекающей информации.

В то же время непосредственному наблюдению, использованию в технической разработке, в юридической практике доступна только информация сообщений и физические действия субъектов.

Например, объектом защиты может быть только конкретный документ (в широком смысле) как физический объект, целями противодейст-

вия - конкретные физические действия нападающего субъекта, прогнозируемые моделью нападения, но никак не получаемая или вводимая им информация воздействия.

Таким образом, системная задача обеспечения информационной безопасности, с одной стороны, и конкретные задачи технической, юридической и других подсистем, с другой - имеют разные предметы действий; именно поэтому система информационной безопасности есть не простая сумма различных (правовых, организационных, технических) компонентов, но качественно отличное явление. Существующее смешение понятий, объединение под одним термином «информация» различных предметов приводит либо к неоправданным попыткам оценивать содержательную сторону информационного процесса неадекватными методами, либо к самоограничению на уровне защиты исключительно документированной информации. И то и другое в конце концов приводит к нарушению защищенности объекта, создается объективная основа для произвольного определения факта нападения и для неадекватных действий защищающейся стороны.

Формирование системы, обеспечивающей информационную безопасность объекта, требует обычно решения ряда задач, связанных с формализованной информацией - информацией взаимодействия в форме документов или обменных сигналов технических систем. В этих случаях вполне применимы методы математической теории информации и удается сформировать весьма точные значения параметров, характеризующих защищенность системы на уровне информации взаимодействия. Однако для полной оценки защищенности эти параметры приходится сопоставлять с оценками для не поддающейся непосредственному доступу информации воздействия.

Например, можно достаточно достоверно оценить вероятность восстановления отдельного слова в перехваченном речевом сообщении (допустим 5 или 12 %). После этого возникает вопрос, какая вероятность допустима. Получить такую оценку можно только экспертным путем, попытки и здесь применить методы математической теории информации создают некоторое наукообразие, но, по сути, неэффективны, так как результат полностью определяется исходными допущениями, формируемыми фактически произвольно. Для различных ситуаций, различного содержания фраз, различного словарного состава экспертные оценки могут дать результаты, отличающиеся на порядок.

Невозможно отрицать тот факт, что сегодня методы, техника, критерии защиты информации в негосударственном секторе явно или неявно заимствованы из многие годы существовавшей государственной системы. Не входя в рассмотрение вопроса, насколько юридически приемлемо

это было сделано, отметим, что по отношению к техническим проблемам такое заимствование достаточно корректно - и законы физики, и методы математической теории информации инвариантны по отношению к формам собственности. В то же время по отношению к содержательной стороне информационных процессов такая экстраполяция ничем не обоснована.

Представляется, что назрела необходимость разработки корпоративных нормативов защищенности содержательной информации, соответствующих информационной специфике конкретных групп защищаемых объектов и конкретным информационным процессам, характерным для этих объектов. Одновременно необходима постановка задачи научного формирования перечня терминов, охватывающего не столько прикладные, сколько фундаментальные понятия в области информационных процессов.

Наконец, несколько слов о проблемах информационной защиты применительно к автономной информации. Научного обоснования возможности ее непосредственного восприятия нет. Нет и обоснования невозможности. Нет и обоснованной оценки граничной сложности объектов, поведение которых определяется автономной информацией. Представление о высокой степени детерминированности поведения микрочастицы и недетерминированности поведения на человеческом уровне, строго говоря, ничем, кроме естественного антропоцентризма, обосновать нельзя. В реальной же действительности при защите ответственного объекта проблему игнорировать невозможно, хотя все понимают сопровождающую ее бездну спекуляций и шарлатанства.

Современный этап развития общества характеризуется возрастающей ролью информационной сферы. Информационная сфера представляет собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений [13].

Информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности РФ. Национальная безопасность РФ существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать [13].

Под информационной безопасностью РФ понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства [13].

Государственная политика обеспечения информационной безопасности РФ основывается на следующих основных принципах [13]:

- соблюдении Конституции РФ, законодательства РФ, общепризнанных принципов и норм международного права при осуществлении деятельности по обеспечению информационной безопасности РФ;
- открытости в реализации функций федеральных органов государственной власти, органов государственной власти субъектов РФ и общественных объединений, предусматривающей информирование общества об их деятельности с учетом ограничений, установленных законодательством РФ;
- правовом равенстве всех участников процесса информационного взаимодействия вне зависимости от их политического, социального и экономического статуса, основывающемся на конституционном праве граждан на свободный поиск, получение, передачу, производство и распространение информации любым законным способом;
- приоритетном развитии отечественных современных информационных и телекоммуникационных технологий, производстве технических и программных средств, способных обеспечить совершенствование национальных телекоммуникационных сетей, их подключение к глобальным информационным сетям в целях соблюдения жизненно важных интересов РФ.

## 2.2. Национальные интересы в информационной сфере

Доктрина информационной безопасности РФ дает две классификации национальных интересов в информационной сфере:

- первую классификацию можно назвать классификацией по принадлежности интересов;
- вторую классификацию можно назвать классификацией по важности интересов.

В соответствии с первой классификацией национальные интересы - это совокупность интересов личности, интересов общества и интересов государства (рис. 1.1-1.4).

| | |
|---|---|
| Интересы личности | Национальные интересы |
| Интересы общества | |
| Интересы государства | |

Рис. 1.1. Состав национальных интересов

| *Интересы личности* |
|---|
| • Реализация **конституционных прав** на доступ к информации. |
| • Использование информации в интересах осуществления не запрещенной законом **деятельности.** |
| • Физическое, духовное и интеллектуальное **развитие.** |
| • Защита информации, обеспечивающей **личную безопасность.** |

Рис. 1.2. Содержание интересов личности в информационной сфере

| *Интересы общества* |
|---|
| • Обеспечение **интересов личности** в информационной сфере. |
| • Упрочение **демократии,** создание правового, социального государства. |
| • Достижение и поддержание **общественного согласия.** |
| • **Духовное обновление** России. |

Рис. 1.3. Содержание интересов общества в информационной сфере

| *Интересы государства* |
|---|
| • Гармоничное развитие российской информационной **инфраструктуры.** |
| • Реализация **конституционных прав человека** и гражданина в области получения информации и пользования ею. |
| • Незыблемость **конституционного строя, суверенитета и территориальной целостности** России. |
| • **Политическая, экономическая и социальная** стабильность. |
| • Безусловное обеспечение **законности** и **поддержание правопорядка.** |
| • Развитие равноправного и взаимовыгодного **международного сотрудничества.** |

Рис. 1.4. Содержание интересов государства в информационной сфере

Вторая классификация национальных интересов в информационной сфере связана, видимо, с оценкой важности этих национальных интересов и выделение изо всей их совокупности четырех наиболее важных. Соответственно в рамках этой классификации выделяют четыре основные составляющие национальных интересов РФ в информационной сфере [13].

1. Соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.

2. Информационное обеспечение государственной политики РФ, связанное с доведением до российской и международной общественности достоверной информации о государственной политике РФ, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам.

3. Развитие современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов. В современных условиях только на этой основе можно решать проблемы создания наукоемких технологий, технологического перевооружения промышленности, приумножения достижений отечественной науки и техники. Россия должна занять достойное место среди мировых лидеров микроэлектронной и компьютерной промышленности.

4. Защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России.

Первая составляющая национальных интересов РФ в информационной сфере (соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны) предполагает [13]:

- повышение эффективности использования информационной инфраструктуры в интересах общественного развития, консолидацию российского общества, духовное возрождение многонационального народа РФ;
- совершенствование системы формирования, сохранения и рационального использования информационных ресурсов, составляющих основу научно-технического и духовного потенциала РФ;
- обеспечение конституционных прав и свобод человека и гражданина свободно искать, получать, передавать, производить и распространять информацию любым законным способом, получать достоверную информацию о состоянии окружающей среды;

- обеспечение конституционных прав и свобод человека и гражданина на личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, на защиту своей чести и своего доброго имени;
- укрепление механизмов правового регулирования отношений в области охраны интеллектуальной собственности, создание условий для соблюдения установленных федеральным законодательством ограничений на доступ к конфиденциальной информации;
- обеспечение свободы массовой информации и запрет цензуры;
- недопущение пропаганды и агитации, которые способствуют разжиганию социальной, расовой, национальной или религиозной ненависти и вражды;
- запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия и другой информации, доступ к которой ограничен федеральным законодательством.

Вторая составляющая национальных интересов РФ в информационной сфере (информационное обеспечение государственной политики РФ) предполагает [13]:

- укрепление государственных СМИ, расширение их возможности по своевременному доведению достоверной информации до российских и иностранных граждан;
- ускоренное формирование открытых государственных информационных ресурсов, повышение эффективности их использования.

Третья составляющая национальных интересов РФ в информационной сфере (развитие современных информационных технологий, отечественной индустрии информации) предполагает [13]:

- развитие и совершенствование инфраструктуры единого информационного пространства РФ;
- развитие отечественной индустрии информационных услуг и повышение эффективности использования государственных информационных ресурсов;
- развитие производства в РФ конкурентоспособных средств и систем информатизации, телекоммуникации и связи, расширение участия России в международной кооперации производителей этих средств и систем;

- обеспечение государственной поддержки отечественных фундаментальных и прикладных исследований, разработок в сферах информатизации, телекоммуникации и связи.

Четвертая составляющая национальных интересов РФ в информационной сфере (защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем) предполагает [13]:

- повышение безопасности информационных систем, включая сети связи, прежде всего безопасность первичных сетей связи и ИС федеральных органов государственной власти, органов государственной власти субъектов РФ, финансово-кредитной и банковской сфер, сферы хозяйственной деятельности, а также систем и средств информатизации вооружения и военной техники, систем управления войсками и оружием, экологически опасными и экономически важными производствами;
- ускоренное развитие отечественного производства аппаратных и программных средств защиты информации и методов контроля за их эффективностью;
- обеспечение защиты сведений, составляющих государственную тайну;
- расширение международного сотрудничества РФ в области развития и безопасного использования информационных ресурсов, противодействия угрозе развязывания противоборства в информационной сфере.

## 2.3. Источники и содержание угроз в информационной сфере

По своей общей направленности угрозы информационной безопасности РФ подразделяются на следующие виды [13]:

- угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;
- угрозы информационному обеспечению государственной политики РФ;
- угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;

- угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.

Угрозами конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России могут являться:

- принятие федеральными органами государственной власти, органами государственной власти субъектов РФ нормативных правовых актов, ущемляющих конституционные права и свободы граждан в области духовной жизни и информационной деятельности;
- создание монополий на формирование, получение и распространение информации в РФ, в том числе с использованием телекоммуникационных систем;
- противодействие, в том числе со стороны криминальных структур, реализации гражданами своих конституционных прав на личную и семейную тайну, тайну переписки, телефонных переговоров и иных сообщений;
- нерациональное, чрезмерное ограничение доступа к общественно необходимой информации;
- противоправное применение специальных средств воздействия на индивидуальное, групповое и общественное сознание;
- неисполнение федеральными органами государственной власти, органами государственной власти субъектов РФ, органами местного самоуправления, организациями и гражданами требований федерального законодательства, регулирующего отношения в информационной сфере;
- неправомерное ограничение доступа граждан к открытым информационным ресурсам федеральных органов государственной власти, органов государственной власти субъектов РФ, органов местного самоуправления, к открытым архивным материалам, к другой открытой социально значимой информации;
- дезорганизация и разрушение системы накопления и сохранения культурных ценностей, включая архивы;
- нарушение конституционных прав и свобод человека и гражданина в области массовой информации;

- вытеснение российских информационных агентств, средств массовой информации с внутреннего информационного рынка и усиление зависимости духовной, экономической и политической сфер общественной жизни России от зарубежных информационных структур;
- девальвация духовных ценностей, пропаганда образцов массовой культуры, основанных на культе насилия, на духовных и нравственных ценностях, противоречащих ценностям, принятым в российском обществе;
- снижение духовного, нравственного и творческого потенциала населения России, что существенно осложнит подготовку трудовых ресурсов для внедрения и использования новейших технологий, в том числе информационных;
- манипулирование информацией (дезинформация, сокрытие или искажение информации).

Угрозами информационному обеспечению государственной политики РФ могут являться [13]:

- монополизация информационного рынка России, его отдельных секторов отечественными и зарубежными информационными структурами;
- блокирование деятельности государственных средств массовой информации по информированию российской и зарубежной аудитории;
- низкая эффективность информационного обеспечения государственной политики РФ вследствие дефицита квалифицированных кадров, отсутствия системы формирования и реализации государственной информационной политики.

Угрозами развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов могут являться [13]:

- противодействие доступу РФ к новейшим информационным технологиям, взаимовыгодному и равноправному участию российских производителей в мировом разделении труда в индустрии информационных услуг, средств информатизации, телекоммуникации и связи, информационных продуктов, а также создание условий для усиления технологической зависимости России в области современных информационных технологий;

- закупка органами государственной власти импортных средств информатизации, телекоммуникации и связи при наличии отечественных аналогов, не уступающих по своим характеристикам зарубежным образцам;
- вытеснение с отечественного рынка российских производителей средств информатизации, телекоммуникации и связи;
- увеличение оттока за рубеж специалистов и правообладателей интеллектуальной собственности.

Угрозами безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России, могут являться [13]:

- противоправные сбор и использование информации;
- нарушения технологии обработки информации;
- внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;
- разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;
- уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;
- воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации;
- компрометация ключей и средств криптографической защиты информации;
- утечка информации по техническим каналам;
- внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти, предприятий, учреждений и организаций независимо от формы собственности;
- уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;
- перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации;

- использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии российской информационной инфраструктуры;
- несанкционированный доступ к информации, находящейся в банках и базах данных;
- нарушение законных ограничений на распространение информации.

Источники угроз информационной безопасности РФ подразделяются на внешние и внутренние. К внешним источникам относятся [13]:

- деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов РФ в информационной сфере;
- стремление ряда стран к доминированию и ущемлению интересов России в мировом информационном пространстве, вытеснению ее с внешнего и внутреннего информационных рынков;
- обострение международной конкуренции за обладание информационными технологиями и ресурсами;
- деятельность международных террористических организаций;
- увеличение технологического отрыва ведущих держав мира и наращивание их возможностей по противодействию созданию конкурентоспособных российских информационных технологий;
- деятельность космических, воздушных, морских и наземных технических и иных средств (видов) разведки иностранных государств;
- разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним.

К внутренним источникам относятся [13]:

- критическое состояние отечественных отраслей промышленности;
- неблагоприятная криминогенная обстановка, сопровождающаяся тенденциями сращивания государственных и криминальных структур в информационной сфере, получения криминальными структурами доступа к конфиденциальной информации, усиления влияния организованной преступности на жизнь общества, снижения степени

защищенности законных интересов граждан, общества и государства в информационной сфере;

- недостаточная координация деятельности федеральных органов государственной власти, органов государственной власти субъектов РФ по формированию и реализации единой государственной политики в области обеспечения информационной безопасности РФ;
- недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика;
- неразвитость институтов гражданского общества и недостаточный государственный контроль за развитием информационного рынка России;
- недостаточное финансирование мероприятий по обеспечению информационной безопасности РФ;
- недостаточная экономическая мощь государства;
- снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности;
- недостаточная активность федеральных органов государственной власти, органов государственной власти субъектов РФ в информировании общества о своей деятельности, в разъяснении принимаемых решений, в формировании открытых государственных ресурсов и развитии системы доступа к ним граждан;
- отставание России от ведущих стран мира по уровню информатизации федеральных органов государственной власти, органов государственной власти субъектов РФ и органов местного самоуправления, кредитно-финансовой сферы, промышленности, сельского хозяйства, образования, здравоохранения, сферы услуг и быта граждан.

# 3. Государственная информационная политика

## 3.1. Основные положения государственной информационной политики Российской Федерации

Государственная политика обеспечения информационной безопасности РФ определяет основные направления деятельности федеральных органов государственной власти и органов государственной власти субъек-

тов РФ в этой области, порядок закрепления их обязанностей по защите интересов РФ в информационной сфере в рамках направлений их деятельности и базируется на соблюдении баланса интересов личности, общества и государства в информационной сфере.

Государственная политика обеспечения информационной безопасности РФ основывается на принципах, приведенных в п. 2.1.

Государство в процессе реализации своих функций по обеспечению информационной безопасности РФ [13]:

- проводит объективный и всесторонний анализ и прогнозирование угроз информационной безопасности РФ, разрабатывает меры по ее обеспечению;
- организует работу законодательных (представительных) и исполнительных органов государственной власти РФ по реализации комплекса мер, направленных на предотвращение, отражение и нейтрализацию угроз информационной безопасности РФ;
- поддерживает деятельность общественных объединений, направленную на объективное информирование населения о социально значимых явлениях общественной жизни, защиту общества от искаженной и недостоверной информации;
- осуществляет контроль за разработкой, созданием, развитием, использованием, экспортом и импортом средств защиты информации посредством их сертификации и лицензирования деятельности в области защиты информации;
- проводит необходимую протекционистскую политику в отношении производителей средств информатизации и защиты информации на территории РФ и принимает меры по защите внутреннего рынка от проникновения на него некачественных средств информатизации и информационных продуктов;
- способствует предоставлению физическим и юридическим лицам доступа к мировым информационным ресурсам, глобальным информационным сетям;
- формулирует и реализует государственную информационную политику России;
- организует разработку федеральной программы обеспечения информационной безопасности РФ, объединяющей усилия государственных и негосударственных организаций в данной области;
- способствует интернационализации глобальных информационных сетей и систем, а также вхождению России в мировое информационное сообщество на условиях равноправного партнерства.

Совершенствование правовых механизмов регулирования общественных отношений, возникающих в информационной сфере, является приоритетным направлением государственной политики в области обеспечения информационной безопасности РФ.

Это предполагает:

- оценку эффективности применения действующих законодательных и иных нормативных правовых актов в информационной сфере и выработку программы их совершенствования;
- создание организационно-правовых механизмов обеспечения информационной безопасности;
- определение правового статуса всех субъектов отношений в информационной сфере, включая пользователей информационных и телекоммуникационных систем, и установление их ответственности за соблюдение законодательства РФ в данной сфере;
- создание системы сбора и анализа данных об источниках угроз информационной безопасности РФ, а также о последствиях их осуществления;
- разработку нормативных правовых актов, определяющих организацию следствия и процедуру судебного разбирательства по фактам противоправных действий в информационной сфере, а также порядок ликвидации последствий этих противоправных действий;
- разработку составов правонарушений с учетом специфики уголовной, гражданской, административной, дисциплинарной ответственности и включение соответствующих правовых норм в уголовный, гражданский, административный и трудовой кодексы, в законодательство РФ о государственной службе;
- совершенствование системы подготовки кадров, используемых в области обеспечения информационной безопасности РФ.

Правовое обеспечение информационной безопасности РФ должно базироваться прежде всего на соблюдении принципов законности, баланса интересов граждан, общества и государства в информационной сфере.

Соблюдение принципа законности требует от федеральных органов государственной власти и органов государственной власти субъектов РФ при решении возникающих в информационной сфере конфликтов неукоснительно руководствоваться законодательными и иными нормативными правовыми актами, регулирующими отношения в этой сфере.

Соблюдение принципа баланса интересов граждан, общества и государства в информационной сфере предполагает законодательное закреп-

ление приоритета этих интересов в различных областях жизнедеятельности общества, а также использование форм общественного контроля деятельности федеральных органов государственной власти и органов государственной власти субъектов РФ. Реализация гарантий конституционных прав и свобод человека и гражданина, касающихся деятельности в информационной сфере, является важнейшей задачей государства в области информационной безопасности.

Разработка механизмов правового обеспечения информационной безопасности РФ включает в себя мероприятия по информатизации правовой сферы в целом.

В целях выявления и согласования интересов федеральных органов государственной власти, органов государственной власти субъектов РФ и других субъектов отношений в информационной сфере, выработки необходимых решений государство поддерживает формирование общественных советов, комитетов и комиссий с широким представительством общественных объединений и содействует организации их эффективной работы.

### 3.2. Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности

Первоочередными мероприятиями по реализации государственной политики обеспечения информационной безопасности РФ являются [13]:

- разработка и внедрение механизмов реализации правовых норм, регулирующих отношения в информационной сфере, а также подготовка концепции правового обеспечения информационной безопасности РФ;
- разработка и реализация механизмов повышения эффективности государственного руководства деятельностью государственных средств массовой информации, осуществления государственной информационной политики;
- принятие и реализация федеральных программ, предусматривающих формирование общедоступных архивов информационных ресурсов федеральных органов государственной власти и органов государственной власти субъектов РФ, повышение правовой культуры и компьютерной грамотности граждан, развитие инфраструктуры единого информационного пространства России, комплексное противодействие угрозам информационной войны, создание безопасных информационных технологий для систем, используемых в процессе реализации жизненно важных функций общества и государства, пресечение

компьютерной преступности, создание информационно-телекоммуникационной системы специального назначения в интересах федеральных органов государственной власти и органов государственной власти субъектов РФ, обеспечение технологической независимости страны в области создания и эксплуатации информационно-телекоммуникационных систем оборонного назначения;

- развитие системы подготовки кадров, используемых в области обеспечения информационной безопасности РФ;
- гармонизация отечественных стандартов в области информатизации и обеспечения информационной безопасности автоматизированных систем управления, информационных и телекоммуникационных систем общего и специального назначения.

# 4. Информация - наиболее ценный ресурс современного общества

## 4.1. Понятие «информационный ресурс»

Материал данного раздела основан на источнике [14]. Несмотря на все более широкое использование понятия «информационный ресурс», в настоящее время отсутствует его общепринятое определение, что делает проблематичным разработку эффективной политики любого уровня (международного, национального, регионального, республиканского и отраслевого) по созданию информационных ресурсов и их промышленной эксплуатации в интересах науки, техники, производства и управления.

Прежде всего необходимо обратить внимание на то, что понятие «информационный ресурс» возникло не в процессе переосмысления роли информации во всех видах общественной деятельности, как утверждают многие, а в результате внедрения в исследования по созданию и интеграции информационных служб программно-целевого подхода.

Ресурсами называют элементы экономического потенциала, которыми располагает общество и которые, при необходимости, могут быть использованы для достижения конкретных целей хозяйственного и социального развития [15].

В рамках программно-целевого подхода информация рассматривается как один из видов ресурсов при реализации целевых программ наряду с рабочей силой, материалами, оборудованием, энергией, денежными средствами и т. д.

Это означает, что информация стала рассматриваться как один из видов ресурсов, потребляемых в общественной практике.

Но включение информации в состав ресурсов не снимает неопределенности термина «информационный ресурс», поскольку нет однозначного подхода к тому, какую информацию считать ресурсом, а какую не считать. Анализ определений, приведенных в различных источниках, показывает, что в состав информационных ресурсов включается либо вся (любая) информация, либо ее подмножества, для выделения которых разные авторы используют различные, несовместимые друг с другом критерии, например: классы информации, и/или виды документов, и/или виды носителей (способы фиксации), и/или организационные структуры, и/или возможность обработки на различных технических средствах и др.

Информация в контексте данного раздела может трактоваться как знание, включенное непосредственно в коммуникативный процесс.

Исходным моментом включения информации в сферу обращения по различным социальным каналам является ее фиксация на тех или иных видах носителей - документирование (закрепление на тех или иных материальных носителях), ибо только в этом случае она может быть передана между пользователями и процессами, распределенными во времени и пространстве.

С момента фиксации знания на том или ином носителе оно становится информацией, и только эта информация может рассматриваться как информационный ресурс.

Каждый новый тип носителя информации порождает свой класс информационных ресурсов, характеризуемый своим множеством свойств, связанных с фиксацией, воспроизводством, доступом, восприятием и процессами обработки зафиксированной на носителе информации, а также реализацией процессов передачи информации во времени.

Обобщая изложенное, предлагается под информационными ресурсами понимать всю накопленную информацию об окружающей нас действительности, зафиксированную на материальных носителях и в любой другой форме, обеспечивающей ее передачу во времени и пространстве между различными потребителями для решения научных, производственных, управленческих и других задач.

Особо следует выделить положение о том, что ресурсом является вся накопленная информация, в том числе и информация недостоверная («дефектологическая»), представленная сомнительными фактами, ложными положениями, неэффективными подходами, а также устаревшая информация; несопоставимые данные, накопленные по нестандартным методикам; информация, потерявшая конкретность в результате субъективных толкований в процессе частных «теоретических» построений; за-

ведомая «дезинформация», поступившая в информационные потоки, и сбалансированная информация.

Только такой подход к определению информационных ресурсов создает предпосылки для выявления противоречивых данных, исключаются случаи пропуска «неудобной» информации и сложных ситуаций (под сложной ситуацией понимается информация о «необычном», «невозможном» использовании известных средств и методов, «принципиально невозможных» явлениях и действиях, т. е. всего того, что не укладывается в тезаурус отдельного исполнителя и/или целого коллектива исполнителей).

Учет фактора «дезинформирования» (возможности поступления к пользователю недостоверной и устаревшей информации) требует включения в процессы информационной деятельности специальных процедур оценки информации на достоверность. Без выявления недостоверной и устаревшей информации, накапливаемой в информационных ресурсах, создаются предпосылки принятия неэффективных, а в ряде случаев и ошибочных решений, наносящих существенный ущерб.

В то же время следует подчеркнуть, что недостоверная и устаревшая информация не должна уничтожаться. Она должна локализовываться, обособляться и на ее основе необходимо строить системные фильтры для контроля информационных ресурсов любого уровня (организаций, объединений, национальных и международных). При этом сама недостоверная информация должна непрерывно переоцениваться, уточняться и одновременно должны подвергаться переоценке решения, принятые ранее на основании такой информации.

Сбор всей информации и требование сохранности «дефектной», устаревшей информации лежит в основе деятельности наиболее эффективных информационных систем и является важным методологическим принципом их построения.

С другой стороны, когда мы говорим о том, что информационный ресурс - это вся информация, то имеется в виду мировой информационный ресурс, полнота и эффективность использования которого в настоящее время недостаточна и определяется уровнем достигнутого баланса соглашений на международной (через ООН), региональной, двух- и многосторонней основе между различными источниками и пользователями информационных ресурсов.

В реальной деятельности каждая из сторон обладает своим подмножеством информации, ограниченным по проблемам, полноте, качеству и актуальности для решения стоящих перед ней задач. Оно определяется как информационный ресурс конкретного пользователя (отдельного лица, группы лиц, предприятия, объединения, ведомства, региона, государства и т. д.).

В зависимости от носителей информация информационные ресурсы предлагается разделить на 5 основных классов:

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

При этом следует обратить особое внимание на то, что одна и та же информация, относящаяся к той или иной проблеме, может быть зафиксирована на различных носителях и/или различные информационные фрагменты одной и той же проблемы могут быть зафиксированы таким образом, что правильное восприятие информации становится невозможным, если отсутствует доступ ко всем информационным фрагментам, представленным на различных носителях.

Поэтому целостность информационных ресурсов обеспечивается в том и только том случае, если потребитель (пользователь) имеет доступ ко всем классам носителей, на которых зафиксирована информация, необходимая для решения стоящих перед ним задач.

Создание национальных информационных ресурсов невозможно (особенно в условиях динамически изменяющихся задач) без изучения и учета всей структуры связей между различными классами информационных ресурсов. Поэтому одной из важнейших задач построения эффективной информационной системы является создания в структуре документальных информационных ресурсов машиночитаемого регистра, который должен обеспечить координацию Использования информационных ресурсов организаций, фирм и государственных учреждений, работающих в различных областях.

## 4.2. Классы информационных ресурсов

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

Каждый новый тип носителя информации порождает свой класс информационных ресурсов, характеризуемый своим множеством свойств, связанных с фиксацией, воспроизводством, доступом, восприятием и процессами обработки зафиксированной на носителе информации, а также реализацией процессов передачи информации во времени.

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

В зависимости от носителей информации информационные ресурсы предлагается разделить на следующие основные классы.

1. Документы.
2. Персонал (память людей).
3. Организационные единицы.
4. Промышленные образцы, рецептуры и технологии, конструкционные материалы, программные продукты, технические системы (объекты).
5. Научный инструментарий.

Следует обратить внимание на то, что принятое в федеральном законе понятие информационных ресурсов значительно уже и включает только документы: «информационные ресурсы - отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, банках данных, других видах информационных систем)». (Федеральный закон от 04.07.1996 г. № 85-ФЗ «Об участии в международном информационном обмене. Ст. 2). Это же определение используется в Законе «Об информации, информатизации и защите информации».

Для обоснования принятого подхода к определению информационного ресурса сделаем следующие разъяснения, показывающие ограниченность и неполноту определения, используемого в законодательных документах.

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

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

2. Сужение понятия информационных ресурсов до класса документов исключает из рассмотрения значительные объемы информации, зафиксированные на иных классах носителей. Но каждый класс информационных ресурсов - это еще и иные способы взаимодействия с информационными ресурсами, способы их создания, регистрации, сбора, сохранения, взаимодействия с ними и, следовательно, иные способы управления информационными технологиями, а также иная правовая база, определяющая их использование.
3. Разрыв информационных связей между выделенными классами информационных ресурсов порождает разрывы в информационных процессах и технологиях. Это, в свою очередь, ведет к потере целостности восприятия окружающей действительности, резкому снижению качества информации и результативности при принятии информационных решений.
4. Создаются предпосылки к безвозвратной утрате важнейшей информации, которая не может быть содержательно осмыслена только на основе документальных информационных ресурсов. Учет только документальных информационных ресурсов может привести к полной утрате конкретной проблемной информации.
5. Нарушение целостности понимания информационных ресурсов создает предпосылки к нарушению информационной безопасности.

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

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

1. В уголовной практике.

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

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

- создание коллекций оружия для отождествления типа оружия по боеприпасу;
- коллекции гильз («гильзотеки») и использованных пуль, для прослеживания движения «стволов» по преступлениям.

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

3. В экспертизе, метрологии, сельском хозяйстве:

- эталонные образцы, реактивы и пр.;
- реперные объекты (например, кронштадтский футшток («уровень моря»); гринвичский и пулковский меридианы, системы мегалитических памятников (как материализованная фиксация астрономических знаний древности (скрытые и «раскрытые»), геодезические знаки опорной геодезической сети (по классам точности);
- «линии производителей», элитный семенной материал и пр.;
- мощнейший инструментальный комплекс «эталонного времени», сеть сейсмических и метеорологических станций, контрольно-измерительные полигонные комплексы (данный пример может быть примером класса «организационная единица» в чистом виде).

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

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

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

Например:

- многократные переоценки экспедиционных материалов по тунгусскому метеориту;
- новые оценки гипотезы «жизни на Марсе» по результатам анализа метеоритного материала.

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

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

8. «Персонал» для выполнения специфических работ:

- Специальные группы экспертов для проведения органолептических оценок (виноделие, производство парфюмерных изделий и др.). Это класс информационных ресурсов «персонал» - в чистом виде.
- Специфические профессиональные группы: испытатель (всех категорий), проводник, лоцман, «колодезник», следопыт, некоторые специалисты таможенных профессий и др.
- «Язык», свидетель (утрата свидетеля в ряде случаев ведет к «развалу» дела), «пленный».
- Оперативные работники, резидентура, специалисты по опознанию.
- Особо доверенные лица («хранители тайн»): в древности - особо посвященные члены религиозных групп, вожди племен; хранители утерянных тайн (греческий огонь, сокровища инков, целые системы знаний древних и пр.); в современной истории - три специалиста, сохраняющие рецепт кока-колы; хранители тайн ценностей и местонахождения документохранилищ германского рейха (по решениям совещания 1944); полная группа хранителей кодовых комбинаций (ключей) «особых кладовых»; «старшие призыва» (в германской армии) и другие подобные персоны и группы.
- Группы «трофейных специалистов»: группа Брауна, Гелен, Гесс, Паулюс на Нюрнбергском процессе и др.
- «Законсервированная» резидентура.

9. В принципе понятие машиночитаемого информационного ресурса и сам машиночитаемый документ не могут существовать без некоторого инструментального комплекса (*0* - «промышленного образца»), который превращает носитель с зафиксированной на нем информацией в документ, доступный пользователю.

Есть инструментальный комплекс - существует документ, нет инструментального комплекса - нет документа!! А следовательно, нет информационного ресурса!

10. Самолет-лидер, точные «двойники» космических аппаратов на земле, синхронно с основным работающие на земле и на которых прохо-

дит обследование внештатных ситуаций. Указанные образцы выполняют роль долговременного эталонного дублера основного объекта на все время его существования.

11. Приведем высказывания, свидетельствующие о том, что Туполев рассматривал персонал, промышленные образцы и организации (КБ, школы) в качестве основной составляющей части того, что мы именуем информационным ресурсом. Одновременно необходимо обратить внимание на то, что знание, зафиксированное в книге (документе), для него вторично, неоперативно. Накопление конструкций, технических решений, «новшеств» (закрепленных в конструкциях с той или иной степенью реализации, проверенных в действии, на стенде и т. д.) - основа успешного решения практических задач.

С некоторой степенью условности его можно считать сторонником (по крайней мере после завершения специального образования) передачи знаний и умений в процессе совместной работы над реальными проектами: «Наша работа, результатом которой является постройка самолетов, отнимает настолько много сил и энергии, что я ни одной строчки не пишу. Вы должны рассматривать как оправдание результаты, которые мы даем. *Я* просил бы, чтобы эта точка зрения была принята всеми...» Еще одна цитата: «Мы расширяем круг лиц, которые могут принять от нас работу... Никто с должной отчетливостью не представляет того напряжения в отделе, в смысле передачи опыта и знаний, которое у нас создалось. Если возьмете каждого из сотрудников, вы увидите, сколько человек у каждого из них учатся. Создается школа, которая имеет очень большое значение. Передаем ли мы свои знания в промышленность? Передаем. Например, возьмите 5-й завод - много взял от бомбовоза. Это - передача опыта в наивысшей форме, которая дороже книг, так как это живая передача. Это один из самых трудных способов передачи, гораздо труднее, чем написать книгу» [16, 17].

Приведем краткую характеристику каждого из перечисленных классов информационных ресурсов и их места в структуре информационных ресурсов.

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

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

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

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

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

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

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

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

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

Между информацией, зафиксированной в документе, и пользователем появляется система барьеров (технических, программных, технологических и других), которые существенно ограничивают и/или полностью исключают возможность доступа к информации.

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

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

$$Д=f(с[g], н[i], а[q], ф[j], у[h], п[w], м[z]),$$

где Д - документ; с[g] - содержание информации, отражаемой в документе; н[i] - носитель информации; а[q] - алфавит представления информации; ф[j] - метод (способ) фиксации информации (данных), зафиксированной в документе; у[h] - устройство (техническое средство), обеспечивающее как воспроизводство документа в форме, пригодной для восприятия человеком, так и регистрацию (фиксацию), сбор, передачу, хранение и обработку, ввода-вывода документов; п[w] - правила (способы, методы, алгоритмы, программы) преобразования документов (информации (данных)) при изменении носителя информации, устройств воспроизведения, фиксации, сбора, передачи, хранения, обработки, ввода-вывода документов; м[z] - метаинформация о документе (информация, описывающая документ).

В первом приближении документообразующие признаки могут быть заданы следующим перечнем.

1. Содержание информации, отражаемой в документе (с[g]).

1.1. Проблемная область информации, отраженной в документе.

1.1.1. Научно-техническая информация.

1.1.2. **Экономическая информация.**

1.1.3. Управленческая информация.

1.1.4. **Технологическая информация.**

1.1.5. Производственная информация.

1.1.6. **Юридическая информация.**

1.1.7. **Справочная информация.**

1.1.8. Социальная информация.

1.1.9. **Медицинская информация.**

1.1.10. Прочая (в том числе художественная, религиозная, музыка, искусство, литература и т. д.).

1.2. Описательная информация о документе (информация, описывающая документ).

1.2.1. Реферативно-библиографические данные (в соответствии с принятыми нормами описания конкретного вида документа).

1.2.2. Лингвистические средства, раскрывающие содержание документа (классификации, классификаторы, рубрикаторы, тезаурусы и дескрипторные словари, прочие словарно-терминологические средства).

1.2.3. Идентификационная информация, способствующая однозначной идентификации документа и его места в совокупности взаимосвязанных документов, а также связей документа с другими документами, фондами документов, владельцами и пр.

2. Носитель информации (н[i]).

2.1. Бумажный носитель:

2.1.1. Документы, подготовленные с помощью традиционных средств полиграфии.

2.1.2. Бумажный носитель для устройств типа принтера.

2.1.3. Перфолента

2.1.4. Перфокарта.

2.1.5. Носители для устройств отображения.

2.2. Магнитные и магнитооптические (CD ROM) носители:

2.2.1. Магнитная лента.

2.2.2. Магнитные диски и дискеты.

2.2.3. Жесткие диски (винчестеры).

2.2.4. CD ROM.

2.2.5. Оперативная память.

2.3. Микрофильмовые носители и кинофотоматериалы:

2.3.1. Микрофильмы.

2.3.2. Микрофиши.

2.3.3. Фотоносители.

2.3.4. Киноматериалы.

2.4. Устройства отображения:

2.4.1. Табло для алфавитно-цифровой информации.

2.4.2. Экраны.

2.4.3. Самописцы.

2.5. Сообщения по линиям связи.

3. Алфавит представления информации (а[q]).

3.1. Цифры.

3.2. Буквы.

3.3. Символы иероглифических систем письменности.

3.4. Знаки:

3.4.1. Математические и химические знаки.

3.4.2. Почтовые знаки.

3.4.3. Картографические знаки.

3.4.4. Железнодорожные и пароходные знаки, знаки правил уличного движения и пр.

3.4.5. Метеорологические знаки.

3.4.6. Астрономические и лунные знаки.

3.5. Прочие системы специальных знаков и условных обозначений (знаки радиоэлектронных схем, технологических процессов и пр.).

4. Метод (способ) фиксации информации (данных), зафиксированной в документе (ф[j]).

4.1. Тексты.

4.2. Формульная информация (в том числе различные методы представления химических формул и структур).

4.3. Табличная информация (в том числе бланковая, анкетная).

4.4. Графика (рисунки, чертежи, карты, изображения, видеоматериалы и пр.).

4.5. Представление пространственных данных.

4.6. Аудиоинформация.

4.7. Аудиовизуальная информация.

4.8. Цифровая и аналоговая информация, записываемая различной регистрирующей аппаратурой.

4.9. Перфорация (от азбуки для слепых до кодовых комбинаций на перфоносителях).

5. Устройство (техническое средство), обеспечивающее как воспроизводство документа в форме, пригодной для восприятия человеком, так и регистрацию (фиксацию), сбор, передачу, хранение и обработку, ввода-вывода документов (у[h]).

5.1. Средства ручной обработки.

5.2. Оргтехника.

5.3. Микрофильмовая техника (все средства кинофототехники).

5.4. Элекронно-вычислительная техника (в том числе ЭВМ, телевизионная техника).

5.5. Средства и каналы связи.

6. Правила (способы, методы, алгоритмы, программы) преобразования документов (информации (данных)) при изменении носителя информации, устройств воспроизведения, фиксации, сбора, передачи, хранения, обработки, ввода-вывода документов (п[w]).

6.1. Преобразования:

6.1.1. Информации (данных).

6.1.2. Носителей.

6.1.3. Технических средств.

6.1.4. Алгоритмов, программ, правил.

6.2. Операции обработки;

6.2.1. Копирование.

6.2.2. Контроль.

6.2.3. Поиск.

6.2.4. Восстановление.

6.2.5. Защита.

6.2.6. Ввод-вывод.

6.2.7. Преобразование:

6.2.7.1. Редактирование (включение, замена, извлечение, объединение, сегментирование, гашение, уничтожение, создание связи, изменение положения, упорядочение, слияние, группировка).

6.2.7.2. Кодирование-декодирование, транслитерация, транскрибирование.

6.2.8. Просмотр.

6.2.9. Обмен.

6.2.10. Хранение.

6.2.11. Прочие операции.

7. Метаинформация о документе (информация, описывающая документ) (м[z]).

7.1. Описание структуры документа.

7.2. Описание системы кодирования, включаемой в документ.

7.3. Описание операций, разрешенных над информацией, включаемой в документ.

7.4. Описание информации, включаемой в документ.

7.5. Описание информации, идентифицирующей документ.

7.6. Описание технических средств, необходимых для обработки документов и информации, включенной в документ.

7.7. Описание правил, алгоритмов, программ, обеспечивающих работу с документом.

Перечень составлен на основании анализа документов, циркулирующих в различных сферах человеческой деятельности.

Приведенный перечень с достаточной полнотой отражает состояние (уровень развития) современных информационных технологий, опирающихся на документальные информационные ресурсы.

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

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

Существуют различные классификационные перечни этих видов документов. Применительно к фондам научно-технических документов, как правило, выделяют 6 классификационных групп:

- библиографию литературных источников (планы издательств, проспекты информационных изданий, справочный аппарат государственных библиотек и т. д.);
- библиографию неопубликованных источников (бюллетени регистрации, отраслевые сборники рефератов НИР и ОКР, тезисы докладов на конференциях и семинарах и т. д.);
- фактографическую информация (прейскуранты оптовых цен, каталоги изделий внутриведомственной кооперации, документация по ценообразованию и т. д.);
- нормативную документацию (государственные и республиканские стандарты, отраслевые нормативы трудоемкости, стандарты предприятий на унифицированные узлы и компоненты и т. д.);
- патентную информацию (патентные зарубежные журналы, выдержки из патентных заявок, описания отечественных изобретений и т. д.);
- основную первичную информацию (книги, периодика, отечественные и зарубежные научно-технические сборники и труды НИИ, конструкторская и технологическая документация и т. д.).

Морфологический анализ позволяет на основании перечисленных документообразующих признаков выявить более широкую гамму видов документов, которые находятся в жесткой зависимости от информационной инфраструктуры (технической, программной и технологической).

Функционирование документальных информационных ресурсов (особенно представленных на машиночитаемых носителях) свидетельствует о том, что период их «жизненного цикла» существенно превосходит периоды «жизненного цикла» конкретных технических средств, программных продуктов, поколения ПЭВМ. Изменение технической и программной конфигурации автоматизированных информационных систем порождает проблему непрерывного конвертирования информационных массивов, которая по мере увеличения их объема становится все более дорогостоящей процедурой. С другой стороны, процессы конвертирования создают условия безвозвратной утраты тех или иных ресурсов в результате неадекватных процессов преобразования и/или утраты связей массивов с программной и технической средой, обеспечивающей их целостность и обработку, и/или утратой массивов и/или программных

средств, обеспечивающих идентификацию и однозначное декодирование данных и т. п.

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

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

Основные барьеры доступа к документальным информационным ресурсам в зависимости от различных документообразующих признаков в первом приближении могут быть заданы следующим перечнем.

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

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

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

- размерные характеристики носителя (длина, ширина, толщина, диаметр, количество поверхностей, с которых происходит чтение-запись информации);
- конструктивные, связанные с возможностью установки на конкретные устройства ввода-вывода информации;

- тип записи (плотность, число дорожек, ширина межблочных промежутков и т. п.);
- организация файлов;
- методы кодирования информации (используемый алфавит и методы кодирования символов алфавита, стандарты представления видеоинформации, графики пространственной информации, звука, аналоговой информации и т. д.);
- используемые методы защиты информации (криптография, электронные ключи, другие аппаратные методы защиты).

3. Алфавит представления информации:

- несовместимость символьного набора;
- несовместимость системы кодирования;
- несовместимые системы правил лексикографического упорядочения;
- несовместимость используемых символьных множеств с языками представления информации и типами представляемой информации;
- неразличимость «синонимии» символов (начертательной и кодовой);
- несовместимость правил транслитерирования.

4. Устройство (техническое средство):

- техническая несовместимость (общая, частичная);
- несогласованность конфигурации с требованиями к процессам обработки конкретных машиночитаемых носителей (объемы памяти, комплектация средств ввода-вывода, типы мониторов, видеокарты и пр.);
- невозможность использования требуемых программных продуктов.

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

- несовместимость и различие методов обработки;
- алгоритмическая и программная несовместимость;
- несовместимость по набору процедур обработки и набору обрабатываемых типов данных;
- несовместимость форматов представления данных;
- несовместимость систем кодирования, драйверов, электронных ключей;
- несовместимые методы представления и обработки данных в однотипных программных продуктах;

- различия интерфейса программных продуктов;
- несовместимость документов, подготовленных на одноименных программных продуктах различных версий и их модификаций;
- неэквивалентное преобразование информационных массивов при конвертировании.

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

- несовместимые методы и схемы описания (по содержанию, набору параметров);
- закрытость параметров и схем описания.

Исходя из изложенного, следует сделать следующие выводы.

1. Современный уровень развития информационных технологий с документальными ресурсами и тенденции их развития встраивают между носителем информации и пользователем информации, зафиксированной на носителе, сложнейшую техногенную среду (техническую, алгоритмическую, программную, технологическую), без участия которой пользователь не способен получить доступ к информации и воспринимать ее.
2. Несовместимость техногенной среды создает значительные трудности для восприятия информации, зафиксированной на машиночитаемых носителях, и во многих случаях ведет к их безвозвратной утрате.
3. Использование машиночитаемых ресурсов возможно в том и только в том случае, если они используются в согласованной (нормализованной, стандартизованной) техногенной среде. Требуемый уровень согласования для различных типов машиночитаемых документов различен. Соответственно каждая техногенная среда позволяет осуществлять работу с различными (свойственными только для нее) типами машиночитаемых ресурсов. Более того, различные модификации (версии) одной и той же техносферы могут порождать несовместимые машиночитаемые информационные ресурсы. К этой категории барьеров относятся ситуации, связанные с использованием несовместимых текстовых редакторов, драйверов, видеокарт, системные требования к конфигурации и пр.
4. Современный уровень развития техносферы визуализации и использования информации, зафиксированной на машиночитаемых носителях, порождает формирование информационных ресурсов с высокой степенью «нерегулируемой (скрытой) криптографичности», определяемой несогласованностью инструментальных средств, находящих-

ся в распоряжении конкретных пользователей. «Нерегулируемая (скрытая) криптографичность» информационных ресурсов, в свою очередь, порождает неадекватное воспроизводство информации, содержащейся на носителе, что исключает ее использование.

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

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

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

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

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

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

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

Ситуация осложняется тем, что:

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

# 5. Проблемы информационной войны

...С повышением способностей информационных систем в части их обучения акцент будет все более и более смещаться в сторону применения не огнестрельного оружия, а информационного.
*С. П. Расторгуев*

Поле боя в конфликтах XXI века - это виртуальное киберпространство, в котором разворачиваются действия информационных войн.
*С. Н. Гриняев*

## 5.1. Информационное оружие и его классификация

Одна из первых публикаций, посвященных классификации информационного оружия, появилась в журнале «Военная мысль» и принадлежит профессору А. И. Позднякову [19]. Данная классификация приведена на рис. 1.5 и включает две подгруппы информационного оружия.

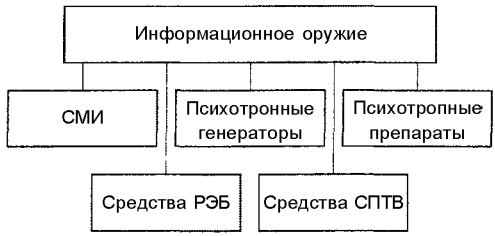



Рис. 1.5. Классификация информационного оружия

Первая подгруппа включает в себя:

- СМИ;
- психотронные генераторы;
- психотропные препараты.

Информационное оружие данной подгруппы предназначено для негативного воздействия на человека. В частности, это воздействие может осуществляться через различные СМИ. В соответствии с Федеральным законом «О средствах массовой информации» под этими средствами понимается периодическое печатное издание, радио-, теле-, видеопрограмма, кинохроникальная программа, иная форма периодического распространения массовой информации. Под массовой информацией понимаются предназначенные для неограниченного круга лиц печатные, аудио-, аудиовизуальные и иные сообщения и материалы. Хронология многих военных конфликтов последних лет включала, как правило, в начале их развития этап психологической обработки мировой общественности через СМИ. Так, например, при подготовке войны в районе Персидского залива США убедили мировую общественность в необходимости мер, принимаемых коалиционным руководством. Основная нагрузка в этой связи легла на печать, радио и телевидение. Они широко распространяли слухи о наличии у Ирака огромных запасов химического оружия, а также о планах его возможного применения, сообщали завышенные данные о численности иракских вооруженных сил, о поддержке режимом Хусейна ряда террористических организаций и т. п. [20].

Психотронные генераторы - это устройства, осуществляющие воздействие на человека путем передачи информации через внечувственное (неосознаваемое) восприятие.

Уже давно установлено [21], что разные органы человека имеют собственные резонансные частоты (рис. 1.6), используя которые можно воздействовать на психико-физиологическое состояние индивида или коллектива людей, вызывая у них страх, подавленность или другие чувства.

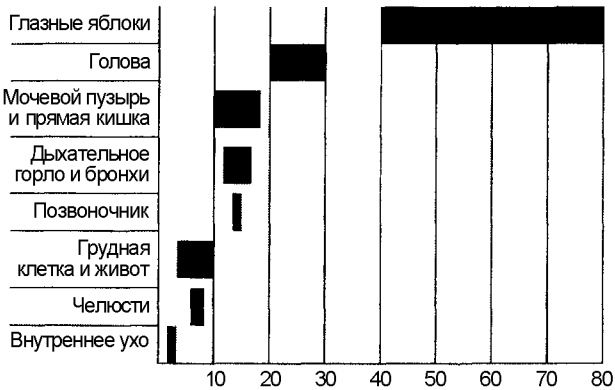



Рис. 1.6. Резонансные частоты (в Гц) отдельных частей тела человека

Эти и другие особенности человеческого организма используются при построении и подборе параметров (частотный диапазон, мощность излучения, длительность работы и др.) психотронных генераторов.

Психотропные препараты - это лекарственные (наркотические) средства, которые способны вызывать состояние зависимости, оказывать стимулирующее или депрессивное воздействие на центральную нервную систему, вызывая галлюцинации или нарушение моторной функции организма, под воздействием которых происходит нарушение мышления, меняется настроение, поведение [4].

Средства радиоэлектронной борьбы (РЭБ) - это средства для выявления и радиоэлектронного подавления систем управления войсками и оружием противника, его систем разведки и навигации, а также средства для обеспечения устойчивой работы своих систем.

Средства специального программно-технического воздействия (СПТВ) - программные, аппаратные или программно-аппаратные средства, с использованием которых может быть осуществлено несанкционированное копирование, искажение, уничтожение информации, ее передача за пределы контролируемой зоны или блокирование доступа к ней.

## 5.2. Информационная война

В настоящее время в число сфер ведения боевых действий, помимо земли, моря, воздуха и космоса, добавилась и информационная сфера. Как подчеркивают военные эксперты, основными объектами поражения в новых войнах будут информационная инфраструктура и психология противника (появился даже термин «human network»).

В качестве основных объектов воздействия в информационной войне выступают [29]:

- сети связи и информационно-вычислительные сети, используемые государственными организациями при выполнении своих управленческих функций;
- военная информационная инфраструктура, решающая задачи управления войсками;
- информационные и управляющие структуры банков, транспортных и промышленных предприятий;
- СМИ (в первую очередь электронные).

Сейчас имеется множество определений информационной войны. Остановимся на одном из них [22]. В августе 1995 г. Национальный институт обороны США опубликовал работу Мартина Либики «Что такое информационная война?». В ней автор определил 7 разновидностей информационной войны: командно-управленческая, разведывательная, психологическая, хакерская, экономическая, электронная и кибервойна.

Командно-управленческая (Command-and-control) война в качестве основного объекта воздействия рассматривает каналы связи между командованием и исполнителями. Перерезая «шею» (каналы связи), нападающий изолирует «голову» от «туловища». Утверждается, что это лучше, нежели просто убивать «голову». Считается, что Интернет родился как оборонный вариант этой войны («рассредоточенная шея»).

Разведывательная война имеет целью сбор важной в военном отношении информации и защиту собственной.

Электронная война объектом своего воздействия имеет средства электронных коммуникаций - радиосвязи, радаров, компьютерных сетей. Ее важная составляющая - криптография, позволяющая осуществлять шифрование и расшифровку электронной информации.

Психологическая война - осуществляется путем пропаганды, «промывания мозгов» и другими методами информационной обработки населения.

Либики выделяет 4 составляющие психологической войны: подрыв гражданского духа; деморализация вооруженных сил; дезориентация командования; война культур (Kulturkampf).

Хакерская война имеет целями тотальный паралич сетей, перебои связи, введение ошибок в пересылку данных, хищение информации, хищение услуг за счет несанкционированных подключений к сетям, их тай-

ный мониторинг, несанкционированный доступ к закрытым данным. Для достижения этих целей используются различные программные средства: вирусы, «троянские кони», «логические бомбы», сниферы («нюхалки», «следилки»).

Экономическая информационная война. Либики выделяет две ее формы - информационную блокаду (направленная против США) и информационный империализм (метод самих США).

Мир продолжает стремительно изменяться и ставит множество новых вопросов перед человечеством.

Революционные изменения видны во многих отраслях мировой экономики, в первую очередь это область информатизации общества. Волна «цифровой революции» создала абсолютно новый экономический сектор, которого раньше просто не было. Это провоцирует рост интенсивности конфликтов с целью захвата и удержания превосходства в данном секторе новой мировой экономики. Капиталом, который играет главенствующую роль в «цифровой революции», является интеллектуальный капитал, прежде всего в области информационных технологий.

И наконец, основной продукт этого сектора - информация - обладает уникальными свойствами, не присущими другим секторам экономики. Информация в отличие от всех других ресурсов пригодна для многократного использования и для многочисленных пользователей, при этом чем больше она применяется, тем более ценной становится. То же самое можно сказать о сетях, связывающих различные источники информации.

Таков один из подходов к определению сущности и содержания информационной войны, описанный в работе [22]. Читателю, безусловно, будет полезно ознакомиться и с другими трактовками этого понятия, приведенными в работах [23, 24, 25, 26].

Множество определений информационной войны связано, по-видимому, со сложностью и многогранностью такого явления, как информационная война, трудностью построения аналогий с традиционными войнами. Начнем с определения известного теоретика и историка К. Клаузевица [27], в соответствии с которым война есть не что иное, как продолжение государственной политики иными средствами. В. И. Ленин уточнил это определение [28], добавив перед словом «средствами» прилагательное «насильственными». Если попытаться трансформировать приведенные определения в понятие «информационная война», то вряд ли что конструктивное получится. Это связано с рядом особенностей информационной войны.

Для войны в ее обычном понимании субъекты (противостоящие стороны) четко определены, существуют понятия начала и окончания войны, линии фронта. Противостоящие стороны, как правило, описываются одинаковыми моделями. Исход войны во многом определяется соотношением военных потенциалов сторон.

Для информационной войны обычно четко определена обороняющаяся сторона, понятия начала и окончания можно применить лишь к отдельным операциям информационной войны, линия фронта не определена. Обороняющаяся и наступающая стороны описываются различными моделями. Успех проводимых информационных операций не имеет прямой связи с соотношением военных потенциалов сторон.

# 6. Проблемы информационной безопасности в сфере государственного и муниципального управления

## 6.1. Информационные процессы в сфере государственного и муниципального управления

Обеспечение информационной безопасности в сфере государственного и муниципального управления (ГМУ) основывается на подробном анализе структуры и содержания ГМУ, а также информационных процессов и используемых при управлении технологий.

Государственное (муниципальное) управление - это процесс выполнения комплекса мероприятий, ориентированных на достижение государственных (муниципальных) целей, которые описываются на языке, отображающем желаемые состояния государства, отраслей, регионов и муниципальных образований. Мероприятия при этом должны соответствовать стратегическим целям и тактическим задачам, быть упорядоченными по времени выполнения и составу участников, а также быть обеспеченными необходимыми ресурсами [18].

Учитывая большое количество и разнообразие управляющих систем в сфере ГМУ, возьмем за основу рассмотрения региональный уровень органов ГМУ (субъекта РФ и его муниципальных образований) и воспользуемся результатами работы [18].

Систему органов власти и управления составляют:

- законодательный орган государственной (муниципальной) власти субъекта РФ и представительные органы его муниципальных образований;

- исполнительный орган государственной власти субъекта РФ и органы муниципального управления;
- иные органы государственной власти субъекта РФ, образуемые в соответствии с конституцией субъекта РФ.

Законодательный и исполнительный органы государственной власти субъекта РФ, а также органы муниципального управления взаимодействуют в целях эффективного управления процессами экономического и социального развития субъекта Федерации и в интересах его населения.

Территориальные органы федеральных органов исполнительной власти осуществляют свою деятельность под руководством соответствующих центральных органов, а по вопросам, входящим в компетенцию субъектов РФ, - во взаимодействии с региональными органами исполнительной власти и управления. Основные задачи и функции территориальных органов определяются исходя из задач и функций соответствующих министерств и ведомств РФ с учетом конкретных особенностей регионов, в которых они осуществляют свою деятельность. Территориальные органы принимают участие в выработке мер и способов государственного регулирования социально-экономического развития субъектов Федерации, информируют министерства и ведомства, органы исполнительной власти субъектов Федерации о проводимой ими работе в регионах.

Территориальные органы имеют право запрашивать и получать:

- от органов исполнительной власти субъектов РФ и местного самоуправления - необходимую для осуществления своей деятельности информацию;
- от предприятий, организаций и учреждений независимо от форм собственности - сведения, необходимые для выполнения возложенных на них задач;
- от органов статистики - информационно-аналитические материалы, экономико-статистические данные в установленном порядке.

Информационная сфера субъектов РФ и муниципальных образований представляет собой совокупность субъектов, осуществляющих деятельность в этой информационной сфере, региональных (муниципальных) информационных систем и сетей связи, включая телекоммуникационные системы, информационные ресурсы и общественные отношения в информационной сфере, правовое регулирование которых Конституцией РФ отнесено к предметам совместного ведения РФ, ее субъектов и муниципальных образований.

По своей природе и целям подавляющее число процессов в сфере ГМУ являются информационными и составляют замкнутый цикл. К этим процессам относятся:

- получение управляющими субъектами информации;
- переработка и анализ полученной информации;
- принятие управленческих решений;
- доведение их до исполнителей;
- контроль исполнения;
- получение информации о результатах управления.

Применительно к сфере ГМУ информационные процессы можно определить как процессы получения, использования или преобразования информации в ходе выполнения органом ГМУ или его должностным лицом нормативно закрепленной за ним функции или задачи.

Типовыми информационными процессами в сфере ГМУ являются:

- ведение документооборота;
- накопление информации;
- анализ информации;
- прогноз и планирование;
- принятие управленческих решений;
- информирование населения.

Перечисленные процессы в работе [18] рассматриваются только в контексте их реализации с помощью компьютерных систем.

Компьютерная система (КС) - это организационно-техническая система, представляющая собой совокупность следующих взаимосвязанных элементов:

- технических средств обработки и передачи данных (средств вычислительной техники и связи);
- методов и алгоритмов обработки в виде соответствующего программного обеспечения;
- информации (массивов, наборов, баз данных) на различных носителях;
- персонала и пользователей системы, объединенных по организационно-структурному, тематическому, технологическому или другим признакам для выполнения автоматизированной обработки информации с целью удовлетворения информационных потребностей субъектов информационных отношений.

По терминологии в области защиты информации от несанкционированного доступа КС относится к автоматизированным системам.

Основными носителями и средствами передачи информации в КС являются:

- средства хранения информации (магнитные диски, оптические диски, ОЗУ, ПЗУ и т. д.);
- средства отображения информации (терминалы, принтеры, бумажные носители, графопостроители и т. д.);
- средства передачи информации (аппаратура передачи и приема информации, линии связи, модемы и т. д.).

Рассмотрим более подробно типовые информационные процессы в органах ГМУ.

1. Ведение документооборота. Этот процесс осуществляется в целях:

- обеспечения внутреннего цикла движения организационно-распорядительной и другой требуемой в повседневной работе информации;
- взаимодействия с вышестоящими и подчиненными органами;
- реализации установленных нормативными документами функций в отношении юридических и физических лиц.

Ведение документооборота включает следующие операции:

- прием, подготовку, оформление, учет, согласование, рассылку документов;
- организацию и контроль исполнения принимаемых решений.

2. Накопление информации. Этот процесс осуществляется в целях:

- облегчения поиска требуемой информации;
- сохранения циркулирующей информации.

Накопление информации включает следующие операции:

- ввод информации в базы данных;
- создание и копирование файлов документов.

3. Анализ информации и на его основе прогноз и планирование. Этот процесс осуществляется в целях:

- подготовки отчетности для вышестоящих органов;
- обеспечения принятия оперативных решений;
- прогнозирования будущих состояний объекта управления;
- планирования дальнейших управленческих действий.

Данный процесс включает следующие операции:

- выборку требуемой информации по признакам из баз данных или электронных архивов;
- систематизацию и агрегирование отобранных данных;
- визуализацию числовой информации;
- выявление закономерностей, тенденций и т. д.;
- формулирование выводов, прогнозов, планов;
- изготовление аналитических и плановых документов.

Уровни агрегирования информационно-аналитических материалов:

- на муниципальном (городском) уровне информация, как правило, агрегируется в масштабе предприятий и районов;
- на региональном уровне - информация агрегируется по отраслям, городам и районам.

4. Принятие управленческих решений. Этот процесс осуществляется в целях:

- выполнения функций и задач управления;
- регулирования состояния (деятельности) объекта управления.

Принятие управленческих решений включает следующие операции:

- сопоставление и обобщение полученной информации;
- выбор наиболее приемлемого для конкретной ситуации варианта возможных действий;
- доведение управленческой информации до исполнителей.

5. Информирование населения. Этот процесс осуществляется в целях:

- отчетности о принятых решениях и результатах работы органов ГМУ;
- повышения уровня информированности населения.

Он включает следующие операции:

- публикацию материалов в СМИ;
- ведение сайта в Интернете;
- подготовку ответов на запросы и обращения юридических и физических лиц.

Участвующие в информационных процессах субъекты и объекты вступают между собой в различные информационные отношения.

Информационные отношения - это вид общественных отношений, связанных с информационными процессами - процессами сбора, обра-

ботки, накопления, хранения, поиска и распространения информации с использованием ЭВМ, их систем и сетей.

В качестве субъектов информационных отношений в сфере ГМУ выступают:

- органы ГМУ всех уровней и направлений;
- госслужащие (чиновники, персонал КС);
- юридические лица (коммерческие и общественные организации);
- граждане.

Различные субъекты в процессе информационных отношений могут выступать в качестве:

- источников (поставщиков) информации;
- пользователей (потребителей) информации;
- собственников (владельцев, распорядителей) информации;
- участников процессов обработки и передачи информации.

## 6.2. Виды информации и информационных ресурсов в сфере ГМУ

С тематической и функциональной точки зрения информация бывает организационно-распорядительной, нормативно-правовой, планово-финансовой, социально-экономической, индикативной и т. д. По уровню агрегирования - первичной, структурированной, статистической, аналитической и др. [18].

По правовому режиму доступа информация может быть открытой и ограниченного доступа.

Документированная информация ограниченного доступа подразделяется на информацию, отнесенную к государственной тайне, и конфиденциальную.

Конфиденциальная информация - это документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ.

Персональные данные - это сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность. Персональные данные о гражданах, включаемые в состав федеральных информационных ресурсов, информационных ресурсов совместного ведения, информационных ресурсов субъектов РФ, информационных ресурсов местного самоуправления, а также получаемые и собираемые негосударственными организациями, отнесены к категории конфиденциальной информации.

В действующей нормативно-правовой базе РФ существует более 30 видов тайн (видов конфиденциальной информации). Между ними подчас имеются противоречия, нестыковки, пересечения, что объективно требует совершенствования законодательства в данной сфере.

Фиксируемая (накапливаемая) каким-либо способом информация образует информационные ресурсы.

Информационные ресурсы - это отдельные документы и отдельные массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных и других ИС).

Информационные ресурсы делятся на государственные и негосударственные. Государственные информационные ресурсы РФ формируются в соответствии со сферами ведения (федеральные информационные ресурсы; информационные ресурсы, находящиеся в совместном ведении РФ и субъектов Федерации; информационные ресурсы субъектов РФ). Государственные информационные ресурсы являются открытыми и общедоступными. Исключение составляют ресурсы, включающие документированную информацию, отнесенную законом к категории ограниченного доступа [18].

### 6.3. Состояние и перспективы информатизации сферы ГМУ

Согласно Закону «Об информации, информатизации и защите информации», информация - это 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.

К сожалению, информатизация сферы ГМУ в России происходит в целом весьма хаотично и со значительным отставанием от требований времени. Так, например, по результатам исследований, проведенных в Санкт-Петербурге, уровень эффективности использования информации в системе управления городом характеризуется следующими данными [18]:

- только 10-15 % информации используется для обоснования и принятия решений;
- соотношение между входной и выходной информацией в различных системах управления составляет от 4:1 до 40:1;
- объем дублирующей информации в системах управления достигает 30 % от ее общего объема.

Такому положению дел способствовало отсутствие системной государственной политики в информационной сфере. Тем не менее определенные положительные сдвиги в этом направлении начинают происходить. Так, в начале 2002 г. правительством РФ утверждена федеральная целевая программа «Электронная Россия» на период 2002-2010 гг. Основной целью программы является повышение эффективности функционирования экономики, государственного управления и местного самоуправления за счет внедрения и массового распространения информационных технологий, создание технологических предпосылок для развития гражданского общества за счет обеспечения прав на свободный доступ к информации, расширение подготовки специалистов по информационным технологиям и квалифицированных пользователей.

Для достижения целей программы в сфере ГМУ планируется [18]:

На первом этапе:

- проведение полномасштабного аудита всех информационных активов и ресурсов федеральных органов государственной власти, анализ зарубежного опыта реализации подобных программ;
- будет сформирована система межведомственной координации деятельности органов государственной власти всех уровней в целях развития и массового распространения информационных технологий, разработаны критерии эффективности бюджетных расходов этой области и создан механизм, обеспечивающий их достижение;
- будут созданы предпосылки для законодательного обеспечения прав граждан на доступ к открытой информации государственных органов власти и местного самоуправления на основе использования информационных технологий;
- начнут реализовываться первые пилотные проекты по переходу к электронному документообороту в государственных и муниципальных органах власти, по развитию инфраструктуры доступа к телекоммуникационным сетям для органов государственной власти и местного самоуправления.

На втором этапе:

- будут реализованы организационные мероприятия по расширению и развитию проектов по интерактивному взаимодействию органов государственной власти и местного самоуправления с гражданами и хозяйствующими субъектами;
- будут разработаны и приняты изменения и дополнения к действующим нормативным актам, уравнивающие в правах электронную

и бумажную форму представления информации в государственные органы и органы местного самоуправления (в частности, в налоговые и статистические органы, органы регистрации имущественных и других прав и т. п.);

- будет в основном сформирована единая телекоммуникационная инфраструктура для органов государственной власти и местного самоуправления;
- будут разработаны меры, регламентирующие права граждан и обязанности государственных и муниципальных учреждений по принятию к рассмотрению заявок, жалоб и других запросов граждан в электронной форме;
- предполагается расширение сферы обязательного для государственных органов применения информационных технологий в сфере взаимодействия государства и общества, позволяющее гражданам реализовать свои конституционные права на получение информации по нормотворческой деятельности, бюджетному процессу, проведению закупок для государственных нужд, процесса управления государственной собственностью и т. д.;
- будут развиваться системы внутриведомственного и межведомственного электронного документооборота, включая развитие локальных информационных сетей и интранет, в том числе с использованием открытых международных стандартов;
- будет осуществлена разработка и начата реализация мер по оцифровке и ускоренному переводу в открытый доступ всей не запрещенной к открытому распространению, имеющейся у государственных органов информации;
- будут разработаны и введены в действие необходимые поправки в процессуальное законодательство, позволяющие осуществлять ряд процессуальных действий с использованием информационных технологий;
- будет сформирована основная конфигурация «электронного правительства».

На третьем этапе по результатам предыдущих этапов:

- будет обеспечено комплексное внедрение стандартизированных систем документооборота;
- будет реализовываться концепция представительства органов власти в сети Интернет.

Таким образом, при условии выполнения программы компьютерные технологии к концу первого десятилетия XXI в. станут основой повседневной деятельности органов ГМУ, а компьютерные системы - ее главными инструментами [18].

# 7. Система подготовки кадров в области информационной безопасности в Российской Федерации

## 7.1. Структура системы подготовки кадров в области информационной безопасности

В настоящее время система подготовки кадров опирается на Учебно-методическое объединение (УМО) по образованию в области информационной безопасности, созданное в 1996 г. на базе известнейшего учебного заведения в этой области - Института криптографии, связи и информатики Академии ФСБ России. Важными структурами в этой системе являются также Учебно-методический совет Российского государственного гуманитарного университета (РГГУ) и сеть региональных учебно-научных центров по проблемам информационной безопасности (ИБ) в системе высшей школы, созданных Минобразованием России в 1997 г. (головной вуз - МИФИ).

Характеристика системы подготовки кадров представлена в работе [30].

Система включает в себя следующие составляющие:

- государственные образовательные стандарты высшего профессионального образования и разработанные на их базе основные образовательные программы в области ИБ по семи специальностям: «Криптография» - 075100 (090101*), «Компьютерная безопасность» - 075200 (090102), «Организация и технология защиты информации» - 075300 (090103), «Комплексная защита объектов информатизации» - 075400 (090104), «Комплексное обеспечение информационной безопасности автоматизированных систем» - 075500 (090105), «Информационная безопасность телекоммуникационных систем» - 075600 (090106), «Противодействие техническим разведкам» - 075700 (090107). Эти специальности в перечне направлений и специально-

* В скобках указаны коды специальностей по ОКСО (Общероссийский классификатор специальностей по образованию).

стей выделены в отдельную группу «Информационная безопасность»;

- государственный образовательный стандарт среднего профессионального образования по специальности «Информационная безопасность» - 2206;
- Учебно-методическое объединение вузов России по образованию в области ИБ на базе ИКСИ Академии ФСБ (УМО ИБ) и Учебно-методический совет УМО в области историко-архивоведения (УМС РГГУ);
- Сибирское региональное отделение УМО по образованию в области информационной безопасности (СиБРУМО) (головной вуз ТУРУС);
- более 100 вузов и 10 средних специальных учебных заведений России различной ведомственной принадлежности, которые ведут образовательную деятельность по подготовке специалистов в области ИБ;
- 12 министерств и ведомств и их органов управления профессиональным образованием, а также научные организации и учреждения, ведущие научные исследования в данной области, в том числе два головных центра - МГУ им. М. В. Ломоносова и Академия криптографии РФ;
- специальности и специализации (соответствующие образовательные программы, включающие вопросы ИБ), реализуемые в рамках других УМО, смежные с входящими в группу по ИБ;
- 25 региональных учебно-научных центров (РУНЦ) по проблемам ИБ в системе высшей школы с головным центром на базе МИФИ;
- образовательные программы дополнительного образования и соответствующие различные ведомственные курсы переподготовки и повышения квалификации (ИКСИ Академии ФСБ России, РГГУ, Московский институт новых информационных технологий ФСБ России, Военная академия Генерального штаба Вооруженных сил РФ, МОСУЦ Минатома России и др.); ой, не смешите мои тапочки ☺
- образовательные программы послевузовского профессионального образования в данной области (подготовка кадров высшей квалификации), включая единственную открытую специальность 05.13.19 «Методы и системы защиты информации, информационная безопасность» и закрытые специальности.

Структура системы подготовки кадров в области ИБ представлена на рис. 1.7.

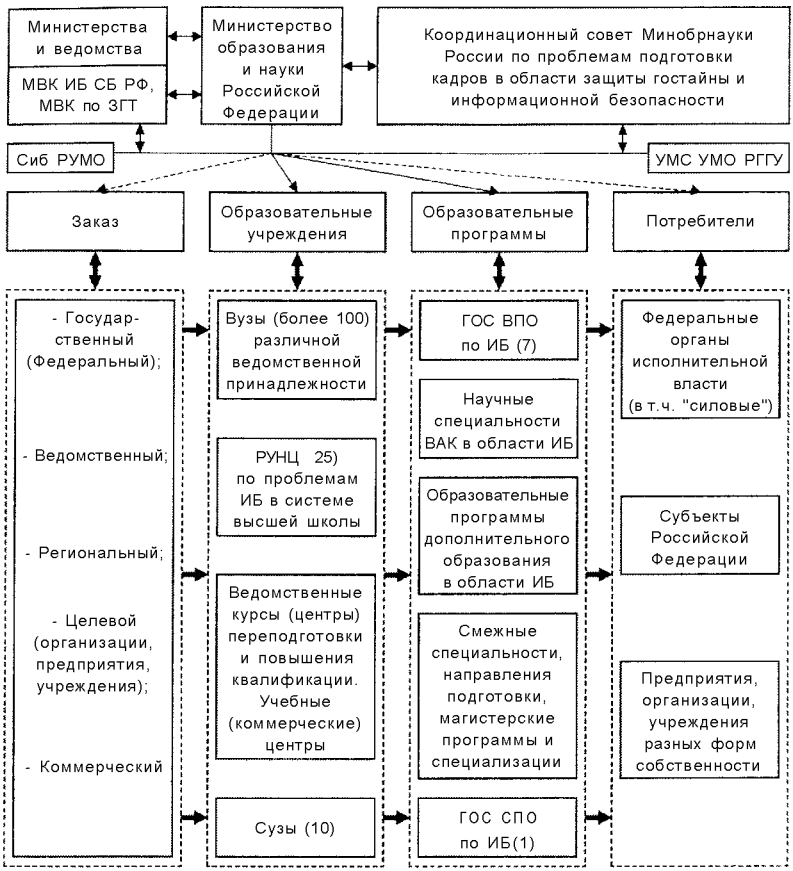



Рис. 1.7. Структура системы подготовки кадров в области информационной безопасности

Объекты системы:

- средние специальные и высшие учебные заведения, которые имеют лицензии на образовательную деятельность по соответствующей специальности, включенной в Общероссийский классификатор специальностей по образованию;
- региональные учебно-научные центры (25), созданные во всех семи федеральных округах на базе ведущих высших учебных заведений и решающие проблемы кадрового обеспечения ИБ конкретного региона;

- учебные центры дополнительного образования (как правило, негосударственные), созданные организациями, активно работающими на рынке средств и услуг, связанных с защитой информации. На свою учебную деятельность данные центры получают лицензии соответствующих региональных управлений образования. Такие учебные центры созданы практически во всех регионах России;
- потребители (заказчики) специалистов.

Субъекты системы:

- студенты и слушатели-специалисты, обучающиеся в высших учебных заведениях, РУНЦ и учебных центрах дополнительного образования;
- преподаватели различных учебных заведений и центров;
- административный персонал, организующий и сопровождающий учебный процесс.

## 7.2. Состав учебно-методического обеспечения системы и ее подсистема управления

В состав учебно-методического обеспечения системы входят:

- государственные образовательные стандарты высшего профессионального образования по семи специальностям, входящим в группу специальностей «Информационная безопасность»;
- государственный образовательный стандарт среднего профессионального образования по специальности «Информационная безопасность» - 2206;
- учебные планы подготовки специалистов по конкретным специальностям;
- учебные программы дисциплин и отдельных учебных курсов, программы итоговой государственной аттестации, относящихся к определенной специальности;
- учебные программы курсов повышения квалификации или курсов переподготовки специалистов с целью получения дополнительной квалификации;
- учебники, учебные и учебно-методические пособия и лабораторные практикумы;
- информационные материалы, поддерживающие учебный процесс.

Подсистема управления:

- Министерство образования и науки РФ и органы управления, осуществляющие лицензирование образовательной деятельности высших учебных заведений;
- органы исполнительной власти на региональном уровне, осуществляющие лицензирование образовательной деятельности, связанной с дополнительным образованием;
- учебно-методические объединения - государственно-общественные организации, объединяющие представителей учебных заведений, в которых ведется подготовка специалистов в области информационной безопасности, а также организаций и ведомств, в интересах которых эта подготовка осуществляется. Данные объединения курируют образовательную деятельность различных учебных заведений и центров с целью обеспечения необходимого уровня подготовки, соответствующего требованиям, сформулированным в государственных образовательных стандартах (рис. 1.8);

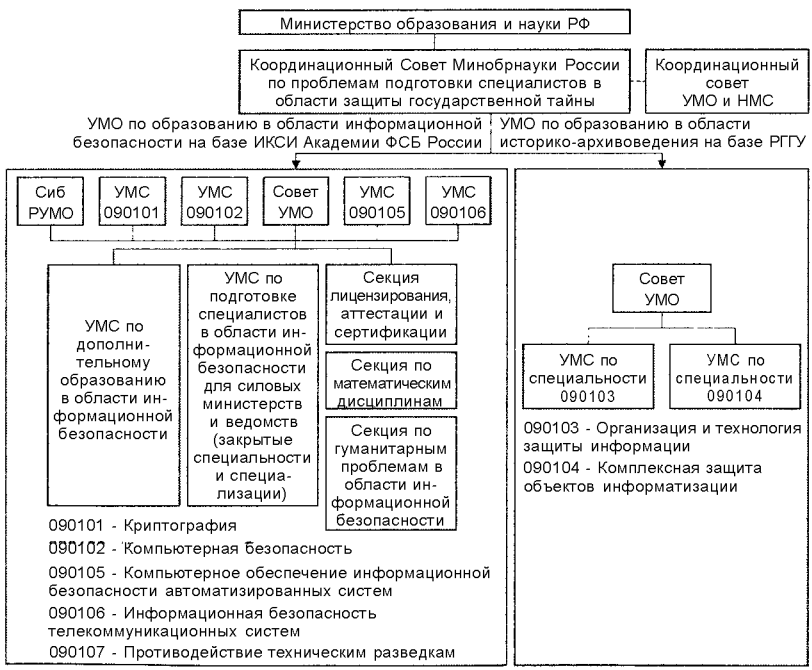



Рис. 1.8. Структурная схема учебно-методических объединений вузов в области информационной безопасности

- Координационный совет Министерства образования и науки РФ по проблемам подготовки кадров в области защиты государственной тайны и информационной безопасности, в который вошли представители заинтересованных министерств и ведомств.

### 7.3. Основные направления учебной деятельности

К основным направлениям учебной деятельности относятся:

- подготовка специалистов с высшим образованием (7 специальностей; квалификации - математик, специалист по защите информации; срок обучения - 5 лет или 5,5 года);
- подготовка специалистов со средним профессиональным образованием (одна специальность; квалификация - техник; срок обучения - 2 года 10 мес);
- дополнительное образование: повышение квалификации (72 уч. ч. и более); дополнительная квалификация (до 500 уч. ч.); переподготовка (более 500 уч. ч.);
- подготовка кадров высшей квалификации - кандидатов и докторов наук по специальности «Методы и системы защиты информации, информационная безопасность» по отраслям физико-математических, технических и юридических наук.

Следует отметить, что в ФСБ России, Минобороны России, ФСО России, МВД России, ФСТЭК России, Министерстве транспорта России, других министерствах и ведомствах сформировались ведомственные подсистемы подготовки кадров, по своей структуре аналогичные общей системе подготовки специалистов в Министерстве образования и науки РФ. В рамках данных министерств и ведомств имеются образовательные учреждения, реализующие образовательные программы среднего, высшего, дополнительного и послевузовского профессионального образования в области информационной безопасности. Данные подсистемы направлены на целевую подготовку кадров в интересах ведомств и по своей организации, содержанию и развитию имеют определенную специфику.

Взаимодействие данных подсистем осуществляется в рамках Координационного совета Министерство образования и науки РФ по проблемам подготовки кадров в области защиты государственной тайны и информационной безопасности, созданного приказом министра образования РФ от 25.02.2003 г. № 670.

К настоящему времени более 100 вузов осуществляют подготовку специалистов по специальностям данной группы. Распределение вузов по

специальностям приведено в табл. 1.1. Подготовкой специалистов охвачены все регионы России.

*Таблица 1.1. Перечень специальностей ВПО в области ИБ*

| *Специальность* | | *Число вузов* |
|---|---|---|
| *Индекс* | *Наименование* | |
| 075100 | Криптография | 1 |
| 075200 | Компьютерная безопасность | 27 |
| 075300 | Организация и технология защиты информации | 44 |
| 075400 | Комплексная защита объектов информатизации | 24 |
| 075500 | Комплексное обеспечение информационной безопасности автоматизированных систем | 30 |
| 075600 | Информационная безопасность телекоммуникационных систем | 11 |
| 075700 | Противодействие техническим разведкам | 1 |
| | *Всего* | *138* |

В качестве проблем в области обеспечения информационной безопасности в сфере образования можно выделить 4 направления:

1. Подготовка высококвалифицированных специалистов всех уровней для структур обеспечения информационной безопасности.
2. Формирование базового уровня понимания правовых и организационных вопросов взаимодействия личности, общества и государства в части информационной безопасности.
3. Формирование достаточно высокого уровня подготовки у выпускников ряда специальностей гуманитарного, управленческого и экономического направлений в области информационной безопасности.
4. Повышение квалификации и переподготовка в направлении информационной безопасности специалистов самого различного уровня и профиля.

*По специальностям группы 075000 «Информационная безопасность» в дополнение к государственным образовательным стандартам высшего профессионального образования разработаны примерные учебные планы и примерные программы дисциплин, требования к учебно-методическому и материально-техническому обеспечению. Сформирована электронная база данных обеспеченности ГОС ВПО по специальностям в области ИБ учебно-методическими изданиями. Разработаны и изданы учебники и учебные пособия по основным дисциплинам.*

## Литература


1. Концепция национальной безопасности Российской Федерации (утверждена Указом Президента Российской Федерации от 17 декабря 1997 г. № 1300 в редакции Указа Президента Российской Федерации от 10 января 2000 г. № 24) // Безопасность. 2000. № 1—12
2. Конституция Российской Федерации. М., 1993.
3. Общая теория национальной безопасности: Учеб./ Под общ. ред. А. А. Прохожева. М.: Изд-во РАГС, 2002. 320 с.
4. Котенев А. А., Лекарев С. В/Современный энциклопедический словарь. Секьюрити. М.: Ягуар, 2001. 504 с.
5. Новейший философский словарь / Сост. А. А. Грицанов. Минск, 1999. С. 274; Всемирная энциклопедия философии. М., 2001. С. 428.
6. Лопатин В. Н. Информационная безопасность России: Человек. Общество. Государство / С-Петерб. ун-т МВД России. СПб.: Фонд «Университет». 2000. С. 23.
7. Новейший философский словарь / Сост. А. А. Грицанов. Минск, 1999. С. 274; Всемирная энциклопедия философии. М., 2001. С. 428.
8. Стрельцов А. А. Содержание понятия «информация»: Тез. докл. на заседании Межведомственного междисциплинарного семинара по науч. проблемам информационной безопасности 13 декабря 2001 г.
9. Кравченко В. Б. Информация - объект или объекты исследования?: Тез. докл. на заседании Межведомственного междисциплинарного семинара по науч. проблемам информационной безопасности 13 декабря 2001 г.
10. Хартли Р. Передача информации // Теория информации и ее приложения: Сб. пер. М.: Гос. изд.-во физ.-мат. лит., 1959.
11. Черри К. Человек и информация. М.: Связь, 1972.
12. Винер Н. Кибернетика. М.: Сов. радио, 1958.
13. Доктрина информационной безопасности Российской Федерации. М., 2000.
14. Веревченко А. П. Информационные ресурсы: определение, основные понятия, параметры, особенности открытого потока информации, помехи возникающие в каналах поступления информации // http://www.mai.ru/~gr08x07/vap/verin010.htm.

15. Елепов Б.С, Чистяков В.М. Управление процессами использования информационных ресурсов. Новосибирск: Наука. Сиб. отд-ние, 1989. 238 с. С. 3,7.
16. Стенограмма заседания коллегии ЦАГИ 28 сентября 1926 г.
17. Андрей Николаевич Туполев. Грани дерзновенного творчества. М.: Наука, 1988. С. 59-60.
18. Мухин Н. Н. Чипига А. Ф. Основы информационной безопасности: Учеб. пособие (курс лекций). Ставрополь: СевкавГТУ, 2003. 69 с.
19. Военная мысль. 1993. № 10.
20. Гуржеянц Т. В., Дербин Е. А., Крылов Г. О., Кубанков А. Н. Информационные операции современности: учеб. пособие. М.: ВАГШ, 2004. 286 с.
21. Шарп М. Р. Человек в космосе / Пер. с англ. М. И. Рохлина и Л.А. Сливко; Под. ред и с предисл. д-ра мед. наук проф. С. М. Городинского. М.: Мир, 1970. 200 с. с илл. (В мире науки и техники).
22. http://gazeta.lenta.ru/dossier/06-08-1999_infowar.htm.
23. Расторгуев С. П. Введение в формальную теорию информационной войны. М.: Вузовская кн., 2002. 120 с.
24. Гриняев С. Н. Интеллектуальное противодействие информационному оружию. Сер. «Информатизация России на пороге XXI века». М.:СИНТЕГ, 1999.232 с.
25. Панарин И. Н., Панарина Л. Г. Информационная война и мир. М.: ОЛМА-ПРЕСС, 2003. 384 с.
26. Словарь терминов и определений в области информационной безопасности / Под общ. ред. генерал-майора Костюхина. М.: 2004. 113 с.
27. Война и мир в терминах и определениях / Под. ред. Д. О. Рогозина. М.: 2004. 624 с.
28. Ленин В. И. Поли. собр. соч. 5 изд. т. 26. С. 224.
29. Гриняев С. Н. Война в четвертой сфере. Превосходство в киберпространстве будет определять победу в конфликтах XXI века // НВО 2000 г. № 42.
30. Безопасность России. Правовые, социально-экономические и научно-технические аспекты. Информационная безопасность. М., 2005.
31. Труд. 2000. № 19. С..5.

# Часть 2

# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

## 1. Современная постановка задачи защиты информации

**Комплексность** - решение в рамках единой концепции двух или более разноплановых задач (целевая комплексность), или использование для решения одной и той же задачи разноплановых инструментальных средств (инструментальная комплексность), или то и другое (всеобщая комплексность).

*Целевая комплексность* означает, что система информационной безопасности должна строиться следующим образом:

- защита информации, информационных ресурсов и систем личности, общества и государства от внешних и внутренних угроз;
- защита личности, общества и государства от негативного информационного воздействия.

*Инструментальная комплексность* подразумевает интеграцию всех видов и направлений ИБ для достижения поставленных целей. В рамках прежнего представления о защите информации практически независимо развивались 4 вида защиты: организационная (режим секретности), техническая (противодействие техническим средствам разведки), криптографическая и обеспечение компьютерной безопасности. При этом имело место дублирование решаемых задач.

*Структурная комплексность* предполагает обеспечение требуемого уровня защиты во всех элементах системы обработки информации.

*Функциональная комплексность* означает, что методы защиты должны быть направлены на все выполняемые функции системы обработки информации.

*Временна́я комплексность* предполагает непрерывность осуществления мероприятий по защите информации как в процессе непосредственной ее обработки, так и на всех этапах жизненного цикла объекта обработки информации.

Можно сформулировать основные требования к системе защиты информации.

1. Система защиты информации должна быть представлена как нечто целое. Целостность системы будет выражаться в наличии единой цели ее функционирования, информационных связей между элементами системы, иерархичности построения подсистемы управления системой защиты информации.
2. Система защиты информации должна обеспечивать безопасность информации, средств информации, защиту интересов участников информационных отношений и невозможность несанкционированного доступа злоумышленника к защищаемой информации.
3. Система защиты информации в целом, применяемые методы и средства защиты должны быть по возможности прозрачными для законного пользователя, не создавать ему больших дополнительных неудобств, связанных с процедурами доступа к информации.

Система защиты информации должна обеспечивать оценку угроз внешних дестабилизирующих факторов и защиту от них.

Путь в несколько тысяч ли
начинается с первого шага.
*Лао-цзы*

# 2. Организационно-правовое обеспечение информационной безопасности

## 2.1. Информация как объект юридической защиты. Основные принципы засекречивания информации

*Организационно-правовое обеспечение* ИБ представляет собою совокупность решений, законов, нормативов, регламентирующих как общую организацию работ по обеспечению ИБ, так и создание и функционирование систем защиты информации на конкретных объектах. Основные функции организационно-правовой базы следующие.

1. Разработка основных принципов отнесения сведений, имеющих конфиденциальный характер, к защищаемой информации.
2. Определение системы органов и должностных лиц,, ответственных за обеспечение ИБ в стране и порядка регулирования деятельности предприятия и организации в этой области.
3. Создание полного комплекса нормативно-правовых руководящих и методических материалов (документов), регламентирующих во-

просы обеспечения ИБ как в стране в целом, так и на конкретном объекте.

4. Определение мер ответственности за нарушения правил защиты.
5. Определение порядка разрешения спорных и конфликтных ситуаций по вопросам защиты информации.

Под юридическими аспектами организационно-правового обеспечения защиты информации понимается совокупность законов и других нормативно-правовых актов, с помощью которых достигались бы следующие цели:

- все правила защиты информации являются обязательными для соблюдения всеми лицами, имеющими отношение к конфиденциальной информации;
- узакониваются все меры ответственности за нарушение правил защиты информации;
- узакониваются (приобретают юридическую силу) технико-математические решения вопросов организационно-правового обеспечения защиты информации;
- узакониваются процессуальные процедуры разрешения ситуаций, складывающихся в процессе функционирования системы защиты.

На рис. 2.1-2.3 представлены варианты концептуальных моделей безопасности продукции, личности и информации. Даже беглый анализ этих моделей дает представление о многообразии действий и мероприятий по обеспечению ИБ.

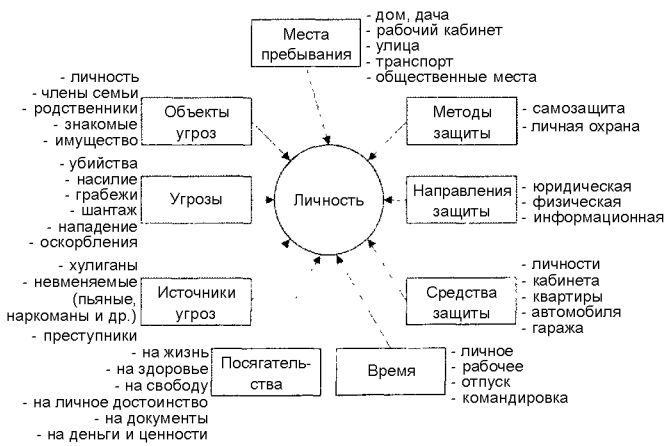



Рис. 2.1. Концептуальная модель безопасности личности

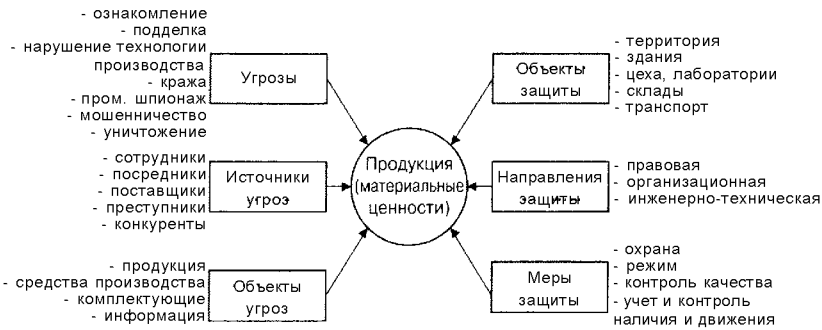



Рис. 2.2. Концептуальная модель безопасности продукции


Рис. 2.3. Концептуальная модель безопасности информации

Разработка законодательной базы ИБ любого государства является необходимой мерой, удовлетворяющей первейшую потребность в защите информации при развитии социально-экономических, политических, военных направлений развития этого государства. Особое внимание со стороны западных стран к формированию такой базы вызвано все возрастающими затратами на борьбу с «информационными» преступлениями. Все это заставляет страны Запада серьезно заниматься вопросами законодательства по защите информации. Так, первый закон в этой области в США был принят в 1906 г., а к настоящему времени уже имеется более

500 законодательных актов по защите информации, ответственности за ее разглашение и компьютерные преступления.

*Определение основных принципов отнесения сведений, имеющих конфиденциальный характер, к защищаемой информации.* Созданием законодательной базы в области ИБ каждое государство стремится защитить свои информационные ресурсы. Информационные ресурсы государства в самом первом приближении могут быть разделены на три большие группы:

- информацию открытую - на распространение и использование которой не имеется никаких ограничений;
- информацию запатентованную - охраняется внутригосударственным законодательством или международными соглашениями как объект интеллектуальной собственности;
- информацию, «защищаемую» ее собственником, владельцем с помощью отработанных механизмов защиты государственной, коммерческой или другой охраняемой тайны; к этому виду относят обычно информацию, не известную другим лицам, которая или не может быть запатентована, или умышленно не патентуется с целью избежания или уменьшения риска завладения ее соперниками, конкурентами.

Защищают и охраняют, как правило, не всю или не всякую информацию, а наиболее важную, ценную для собственника, ограничение распространения которой приносит ему какую-то пользу или прибыль, возможность эффективно решать стоящие перед ним задачи.

Какую информацию относят к защищаемой?

Во-первых, секретную информацию. К секретной информации в настоящее время принято относить сведения, содержащие государственную тайну.

Во-вторых, конфиденциальную информацию. К этому виду защищаемой информации относят обычно сведения, содержащие коммерческую тайну, а также тайну, касающуюся личной (неслужебной) жизни и деятельности граждан.

Таким образом, под защищаемой информацией понимают сведения, на использование и распространение которых введены ограничения их собственником и характеризуемые понятием «тайна».

Применительно к органам государственной власти и управления под тайной понимается то, что скрывается от других, что известно определенному кругу людей. Иначе говоря, те сведения, которые не подлежат разглашению, и составляют тайну.

Основное направление использования этого понятия - засекречивание государством определенных сведений, сокрытие которых от соперников, потенциального противника дает ему возможность успешно решать жизненно важные вопросы в области обороны страны, политических, научно-технических и иных проблем с меньшими затратами сил и средств.

К подобному же ввиду тайны относится засекречивание предприятием, фирмой сведений, которые помогают ему эффективно решать задачи производства и выгодной реализации продукции.

Сюда же примыкают и тайны личной жизни граждан, обычно гарантируемые государством: тайна переписки, врачебная тайна, тайна денежного вклада в банке и др. Классификацию информации с точки зрения ее владельца можно представить в виде таблицы (табл. 2.1). Цветом выделена та информация, защита которой обеспечивается государством.

*Таблица 2.1. Классификация информации*

| *Владелец* | *Вид информации* | | | | |
|---|---|---|---|---|---|
| | *Защищаемая* | | *Запатентованная* | | *Открытая* |
| | *Секретная* | *Конфиденциальная* | *Патент* | *Авторское право* | |
| Личность | | ← Личная тайна. ← Персональные данные | Патент физического лица | Авторское право физического лица | |
| Общество | | Коммерческая тайна | Патент юридического лица | Авторское право юридического лица | |
| Государство | Государственная тайна | Служебные сведения | Государственный патент | | |

Защищают и охраняют, как правило, не всю или не всякую информацию, а наиболее важную, ценную для собственника, ограничение распространения которой приносит ему какую-то пользу или прибыль, возможность эффективно решать стоящие перед ним задачи. При этом различают признаки защищаемой информации:

- засекречивать информацию, т. е. ограничивать к ней доступ, может только ее собственник (владелец) или уполномоченные им на то лица;

- чем важнее для собственника информация, тем тщательнее он ее защищает; а для того чтобы все, кто сталкивается с этой защищаемой информацией, знали, что одну информацию необходимо оберегать более тщательно, чем другую, собственник определяет ей различную степень секретности;
- защищаемая информация должна приносить определенную пользу ее собственнику и оправдывать затрачиваемые на ее защиту силы и средства;
- секретная информация обладает определенным генетическим свойством: если эта информация является основанием для создания новой информации (документов, изделий и т. п.), то созданная на этой основе информация является, как правило, секретной.

Отличительным признаком защищаемой информации является то, что засекречивать ее может только ее собственник (владелец) или уполномоченные им на то лица.

Владельцами (собственниками) защищаемой информации могут быть:

- государство и его структуры (органы); в этом случае к ней относятся сведения, являющиеся государственной, служебной тайной, иные виды защищаемой информации, принадлежащей государству или ведомству; в их числе могут быть и сведения, являющиеся коммерческой тайной;
- предприятия, товарищества, акционерные общества (в том числе и совместные) и другие - информация является их собственностью и составляет коммерческую тайну;
- общественные организации - как правило, партийная тайна, не исключена также государственная и коммерческая тайна;
- граждане государства (их права - тайна переписки, телефонных и телеграфных разговоров, врачебная тайна, персональные данные и др. - гарантируются государством, личные тайны - их личное дело; следует отметить, что государство не несет ответственности за сохранность личных тайн).

Понятие «государственная тайна» является одним из важнейших в системе защиты государственных секретов в любой стране. От ее правильного определения зависит и политика руководства в области защиты секретов.

Определение этого понятия дано в Законе РФ «О государственной тайне»: «Государственная тайна - защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ».

Модель определения государственных секретов обычно включает в себя следующие существенные признаки.

1. Предметы, явления, события, области деятельности, составляющие государственную тайну.
2. Противник (данный или потенциальный), от которого в основном осуществляется защита государственной тайны.
3. Указание в законе, перечне, инструкции сведений, составляющих государственную тайну.
4. Наносимый ущерб обороне, внешней политике, экономике, научно-техническому прогрессу страны и т. п. В случае разглашения (утечки) сведений, составляющих государственную тайну.

Какие сведения могут быть отнесены к государственной тайне, определено в Указе Президента РФ от 30.11.1995 г. № 1203. К ним отнесены сведения (указаны лишь разделы): в областях военной, внешнеполитической и внешнеэкономической, экономической, научной, разведывательной, контрразведывательной и оперативно-розыскной деятельности.

Нельзя засекречивать информацию как имеющую статус государственной тайны:

- если ее утечка (разглашение и т. п.) не влечет ущерба национальной безопасности страны; в нарушение действующих законов;
- если сокрытие информации будет нарушать конституционные и законодательные права граждан;
- для сокрытия деятельности, наносящей ущерб окружающей природной среде, угрожающей жизни и здоровью граждан. Подробнее этот перечень содержится в ст. 7 Закона РФ «О государственной тайне».

Какие же используются критерии для отнесения сведений, во-первых, к государственной тайне, во-вторых, к той или иной степени секретности?

Ответ на этот вопрос дают Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности, указанные в постановлении Правительства РФ № 870 от 04.09.1995 г.

К сведениям особой важности следует относить сведения, распространение которых может нанести ущерб интересам РФ в одной или нескольких областях.

К совершенно секретным сведениям следует относить сведения, распространение которых может нанести ущерб интересам министерства (ведомства) или отраслям экономики РФ в одной или нескольких областях.

К секретным сведениям следует относить все иные из числа сведений, составляющих государственную тайну. Ущерб может быть нанесен интересам предприятия, учреждения или организации.

Как видно из изложенного, разница между тремя степенями секретности зависит от величины ущерба.

Понятие, виды и размер ущерба разработаны пока еще недостаточно и, видимо, будут отличны для каждого конкретного объекта защиты - содержания сведений, составляющих государственную тайну, сущности отраженных в ней фактов, событий, явлений действительности. В зависимости от вида, содержания и размеров ущерба можно выделить группы некоторых видов ущерба при утечке (или возможной утечке) сведений, составляющих государственную тайну.

Политический ущерб может наступить при утечке сведений политического и внешнеполитического характера, о разведывательной деятельности спецслужб государства и др. Политический ущерб может выражаться в том, что в результате утечки информации могут произойти серьезные изменения в международной обстановке не в пользу РФ, утрата страной политических приоритетов в каких-то областях, ухудшение отношений с какой-либо страной или группой стран и т. д.

Экономический ущерб может наступить при утечке сведений любого содержания: политического, экономического, военного, научно-технического и т. д. Экономический ущерб может быть выражен прежде всего в денежном исчислении. Экономические потери от утечки информации могут быть прямыми и косвенными.

Так, прямые потери могут наступить в результате утечки секретной информации о системах вооружения, обороны страны, которые в результате этого практически потеряли или утратили свою эффективность и требуют крупных затрат на их замену или переналадку.

Косвенные потери чаще всего выражаются в виде размера упущенной выгоды: срыв переговоров с иностранными фирмами, о выгодных сделках с которыми ранее была договоренность; утрата приоритета в научном исследовании, в результате соперник быстрее довел свои исследования до завершения и запатентовал их и т. д.

Моральный ущерб, как правило, неимущественного характера наступает от утечки информации, вызвавшей или инициировавшей противоправную государству пропагандистскую кампанию, подрывающую репутацию страны, приведшую к выдворению из каких-то государств наших

дипломатов, разведчиков, действовавших под дипломатическим прикрытием, и т. п.

Проблема засекречивания информации и определения степени секретности сведений, документов, изделий и работ является одной из стержневых во всей деятельности по защите информации. Она имеет большое государственное значение, определяет методологию и методику защиты информации, объем работ по ее защите и другие обстоятельства, связанные с деятельностью государственных органов, предприятий и организаций в этой области. Правила засекречивания информации определяют в конечном счете политику государства в области защиты секретов. Этим и объясняется, что перечни сведений, составляющих государственную тайну, утверждаются у нас в стране на самом высоком уровне, в них находит отражение концепция руководства страны в области защиты государственных секретов.

Засекречивать информацию имеют право органы власти, управления и должностные лица, наделенные соответствующими полномочиями. Они

- осуществляют политику государства в области защиты информации;
- определяют категории сведений, подлежащих защите и, следовательно, засекречиванию, и закрепляют это в законодательных актах;
- разрабатывают перечни сведений, подлежащих засекречиванию;
- определяют степени секретности документов, изделий, работ и сведений и проставляют на носителях защищаемой информации соответствующие грифы секретности.

Таким образом, засекречивание информации - это совокупность организационно-правовых мер, регламентированных законами и другими нормативными актами, по введению ограничений на распространение и использование информации в интересах ее собственника (владельца).

Обозначим кратко основные принципы засекречивания информации.

1. Законность засекречивания информации. Заключается в осуществлении его строго в рамках действующих законов и других подзаконных нормативных актов. Отступление от этого принципа может нанести серьезный ущерб интересам защиты информации, интересам личности, общества и государства, в частности незаконным сокрытием от общества информации, не требующей засекречивания, или утечки важной информации.
2. Обоснованность засекречивания информации. Заключается в установлении путем экспертной оценки целесообразности засекречивания конкретных сведений, вероятных экономических или иных по-

следствий этого акта, исходя из баланса жизненно важных интересов личности, общества и государства. Неоправданно засекречивать информацию, вероятность раскрытие которой превышает возможность сохранения ее в тайне.

3. Своевременность засекречивания информации. Заключается в установлении ограничений на распространение этих сведений с момента их получения (разработки) или заблаговременно.
4. Подчиненность ведомственных мероприятий по засекречиванию информации общегосударственным интересам. Это в первую очередь относится к области защиты государственной тайны. Что касается коммерческой тайны, то предприятия наделены правами засекречивания информации, кроме оговоренных в законе случаев.

В РФ в соответствии с Законом «О государственной тайне» складывается в настоящее время следующая форма засекречивания информации. Закон определяет категории сведений, отнесенных к государственной тайне, затем президент РФ на основе предложений правительства РФ утверждает два перечня: Перечень должностных лиц органов государственной власти и управления, наделенных полномочиями по отнесению сведений к государственной тайне, и Перечень сведений, отнесенных к государственной тайне - для осуществления единой государственной политики в области засекречивания информации.

Руководители, наделенные полномочиями по засекречиванию информации, утверждают своими приказами перечни сведений, подлежащих засекречиванию, в соответствии с их отраслевой, ведомственной или программно-целевой принадлежностью. Они же наделяются полномочиями распоряжения этими сведениями, пересмотра степени их секретности и рассекречивания.

Предприятия при определении степени (грифа) секретности документов, изделий, работ по-прежнему будут руководствоваться перечнями сведений, подлежащих засекречиванию. Таким образом, до исполнителей будут доводиться стратегические установки на применение режимных ограничений в конкретных ситуациях. Рассмотренный порядок засекречивания сведений представлен на рис. 2.4.

Степень секретности и конфиденциальности информации, отображенной в документах, изделиях и т. д., не остается постоянной. Она обычно уменьшается и, реже (например, документы представляют историческую и иную ценность), может увеличиваться. Степень секретности и конфиденциальности информации периодически должна пересматриваться. При этом она может быть увеличена, снижена до фактической или рассекречена вообще.

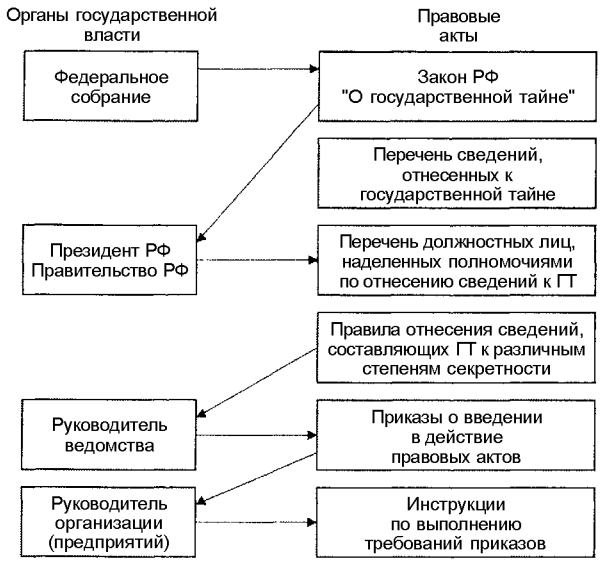



Рис. 2.4. Порядок засекречивания информации, составляющей государственную тайну

Рассекречивание конфиденциальной и секретной информации, работ, документов, изделий - это деятельность предприятий по снятию (частичному или полному) ограничений на доступ к ранее засекреченной информации, на доступ к ее носителям, вызываемая требованиями законов и объективными факторами: изменением международной и внутригосударственной обстановки, появлением более совершенных видов определенной техники, снятием изделий с производства, передачей (продажей) научно-технических решений оборонного характера в народное хозяйство, продажей изделия за границу и т. д., а также взятием государством на себя международных обязательств по открытому обмену сведениями, составляющими в РФ государственную тайну. Информация должна оставаться секретной или конфиденциальной до тех пор, пока этого требуют интересы национальной безопасности или конкурентной и коммерческой деятельности предприятия.

Принципиальные аспекты рассекречивания информации могут быть изложены в следующих основных положениях.

1. Информация не подлежит засекречиванию, а засекреченная должна быть рассекречена, если это сделано необоснованно и в нарушение действующих законов, в целях сокрытия нарушений законности,

в результате неумелого руководства и должностных ошибок, нарушения конституционных и других законодательных прав граждан.

2. Информация рассекречивается не позднее сроков, установленных при ее засекречивании. Ранее этих сроков подлежит рассекречиванию лишь информация, которая попадает под действие взятых РФ на себя международных обязательств по открытому обмену информацией. Срок засекречивания информации, отнесенной к государственной тайне, не должен превышать 30 лет. Правом продления сроков засекречивания информации наделяются руководители центральных органов федеральной исполнительной власти, осуществившие отнесение соответствующих сведений к государственной тайне.
3. Информация не подлежит засекречиванию, а засекреченная должна быть рассекречена, если содержащиеся в ней новые научные, проектные, технологические и т. п. разработки находятся ниже мирового технологического уровня или достаточно подробно раскрыты в опубликованной зарубежной или в отечественной литературе.
4. Рассекречиванию (разглашению) не подлежат сведения, затрагивающие личную (неслужебную) жизнь граждан страны, если на обратное не имеется согласия самих граждан, а в случае их смерти - их ближайших родственников. Иной порядок такого рассекречивания рассматривается через суд.

## 2.2. Государственная система правового обеспечения защиты информации в Российской Федерации

Второй функцией организационно-правового обеспечения информационной безопасности является определение системы органов и должностных лиц, ответственных за обеспечение информационной безопасности в стране. Основой для создания государственной системы организационно-правового обеспечения защиты информации является создаваемая в настоящее время государственная система защиты информации, под которой понимается совокупность федеральных и иных органов управления и взаимоувязанных правовых, организационных и технических мер, осуществляемых на различных уровнях управления и реализации информационных отношений и направленных на обеспечение безопасности информационных ресурсов.

Основные положения правового обеспечения защиты информации приведены в Доктрине информационной безопасности РФ, а также в других законодательных актах.

Под информационной безопасностью РФ понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Напомним содержание интересов личности, общества и государства в информационной сфере.

Интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.

Интересы общества в информационной сфере заключаются в обеспечении интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении России.

Интересы государства в информационной сфере заключаются в создании условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества.

На основе национальных интересов РФ в информационной сфере формируются стратегические и текущие задачи внутренней и внешней политики государства по обеспечению информационной безопасности.

Рассмотрим структуру государственной системы информационной безопасности, представленную на рис. 2.5, и основные функции ее составных частей.

Основным органом, координирующим действия государственных структур по вопросам защиты информации, является Межведомственная комиссия по защите государственной тайны, созданная Указом Президента РФ № 1108 от 8.11.1995 г. Она действует в рамках Государственной системы защиты информации от утечки по техническим каналам, положение о которой введено в действие постановлением Правительства РФ от 15.09.1993 г. №912-51. В этом постановлении определены структура, задачи и функции, а также организация работ по защите информации применительно к сведениям, составляющим государственную тайну. Основной задачей Государственной системы защиты информации является

проведение единой технической политики, организация и координация работ по защите информации в оборонной, экономической, политической, научно-технической и других сферах деятельности страны.

| *НОРМЫ* | | *УПРАВЛЕНИЕ* | | *КОНТРОЛЬ* |
|---|---|---|---|---|
| Международное право | → | Организация Объединенных Наций<br>Совет безопасности ООН | ← | Международный суд |
| Федеральное законодательство | → | Президент РФ<br>Совет безопасности<br>Государственная дума<br>Межведомственная комиссия по защите государственной тайны<br>ФСТЭК, ФСБ, СВР и др. | ← | Конституционный суд<br>Верховный суд<br>Генеральная прокуратура |
| Ведомственные нормативные акты | → | Органы государственного управления<br>Органы по защите информации | ← | Суды<br>Прокуратура |
| Инструктивно-методические документы | → | Руководитель объединения, подразделения<br>Органы по защите информации | ← | Административные органы |

Рис. 2.5. Структура государственной системы информационной безопасности

Общая организация и координация работ в стране по защите информации, обрабатываемой техническими средствами, осуществляется Федеральная служба по техническому и экспортному контролю (ФСТЭК России).

ФСТЭК России является федеральным органом исполнительной власти, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности по следующим вопросам в области обеспечения информационной безопасности:

1) обеспечению безопасности информации в системах информационной и телекоммуникационной инфраструктуры, оказывающих существенное влияние на безопасность государства в информационной сфере;

2) противодействию иностранным техническим разведкам на территории РФ;

3) обеспечению защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом, предотвращению ее утечки по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней на территории РФ;

4) защите информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств.

Основными задачами в области обеспечения информационной безопасности для ФСТЭК России являются:

1) реализация в пределах своей компетенции государственной политики в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации;

2) осуществление государственной научно-технической политики в области защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств;

3) организация деятельности государственной системы противодействия техническим разведкам и технической защиты информации на федеральном, межрегиональном, региональном, отраслевом и объектовом уровнях, а также руководство указанной государственной системой;

4) осуществление самостоятельного нормативно-правового регулирования вопросов: обеспечения безопасности информации в ключевых системах информационной инфраструктуры; противодействия техническим разведкам; технической защиты информации; размещения и использования иностранных технических средств наблюдения и контроля в ходе реализации международных договоров РФ, иных программ и проектов на территории РФ, на континентальном шельфе и в исключительной экономической зоне РФ; координации деятельности органов государственной власти по подготовке развернутых перечней сведений, подлежащих засекречиванию, а также методического руководства этой деятельностью;

5) обеспечение в пределах своей компетенции безопасности информации в ключевых системах информационной инфраструктуры, противо-

действия техническим разведкам и технической защиты информации в аппаратах федеральных органов государственной власти и органов государственной власти субъектов РФ, в федеральных органах исполнительной власти, органах исполнительной власти субъектов РФ, органах местного самоуправления и организациях;

6) прогнозирование развития сил, средств и возможностей технических разведок, выявление угроз безопасности информации;

7) противодействие добыванию информации техническими средствами разведки, техническая защита информации;

8) осуществление координации деятельности федеральных органов исполнительной власти, органов исполнительной власти субъектов РФ и организаций по государственному регулированию размещения и использования иностранных технических средств наблюдения и контроля в ходе реализации международных договоров РФ, иных программ и проектов на территории РФ, на континентальном шельфе и в исключительной экономической зоне РФ;

9) осуществление в пределах своей компетенции контроля деятельности по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, по противодействию техническим разведкам и по технической защите информации в аппаратах федеральных органов государственной власти и органов государственной власти субъектов РФ, в федеральных органах исполнительной власти, органах исполнительной власти субъектов РФ, органах местного самоуправления и организациях;

10) осуществление центральным аппаратом ФСТЭК России организационно-технического обеспечения деятельности Межведомственной комиссии по защите государственной тайны.

ФСТЭК России в своей деятельности руководствуется Конституцией РФ, федеральными конституционными законами, федеральными законами, актами президента РФ и правительства РФ, международными договорами РФ, приказами и директивами министра обороны РФ в части, касающейся ФСТЭК России, настоящим положением о ФСТЭК России, а также другими нормативными правовыми актами РФ, касающимися деятельности ФСТЭК России.

Нормативные правовые акты и методические документы, изданные по вопросам деятельности ФСТЭК России, обязательны для исполнения аппаратами федеральных органов государственной власти и органов государственной власти субъектов РФ, федеральными органами исполни-

тельной власти, органами исполнительной власти субъектов РФ, органами местного самоуправления и организациями.

ФСТЭК России осуществляет свою деятельность во взаимодействии с другими федеральными органами исполнительной власти, органами исполнительной власти субъектов РФ, органами местного самоуправления и организациями.

Обеспечение информационной безопасности является одним из основных направлений деятельности органов Федеральной службы безопасности.

Обеспечение информационной безопасности осуществляется ими в пределах своих полномочий:

- при формировании и реализации государственной и научно-технической политики в области обеспечения информационной безопасности, в том числе с использованием инженерно-технических и криптографических средств;
- при обеспечении криптографическими и инженерно-техническими методами безопасности информационно-телекоммуникационных систем, а также систем шифрованной, засекреченной и иных видов специальной связи в РФ и ее учреждениях, находящихся за пределами РФ.

ФСБ России предоставлено право:

1) осуществлять в соответствии со своей компетенцией регулирование в области разработки, производства, реализации, эксплуатации шифровальных (криптографических) средств и защищенных с использованием шифровальных средств систем и комплексов телекоммуникаций, расположенных на территории РФ, а также в области предоставления услуг по шифрованию информации в РФ, выявления электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах;

2) осуществлять государственный контроль за организацией и функционированием криптографической и инженерно-технической безопасности информационно-телекоммуникационных систем, систем шифрованной, засекреченной и иных видов специальной связи, контроль за соблюдением режима секретности при обращении с шифрованной информацией в шифровальных подразделениях государственных органов и организаций на территории РФ и в ее учреждениях, находящихся за пределами РФ, а также в соответствии со своей компетенцией контроль за обеспечением защиты особо важных объектов (помещений) и находящихся в них технических средств от утечки информации по техническим каналам;

3) участвовать в определении порядка разработки, производства, реализации, эксплуатации и обеспечения защиты технических средств обработки, хранения и передачи информации ограниченного доступа, предназначенных для использования в учреждениях РФ, находящихся за ее пределами;

4) обеспечивать выявление устройств перехвата информации на особо важных объектах (в помещениях) и технических средствах, предназначенных для использования в федеральных органах государственной власти.

Служба внешней разведки РФ для осуществления своей деятельности может при собственных лицензировании и сертификации приобретать, разрабатывать (за исключением криптографических средств защиты), создавать, эксплуатировать информационные системы, системы связи и системы передачи данных, а также средства защиты информации от утечки по техническим каналам.

Министерство обороны (Минобороны России) организует деятельность по обеспечению информационной безопасности, защите государственной тайны в Вооруженных силах, а также в установленном порядке в пределах своей компетенции работы по сертификации средств защиты информации.

Другие органы государственного управления (министерства, ведомства) в пределах своей компетенции:

- определяют перечень охраняемых сведений;
- обеспечивают разработку и осуществление технически и экономически обоснованных мер по защите информации на подведомственных предприятиях;
- организуют и координируют проведение НИОКР в области защиты информации в соответствии с государственными (отраслевыми) программами;
- разрабатывают отраслевые документы по защите информации;
- контролируют выполнение на предприятиях отрасли установленных норм и требований по защите информации;
- создают отраслевые центры по защите информации и контролю эффективности принимаемых мер;
- организуют подготовку и повышение квалификации специалистов по защите информации.

Для осуществления указанных функций в составе органов государственного управления функционируют научно-технические подразделения (центры) защиты информации и контроля.

На предприятиях, выполняющих оборонные и иные секретные работы, функционируют научно-технические подразделения защиты информации и контроля, координирующие деятельность в этом направлении научных и производственных структурных подразделений предприятия, участвующие в разработке и реализации мер по защите информации, осуществляющие контроль эффективности этих мер.

Кроме того, в отраслях промышленности и в регионах страны создаются и функционируют лицензионные центры, осуществляющие организацию и контроль за лицензионной деятельностью в области оказания услуг по защите информации, органы по сертификации средств вычислительной техники и средств связи, испытательные центры по сертификации конкретных видов продукции по требованиям безопасности информации, органы по аттестации объектов информатики.

Государственная система обеспечения информационной безопасности создается для решения следующих проблем, требующих законодательной поддержки:

- защита персональных данных;
- борьба с компьютерной преступностью, в первую очередь в финансовой сфере;
- защита коммерческой тайны и обеспечение благоприятных условий для предпринимательской деятельности;
- защита государственных секретов;
- создание системы взаимных финансовых расчетов в электронной форме с элементами цифровой подписи;
- обеспечение безопасности АСУ потенциально опасных производств;
- страхование информации и информационных систем;
- сертификация и лицензирование в области безопасности, контроль безопасности информационных систем;
- организация взаимодействия в сфере защиты данных со странами-членами СНГ и другими государствами.

Анализ современного состояния информационной безопасности в России показывает, что уровень ее в настоящее время не соответствует жизненно важным потребностям личности, общества и государства.

Такое положение дел в области обеспечения информационной безопасности требует безотлагательного решения ряда ключевых проблем.

1. Формирование законодательной и нормативно-правовой базы обеспечения информационной безопасности, в том числе разработка реестра информационного ресурса, регламента информационного обмена для органов государственной власти и управления, нормативного закрепления ответственности должностных лиц и граждан по соблюдению требований информационной безопасности.
2. Разработка механизмов реализации прав граждан на информацию.
3. Формирование системы информационной безопасности, обеспечивающей реализацию государственной политики в этой области.
4. Совершенствование методов и технических средств, обеспечивающих комплексное решение задач защиты информации.
5. Разработка критериев и методов оценки эффективности систем и средств информационной безопасности.
6. Исследование форм и способов цивилизованного воздействия государства на формирование общественного сознания.
7. Комплексное исследование деятельности персонала информационных систем, в том числе методов повышения мотивации, морально-психологической устойчивости и социальной защищенности людей, работающих с секретной и конфиденциальной информацией.

Разработка правового обеспечения защиты информации идет по трем направлениям.

1. Защита прав личности на частную жизнь.
2. Защита государственных интересов.
3. Защита предпринимательской и финансовой деятельности.

Структура нормативной базы по вопросам информационной безопасности включает:

- Конституцию РФ;
- федеральные законы и законы РФ;
- кодексы РФ (уголовный, гражданский, об административных правонарушениях);
- постановления правительства РФ;
- ведомственные нормативные акты, ГОСТы, руководящие документы.

Среди федеральных законов отметим следующие:

- «О государственной тайне»;
- «О безопасности»;
- «О лицензировании отдельных видов деятельности»;
- «Об информации, информатизации и защите информации»;
- «О правовой охране программ для электронных вычислительных машин и баз данных»;
- «О техническом регулировании»;
- «Об участии в международном информационном обмене»;
- «О связи»;
- «Об органах Федеральной службы безопасности в РФ»;
- «О коммерческой тайне»;
- «Об электронной цифровой подписи».

Пора чудес прошла, и нам
подыскивать приходится причины
всему, что совершается на свете.
*У. Шекспир*

## 3. Информационные системы

XXI в. пройдет под знаком все усиливающейся экспансии информационной технологии в самые различные области человеческой деятельности, включая экономику, промышленность, управление, образование и культуру. Сами понятия информации, информационных процессов, информационных систем все шире используются в науке и практике. Сегодня мало кто сомневается в определяющей роли информации в теории искусственного интеллекта, в науке об ЭВМ, теории связи и коммуникации, в теории управления. А такие производные понятия, как «эра информации», «глобальная информационная революция», «информационное общество», «информационный взрыв», «информационный кризис», все чаще встречаются не только в научно-теоретической литературе, но и в СМИ.

Все это свидетельствует о том, что наступила новая эра, где объективным началом и основанием стало не вещество или энергия, а информация. На смену материальному (физическому) миру с его законами и системой ценностей пришел более сущностный информационный мир.

На смену материальной цивилизации, так долго господствовавшей во всемирной истории, пришла информационная цивилизация, известившая начало периода информации: «всеобщего и неизбежного периода развития человеческой цивилизации, периода освоения его информационной картины мира, осознания единства законов функционирования информации в природе и обществе, практического их применения, создания индустрии производства и обработки информации в виде разнообразных информационных систем» [15]. В современных условиях резко возрастает роль информационных процессов как в производстве, ориентированном на гибкую автоматизацию, так и в духовной сфере, использующей еще традиционные информационные средства и все шире переходящей на использование современных средств автоматизации. Не малую роль здесь играют факторы организации информационной среды, оптимальное определение путей движения информации как товара, проблемы обеспечения ее безопасности.

Последние десятилетия научный и технический прогресс связан со все более глубоким и широким рассматриванием различных свойств информации. Наряду с философскими и математическими проблемами информации большое внимание уделяется различным инженерным проблема ее использования (вопросы передачи, преобразования, хранения и т. д.), обеспечения целостности, достоверности и защиты от различного рода угроз.

Основным инструментом работы с информационными потоками сегодня выступают информационные способы, предназначенные не только для информационных преобразований, сбора и передачи информации, но и для качественного, своевременного и достоверного удовлетворения информационных потребностей пользователей этих систем.

## 3.1. Общие положения

Интенсивно развивающиеся процессы переустройства нашего общественного бытия и сознания требуют высокого уровня информированности общества, его организаций и граждан во всех областях экономической, политической и социальной действительности. Такой процесс сегодня принято называть информатизацией.

**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.

Информатизация базируется на национальных информационных ресурсах и обеспечивается посредством информационных систем и телекоммуникационных сетей. Появление телекоммуникационных сетей создало технические предпосылки для развития информационных систем, использующих коммуникационные ресурсы для обеспечения доступа к информационным ресурсам. Таким образом, информационные системы и сети, средства связи, передачи информации и телекоммуникации составляют инфраструктуру информатизации [9]. Компоненты информант представлены на рис. 2.6.


Рис. 2.6. Компоненты информатизации

При любом рассмотрении вопросов управления производственной деятельностью центральное место занимает информация или информационная потребность.

В самом общем виде при решении проблемы удовлетворения информационной потребности необходимо иметь в виду три компонента: человека (потребителя информации), который формулирует свои задачи; информационный фонд (информационный ресурс), в котором сосредоточена необходимая человеку информация, и соответствующее устройство,

которое является посредником между потребителем и информационным массивом. Это устройство и называется *информационной системой.*

Чтобы объяснить понятие «информационная система» напомним, что любое предприятие или любая организация - система, в которой происходят сложные процессы преобразования материалов в готовую продукцию, обращаются потоки сырья, полуфабрикатов, инструмента, трудовых затрат, денежных средств и т. д. И все это отражается в управлении. Таким образом, управление и планирование, в свою очередь, являются системой, которая информирует нас обо всем, что происходит на предприятии. В ней также происходит преобразование, только не материалов, а информации. Это и будет информационная система [12].

Информационная система, как и любая другая, обладает определенной структурой, составом, специалистами, средствами, оборудованием и порядком функционирования; структура информационной системы представлена на рис. 2.7.


Рис. 2.7. Структура информационной системы

Таким образом, мы приходим к определению информационной системы [31]. **Информационная система** - это организационно упорядоченная совокупность информационных ресурсов, технических средств, технологий, реализующих информационные процессы в традиционном или автоматизированном режиме для удовлетворения информационных потребностей пользователей.

Продуктом информационной системы является информация, свойства которой изменяются в соответствии с заданной технологией с помощью комплекса различных технических средств и людей, выполняющих определенные технологические операции. Известно, что технологические операции - это совокупность действий, направленных на изменение состояния предмета производства. В информационной системе предметом производства является информация, которая на выходе системы приводится к нужному пользователю виду и содержанию [23].

Исходной материальной основой работы информационной системы выступают информационные ресурсы. Ресурсами, как известно, называют элементы экономического потенциала, которыми располагает общество и которые при необходимости могут быть использованы для достижения конкретных целей хозяйственного и социального развития. Давно стали привычными такие категории, как материальные, финансовые, трудовые, природные, энергетические ресурсы. Эти ресурсы вовлекаются в хозяйственный оборот, и их назначение понятно каждому. В последние годы появилось и все больше осознается понятие «информационные ресурсы». Под информационными ресурсами понимаются документы и массивы документов в разных формах и видах (библиотеки, архивы, фонды, базы данных, базы знаний, а равно и другие формы организации, хранения и поиска информации), содержащие информацию по всем направлениям жизнедеятельности общества [9].

Информационные ресурсы могут быть фиксированными и нефиксированными. Фиксированные информационные ресурсы представляют собой информацию, закрепленную на каком-нибудь физическом носителе, а нефиксированные - знания, которыми владеют люди (ученые, специалисты, работники), так или иначе участвующие в общественном производстве и способные передавать эти знания другим участникам производственного процесса или криминального устремления.

Функциональной основой любой информационной системы являются информационные процессы. Под информационными процессами понимается совокупность взаимосвязанных и взаимообусловленных процессов выявления, анализа, ввода и отбора информации, выдачи с помощью различных средств ее потребителю для принятия управленческого решения.

## 3.2. Информация как продукт

Как и всякий продукт, информация имеет потребителей, нуждающихся в ней, и потому обладает определенными потребительскими качествами, а также имеет своих обладателей (владельцев).

С точки зрения потребителя качество используемой при управлении производством информации позволит получить дополнительный экономический или социально-моральный эффект.

С точки зрения обладателя - сохранение в тайне коммерчески важной информации позволяет успешно конкурировать на рынке производства и сбыта товаров и услуг.

Так что же такое информация? Какими свойствами она обладает?

**Информация** - это сведения о лицах, предметах, событиях, явлениях и процессах (независимо от формы их представления), отраженные на материальных носителях, используемые в целях получения знаний и практических решений.

Наиболее важными в практическом плане свойствами информации является: ценность, достоверность, своевременность.

Ценность информации определяется обеспечением возможности достижения цели, поставленной перед получателем.

Достоверность - соответствие полученной информации действительной обстановке.

Своевременность, т. е. соответствие ценности и достоверности определенному временному периоду.

Эффективность принимаемых решений определяется, кроме того, системой факторов, характеризующих показатели информации. Среди них можно выделить такие, как:

- внутренние свойства (достоверность и кумулятивность), сохраняющиеся при переносе данных в другую среду (систему);
- внешние свойства (временные свойства и свойства защищенности, которые характерны для данных, находящихся (используемых) в определенной среде (системе), и которые исчезают при их переносе в другую систему [8].

Рассмотрим подробнее приведенные свойства информации (рис. 2.8).

**Достоверность.** В свойстве достоверности выделяются безошибочность и истинность данных. Под безошибочностью понимается свойство данных не иметь скрытых случайных ошибок. Случайные ошибки в данных обусловлены, как правило, ненамеренными искажениями содержания сведений человеком или сбоями технических средств при переработ-

ке данных в ИС. При анализе истинности данных рассматривают преднамеренные искажения данных человеком-источником сведений (в том числе и из-за неумения или непонимания сути вопроса) или искажения, вносимые средствами обработки информации.


Рис. 2.8. Характеристики информации

**Кумулятивность.** Кумулятивность определяет такие понятия, как «гомоморфизм» (соотношение между объектами двух множеств, при котором одно множество является моделью другого) и «избирательность». Данные, специально отобранные для конкретного уровня пользователей, обладают определенным свойством - избирательностью. Это социальная составляющая кумулятивности.

**Временные свойства.** Временные свойства определяют способность данных отображать динамику изменения ситуации (динамичность). При этом можно рассматривать или время запаздывания появления в данных

соответствующих признаков объектов, или расхождение реальных признаков объекта и тех же признаков, отображаемых в данных. Соответственно можно выделить:

- актуальность - свойство данных, характеризующих текущую ситуацию;
- оперативность - свойство данных, состоящее в том, что время их сбора и переработки соответствует динамике изменения ситуации;
- идентичность - свойство данных соответствовать состоянию объекта.

Нарушение идентичности связано с техническим (по рассогласованию признаков) старением информации, при котором происходит расхождение реальных признаков объектов и тех же признаков, отображенных в информации.

В плане социальных мотивов рассматриваются:

- срочность - свойство данных соответствовать срокам, определяемым социальными мотивами;
- значимость - свойство данных сохранять ценность для потребителя с течением времени, т. е. не подвергаться моральному старению.

**Защищенность данных.** При рассмотрении защищенности можно выделить технические аспекты защиты данных от несанкционированного доступа (свойство недоступности) и социально-психологические аспекты классификации данных по степени их конфиденциальности и секретности (свойство конфиденциальности) [8, 9].

Дополнительно можно выделить и такие свойства информации, как:

1. Общественная природа (источником информации является познавательная деятельность людей, общества).
2. Языковая природа (информация выражается с помощью языка, т. е. знаковой системы любой природы, служащей средством общения, мышления, выражения мысли. Язык может быть естественным, используемым в повседневной жизни и служащим формой выражения мыслей и средством общения между людьми и искусственным, созданным людьми для определенных целей (например, язык математической символики, информационно-поисковый, алгоритмический и др.).
3. Неотрывность от языка носителя.
4. Дискретность (единицами информации как средствами выражения являются слова, предложения, отрывки текста, а в плане содержания - понятия, высказывания, описание фактов, гипотезы, теории, законы и др.).

5. Независимость от создателей.
6. Старение (основной причиной старения информации является не само время, а появление новой информации, с поступлением которой прежняя информация оказывается неверной, перестает адекватно отображать явления и закономерности материального мира, человеческого общения и мышления).
7. Рассеяние (т. е. существование в многочисленных источниках) [11].

Американские менеджеры утверждают: «Бизнес - на 90 % информация и лишь на 10 % - удача». Увы, сегодняшние российские бизнесмены зачастую придерживаются прямо противоположных взглядов. Дело в том, что информационные потребности российского рынка только формируются.

На сегодня рынок информации в России многообразен и динамичен. Активно используя самые совершенные технологии, он расширяется за счет формирования новых общественных потребностей и начинает доминировать в мировой экономике наряду с энергетическим рынком. Чтобы оценить масштабность рынка информации, достаточно посмотреть на его структуру. В число основных секторов этого рынка входят:

- традиционные СМИ (телевидение, радио, газеты);
- справочные издания (энциклопедии, учебники, словари, каталоги и т. д.);
- справочно-информационные службы (телефонные службы, справочные бюро, доски объявлений и др.);
- консалтинговые службы (юридические, маркетинговые, налоговые и др.);
- компьютерные информационные системы;
- отраслевые базы данных;
- Интернет.

Возможно, этот перечень неполон, однако основные направления он отражает.

Компьютерный сектор рынка имеет ряд особенностей, выделяющих его изо всех остальных.

Во-первых, он дает новое качество информационных услуг - быстрый поиск в больших массивах информации. В Интернете существуют различные поисковые системы информации (Aport, Rambler, Яndex и т. д.).

Во-вторых, позволяет реализовать полный цикл технологии ввода, хранения, обновления и доставки информации потребителям с наиболее эффективными алгоритмическими решениями на отдельных этапах.

В-третьих, компьютерный сектор очень быстро развивается и начинает оказывать влияние на другие секторы информационного рынка. В первую очередь это относится к системам телетекста в сочетании с обычным телевидением, а также к системам мультимедиа, которые начинают конкурировать с полиграфическими изданиями справочной и учебной литературы.

В России компьютерный сектор информационного рынка переживает сложный этап становления. Если в 1988 г. этот рынок практически отсутствовал (не считая отдельных попыток продажи баз данных на дискетах и услуг бюджетных информационных институтов), то в 1995 г. - налицо реальное предложение целого спектра информационных товаров и услуг. Это уже рынок со своими лидерами, своей историей и множеством проблем.

Динамику изменения распределения потребителей информации по отраслям можно охарактеризовать следующей таблицей и гистограммой.

| *N n/n* | *Потребители информации* | *1995 г., %* | *2001 г., увелич. в разы* |
|---|---|---|---|
| 1 | Машиностроение | 19,2 | 2,3 |
| 2 | СМИ, библиотеки | 16,7 | 3 |
| 3 | Банки, инвестиционные фонды, страховые компании | 7,4 | 2 |
| 4 | Торговые дома, биржи | 6,9 | 1,5 |
| 5 | Шахты, карьеры, буровые | 5,0 | 1,5 |
| 6 | АЭС, ГЭС, ТЭЦ, ГРЭС | 3,5 | 2 |
| 7 | Высшие и средние УЗ | 4,2 | 11,5 |
| 8 | НИИ, ВЦ | 3,9 | 2 |
| 9 | Пищевая промышленность | 3,5 | 1,5 |
| 10 | Сервис | 2,7 | 4 |
| 11 | Нефтехимия | 2,1 | 2,5 |
| 12 | Предприниматель с.-х. продукции | 2,0 | 1,5 |
| 13 | Транспорт | 2,0 | 4 |
| 14 | Представительства инофирм | 1,8 | 3 |
| 15 | Органы управления | 1,4 | 5 |
| 16 | Информационные и рекламные агентства | 1,4 | 8 |
| 17 | Военные организации | 1,3 | 4 |
| 18 | Прочие | 5,4 | 1,5 |


## 3.3. Информационные услуги

Любая ИС призвана удовлетворить определенные информационные потребности ее пользователей, предоставляя им различные информационные услуги.

Действия, реализующие обеспечение доступа к информационным услугам, осуществляются соответствующей службой информационной системы. При этом под службой понимается совокупность действий и компонентов ИС, обеспечивающих соответствующие услуги.

Используются два способа классификации служб, отражающие различные аспекты предоставляемых услуг - по функциям и по режимам доступа к услугам.

В зависимости от режима доступа пользователя к службам они подразделяются на две категории - интерактивные службы и службы с разветвленным режимом работы. Интерактивные службы, в свою очередь, делятся на три класса - диалоговые, службы с накоплением, службы по запросу.

Диалоговая служба представляет собой совокупность средств для прямой передачи информации в реальном масштабе времени (без промежуточного накопления и хранения) между пользователями. К службам данного вида относится телефония, телетекс, телефакс, речевая конференц-связь, IP-телефония, Интернет-конференции.

Службы с накоплением предназначены для непрямой связи между пользователями с применением средств для промежуточного хранения сообщений. Примером службы данного типа является электронная почта для передачи данных, текстов, графических изображений.

Службы по запросу обеспечивают возможность пользователю извлекать необходимую информацию из банков данных. В общем случае предполагается всеобщее неограниченное использование информации

любым абонентом, имеющим право на доступ к службе. В частных случаях возможно разрешение доступа к той или иной информации только для определенных групп пользователей. Информация в этом случае предоставляется пользователю только по его требованию и в заданный им момент времени. Наиболее типичным примером такой службы является видеотекст.

Службы с разветвленным режимом работы обеспечивают распределение сообщений от одного центрального источника к неограниченному числу абонентов, имеющих право на ее прием. К службам данного типа относится, в частности, телетекс, а также службы передачи звукового и телевизионного вещания.

### *3.3.1. Разновидности информационных систем*

Современные телекоммуникационные сети информационных систем характеризуются следующими основными отличительными признаками:

- видом передаваемой информации - телефонные, телеграфные, передачи данных, факсимильные, с интеграцией служб и т. п.;
- обслуживаемой территорией - международные, междугородные, местные (городские, сельские), внутрипроизводственные;
- сферой применения - общего пользования, ведомственные, производственные, диспетчерские и т. п.;
- способом распределения и доставки информации - по прямым каналам, по коммутируемым каналам;
- методом коммутации - с коммутацией каналов, сообщений, пакетов, с использованием комбинированных методов (гибридных, адаптивных и т. п.);
- используемой физической средой передачи информации - кабельные, оптоволоконные, радио-, спутниковые и т. п. каналы.

В настоящее время на территории России функционируют или вводятся в эксплуатацию телекоммуникационные сети следующих видов:

- сети связи с коммутацией каналов;
- общегосударственная сеть телефонной связи (ОГСТФС) общего пользования;
- общегосударственная сеть телефонной связи «Искра»;
- ведомственные и коммерческие сети телефонной связи;
- сеть абонентского телеграфирования (АТ-50).

Сети передачи данных и документального обмена:

- ведомственные и коммерческие сети с коммутацией сообщений и пакетов;
- телеграфная сеть общего пользования с коммутацией сообщений.

Сети радиосвязи с подвижными и стационарными объектами:

- радиальные сети общего и ведомственного назначения;
- сотовые сети коммерческого назначения,

а также цифровые сети интегрального обслуживания.

Все указанные сети базируются на первичной государственной сети связи, реализованной на основе аналоговых и цифровых систем передачи с использованием кабельных, радиорелейных, спутниковых линий связи. Каналы различных типов первичной сети предоставляются в аренду для организации различных систем передачи информации.

В зависимости от назначения и функциональных возможностей телекоммуникационные сети предоставляют пользователям определенный спектр услуг:

- телефонная местная, междугородная, международная связь;
- передача данных (обмен сообщениями, файлами);
- телеграфная связь (абонентский телеграф, телекс);
- телефакс;
- телетекс;
- видеотекс;
- телетекст;
- электронная почта;
- телеавтограф;
- речевая почта;
- доступ к базам данных;
- интегральные услуги по передаче речи и данных;
- терминальный доступ в сеть, Интернет;
- информационно-справочный сервис сети;
- защита данных и идентификация пользователей.

Указанные услуги относятся к коммуникационным услугам общего пользования, на базе которых на прикладном уровне телекоммуникаци-

онных сетей реализуются дополнительные сервисные услуги, отражающие специфические информационные потребности отдельных групп потребителей:

- компьютерные телеконференции;
- электронный обмен деловыми документами;
- электронные доски объявлений;
- электронные банковские операции;
- электронные торговые операции (базар, рынок, торговый дом);
- электронная коммерция.

Телекоммуникационные сети, предоставляющие услуги телефонной связи, обеспечивают пользователям возможность обмена речевыми сообщениями в режимах автоматической местной, автоматической и полуавтоматической междугородной и международной связи. Абонентам предоставляется широкий набор дополнительных видов обслуживания (сокращенный набор номера, прямой вызов, переадресация, конференц-связь, избирательная связь, постановка в очередь, уведомление о вновь поступивших вызовах во время разговора, приоритетное обслуживание, определение злонамеренных вызовов и т. д.).

Телефонные сети обеспечивают возможность передачи пользователями данных и факсимильной информации через модемы по скоммутированному между ними каналу. Таким образом, ряд функций по передаче данных и документальному обмену, представляющих интерес для пользователей, может быть реализован в телефонной сети общего пользования.

Массовый приток на российский рынок зарубежных персональных компьютеров, факсов, модемов, системного и прикладного программного обеспечения создали потенциальные возможности для реализации услуг обмена данными и факсимильной информацией по коммутируемым каналам ОГСТФС. Преимуществом этого способа является практическое отсутствие ограничений на территориальное размещение абонентов в связи с развитой топологией государственной сети общего пользования. Однако спектр реализуемых таким образом функций ограничивается режимом двухточечного соединения и физическими особенностями среды передачи информации. Низкое качество большинства каналов на аналоговых телефонных сетях в ряде регионов практически не позволяет осуществить устойчивый и безошибочный обмен данными и факсимильной информацией даже в пределах одного района города. Определенное улучшение качества передачи и увеличение скорости обмена может быть

обеспечено за счет использования современных модемов, реализующих протоколы коррекции ошибок и сжатия данных.

Телеграфная сеть связи в России является второй (после ОГСТФС) по общему числу пользователей. По назначению оконечных пунктов, характеру и способу обработки информации она подразделяется на следующие сети:

- общего пользования (ОП), по которой передаются телеграммы, поступающие в городские отделения связи или районные узлы;
- абонентского телеграфирования (АТ), по которой передаются телеграфные сообщения, поступающие от предприятий, являющихся абонентами сети АТ;
- передачи данных (ПД);
- международную, абонентского телеграфирования (телекс);
- международную, общего пользования (гентекс).

### *3.3.2. Службы*

Более развитыми функциональными возможностями обладают ИС, в составе которых имеются средства сетевых служб.

Сетевая телекс-телеграфная служба предназначена для приема телексных и телеграфных сообщений, переданных абонентами со стандартных телексных или телеграфных аппаратов, определения оптимального маршрута пересылки сообщений, их передачи по сети на другую станцию, рассылки сообщений абонентам, находящимся в любом районе страны и за рубежом.

Служба обеспечивает также автоматическую регистрацию и проверку полномочий абонентов, автоматический прием номера абонентской установки для последующей пересылки. Дополнительными услугами могут являться множественная и задержанная (к определенному сроку) рассылка сообщений, шлюзы со службой электронной почты.

Служба телефакс предназначена для обеспечения высококачественного приема сообщений, переданных абонентами со стандартных факсимильных аппаратов. В сети предусматривается конвертирование факсимильных сообщений в специальный формат, определение оптимального маршрута пересылки, передача сообщения, его расконвертирование и пересылка получателю. Обеспечивается автоматическая регистрация сообщений и проверка полномочий абонента. Дополнительными услугами являются множественная и задержанная рассылка сообщений, шлюзы с системами электронной почты, архивация сообщений.

Служба телетекс обеспечивает связь между оконечными установками, которые используются для подготовки, редактирования и печати корреспонденции. За счет промежуточного накопления передаваемой информации в памяти оконечного устройства скорость последующей передачи может быть увеличена.

К службам документальной электросвязи относятся также дата-факс (служба, функционально аналогичная телефаксу, но работающая не по телефонной сети общего пользования, а по сетям с коммутацией пакетов) и бюрофакс - факсимильная служба с клиентским принципом обслуживания (с терминалом коллективного пользования).

Служба видеотекс обеспечивает прием сообщений (текстов, изображений) на экран бытового телевизора или другие видеотерминалы из информационно-вычислительных центров. Запрос на услугу формируется с тастауры телефонного аппарата и через модем в цифровой форме передается по телефонной сети в центр. Найденная по запросу в банке данных информация передается абоненту и выводится на экран. Видеотерминал может дополняться клавиатурой, принтером, факсимильным аппаратом.

В службе телетекст буквенно-цифровая информация передается на экран бытовых телевизоров по сети телевизионного вещания (дополнительно к основной программе). Информационно-вычислительный центр телетекста по запросам абонентов обеспечивает централизованную выдачу оперативной информации, хранящейся в банке данных. Для выбора информации используется тастаура телефонного аппарата. Информация телетекста вводится в телевизионный тракт во время обратного хода луча кадровой развертки. Для пользования услугами телетекста бытовой телевизор оборудуется специальной приставкой-декодером (в телевизорах 5-го поколения имеется встроенный декодер телетекста). При необходимости имеется возможность получения копии информации на принтере.

Электронная почта обеспечивает обмен сообщениями, предоставляет услуги по подготовке, обработке и хранению сообщений. Передача сообщений осуществляется через общедоступный или персональный электронный ящик. Электронное письмо может быть послано наложенным платежом, срочным, с уведомлением о доставке (недоставке), с отправкой в несколько адресов, с доставкой к определенному сроку и т. д.

Служба телеавтограф предназначена для передачи по телекоммуникационным сетям рукописной текстовой и графической информации (в общем случае - одновременно с передачей речи по одному каналу в разных полосах частотного спектра). Ввод информации осуществляется с помощью электронного пера и планшета с координатной сеткой. Координаты положения пера кодируются и передаются по сети абоненту-

получателю, где осуществляется их декодирование, формирование копии документа и вывод информации на экран (принтер).

Голосовая (речевая) электронная почта обеспечивает запись речевых сообщений в цифровом виде и передачу их получателю в соответствии с правилами, характерными для обычной электронной почты. При получении сообщение преобразуется из цифровой формы в аналоговую и в звуковой сигнал.

Доступ к базам данных осуществляется в режимах «он-лайн» и «офф-лайн». Первый режим соответствует работе пользователя с сетью в реальном масштабе времени, а второй - работе по принципу «запрос - ответ» с существенно большим временем реакции сети на запрос пользователя.

Услуга по обмену файлами предоставляет пользователям сетевой сервис, обеспечивающий передачу больших массивов структурированной информации между абонентами, а также управление файлами территориально удаленных ресурсов сети с целью просмотра и манипулирования их атрибутами.

Служба информационно-справочного сервиса обеспечивает получение пользователями сети разнообразной информации о ресурсах и функциональных возможностях данной сети.

Удовлетворение информационных потребностей абонентов ИС связано в первую очередь с обеспечением их доступа к информационным ресурсам данной сети и смежных с ней сетей. Информационными ресурсами являются централизованные и локальные базы данных, доступные пользователю непосредственно либо через сетевые службы, реализующие тематические телеконференции и поддерживающие работу электронных досок объявлений.

Компьютерные телеконференции обеспечивают общение территориально удаленных групп пользователей в определенных прикладных областях. Предоставляются услуги по формированию, поиску и получению тематически ориентированной информации.

Электронный телекоммуникационный обмен деловыми документами (служба EDIFACT) обеспечивает стандартизованный обмен данными (на базе стандартных служб электронной почты), экономическими, финансовыми и распорядительными документами. Используемые международные стандарты задают специальные структуры документов, разработанные в соответствии с требованиями документального сопровождения товарно-транспортных операций.

Электронная доска объявлений (ЭДО) обеспечивает доступ пользователей со своих оконечных установок к специально образованной постоянно действующей файловой системе. Предоставляются услуги просмотра содержимого (или оглавления) ЭДО, размещения информации на ЭДО

с указанием времени ее хранения, снятия информации в любой момент времени. Содержимое ЭДО автоматически обновляется ее абонентами и администрацией службы.

Системы электронных банковских операций предоставляют услуги по связи банков между собой, с их филиалами и клиентами, по передаче банковской информации, выполнению операций с денежными средствами, ценными бумагами, кредитными картами.

Системы электронных торговых операций (электронный базар, рынок, торговый дом) на базе электронных досок объявлений обеспечивают услуги по приему заявок на продажу (обмен) товаров, просмотру ЭДО (поиску требуемого товара), проведению взаимных расчетов между продавцом и покупателем в режиме диалога или электронной почты. Системы отличаются друг от друга структурированностью содержимого ЭДО и ассортиментом товаров.

Биржевые системы обеспечивают автоматизацию деятельности как отдельных бирж, так и проведение одновременных (синхронных) торгов на нескольких биржах.

В обобщенном виде услуги информационных систем [2] представлены в табл. 2.2.

*Таблица 2.2. Услуги информационных систем*

| *Продукция ИС* | *Вид обслуживания* | *Вид общения* |
|---|---|---|
| Диалоговая информационная связь | Телефонная связь<br>Телеграфная и факсимильная связь<br>Передача данных<br>Телеуправление | Диалог |
| Избирательная связь | Почтовые отправления<br>Передача телеграмм<br>Передача телефонограмм<br>Электронная почта<br>Передача данных<br>Вызывная связь (пейджерная) | Сообщение |
| Распространение информации | Распространение печати<br>Радиовещание<br>Радиофикация<br>Телевидение<br>Оповещение<br>(телетекс, видеотекст) | Извещение |
| Избирательная справочная связь | Телесправочная связь<br>Телесигнализация<br>Телеобслуживание | Запрос - ответ |

### 3.4. Источники конфиденциальной информации в информационных системах

Промышленный шпионаж был всегда, возможно с сотворения мира. Особенно активно он развивался в странах с рыночной экономикой. Объяснить этот факт просто: в условиях конкурентной борьбы знание сильных и слабых сторон продукции и производства обеспечивает победу на потребительском рынке.

В своих противоправных действиях, направленных на овладение чужими секретами, злоумышленники стремятся найти такие источники конфиденциальной информации, которые давали бы им наиболее достоверную информацию в максимальных объемах с минимальными затратами на ее получение. Прибегая к различным уловкам, используя множество способов и средств, подбираются пути и подходы к таким источникам. Очевидно, для этого необходимо четко определить, какой источник обладает интересующей их информацией, и подобрать соответствующие способы и средства ее добывания.

В различной зарубежной и отечественной литературе можно встретить разные толкования понятия ИСТОЧНИК. Например, каждому известно, что «книга - источник знаний» или «нефтяное месторождение - источник нефти» и др. Наиболее употребительно понятие «источник информации» в разведке. Например, «главным источником радиоразведки являются радиостанции и их радиопередачи» или «как стало известно из источников в Пентагоне...» и т. п. Очевидно, что в любой из этих формулировок имеется ввиду какой-то объект, обладающий определенной информацией, которую возможно получить (получать) одноразово или многократно интересующимся ею лицом. При этом источник может выступать как активной, так и пассивной стороной.

Источник информации - это материальный объект, обладающий определенными сведениями (информацией), представляющими конкретный интерес для злоумышленников или конкурентов.

В общем плане, без значительной детализации можно считать источниками конфиденциальной информации следующие категории.

1. Людей (сотрудники, обслуживающий персонал, продавцы, клиенты и др.).
2. Документы самого различного характера и назначения.
3. Публикации: доклады, статьи, интервью, проспекты, книги и т. д.
4. Технические носители информации и документов.
5. Технические средства обработки информации: автоматизированные средства обработки информации и средства обеспечения производственной и трудовой деятельности, в том числе и средства связи.

6. Выпускаемую продукцию.
7. Производственные и промышленные отходы.

**Люди** в ряду источников конфиденциальной информации занимают особое место, как активные элементы, способные выступать не только обладателями конфиденциальной информации, но и субъектами злонамеренных действий. Люди являются и обладателями и распространителями информации в рамках своих функциональных обязанностей. Кроме того что люди обладают важной информацией, они еще способны ее анализировать, обобщать, делать соответствующие выводы, а также при определенных условиях скрывать, воровать, продавать и совершать иные криминальные действия, вплоть до вступления в преступные связи с злоумышленниками.

Необходимо особо отметить, что изо всей совокупности источников персонал, сотрудники, продавцы продукции, партнеры, поставщики, клиенты и т. д. - главные источники конфиденциальной информации. Поэтому необходимо тщательно изучать весь состав сотрудников, особо выделяя при этом основных, обладающих особо ценной коммерческой информацией. Следует обращать внимание как на вновь поступивших на работу, так и на тех, кто подлежит увольнению. Эти люди нередко находятся в ситуациях, благоприятных к злонамеренным действиям, особенно последние. Объект особой заботы - персонал, занимающийся сбытом продукции. Часто эти люди получают запросы от клиентов с просьбой сообщить какие-либо сведения о возможной продаже улучшенных или новых моделей, дополнительную информацию об изделии якобы для того, чтобы его лучшим образом применить.

Опытный промышленный шпион сам не стремится проникнуть на фирму, а подбирает из числа служащих подходящую «жертву». Кроме того, он знает, что самые лучшие источники не «жертвы», а болтуны. Вот почему профессионалов промышленного шпионажа привлекают различные съезды, конгрессы, конференции, симпозиумы, научные семинары и другие формы общественного обсуждения научных и практических проблем. В докладах и выступлениях участников зачастую сообщаются такие сведения, которые не найдешь ни в каких документах, в том числе и в публикуемых. Здесь опытный специалист собирает самую ценную информацию.

Формой информационного обмена выступают также различные интервью, выступления на радио и телевидении.

**Документы.** Документы - это самая распространенная форма обмена информацией, ее накопления и хранения. Под документом понимают ма-

термальный носитель информации (бумага, кино- и фотопленка, магнитная лента и т. п.) с зафиксированной на нем информацией, предназначенной для ее использования во времени и пространстве. Документ отличает то, что его функциональное назначение весьма разнообразно. Он может быть представлен не только различным содержанием, но и разными физическими формами - материальными носителями.

По направленности различают организационно-распорядительные, плановые, статистические, бухгалтерские и научно-технические документы, содержащие, по существу, всю массу сведений о составе, состоянии и деятельности любой организационной структуры от государственного до индивидуального уровня, о любом изделии, товаре, замысле, разработке.

Определенную опасность представляют судебные документы, связанные с разбором различных конфликтных ситуаций. Подчас в ходе судебного разбирательства раскрываются весьма тонкие нюансы деятельности фирмы, которые в других ситуациях просто не появились бы ни в документах, ни в действиях. Такое разнообразие форм и содержания документов по назначению, направленности, характеру движения и использованию является весьма заманчивым источником конфиденциальной информации для промышленных шпионов, что, естественно, привлекает их внимание реальными возможностями получения интересующих их сведений.

**Публикации.** Публикации - это информационные носители в виде самых разнообразных изданий, подразделяющихся на первичные и вторичные. К первичным относятся книги, статьи, периодические и продолжающиеся издания, сборники, научно-технические отчеты, диссертации, рекламные проспекты, доклады, препринты и др. Ко вторичным - информационные карты, реферативные журналы, экспресс-информация, обзоры, библиографические указатели, каталоги и др.

По заключению западных специалистов, более 60 % военной информации, являющейся весьма секретной, можно получить из так называемых открытых или легальных источников - прессы, передач радио и телевидения, книг, журналов и т. д. Поэтому современный разведчик, под какой бы «крышей» он ни работал (дипломат, торговый представитель, журналист), занимается в основном сбором и анализом сведений из официальных источников информации.

Что же касается научной, промышленной и экономической информации, то она не в меньшей мере доступна злоумышленникам. Порядка 90 % интересующей их информации можно получить из специализированных журналов, научных трудов, отчетов, внутренних изданий пред-

приятии, брошюр и проспектов, раздаваемых на выставках и ярмарках. Цель шпиона - раздобыть остальные 10% необходимой ему информации, в которой и кроется фирменный секрет, «тайна мастерства».

**Технические носители.** Информация может быть фиксированной и нефиксированной. Фиксированная информация - это сведения, закрепленные на каком-либо физическом носителе, а нефиксированная - это знания, которыми владеют ученые, специалисты, работники (владельцы или источники), так или иначе участвующие в производстве и способные передавать эти знания другим. Фиксированная информация различается в зависимости от вида носителя, на котором она находится. К техническим носителям информации относятся бумажные носители, кино- и фотоматериалы (микро- и кинофильмы), магнитные носители (дискеты, жесткие диски, стримеры), видеозаписи, информация на экранах ПЭВМ, на табло коллективного пользования, на экранах промышленных телевизионных установок и других средствах.

Опасность технических носителей определяется высоким темпом роста парка технических средств, компьютерных сетей и ПЭВМ, находящихся в эксплуатации, их широким применением в самых различных сферах человеческой деятельности, высокой степенью концентрации информации на технических носителях и масштабностью участия людей в использовании этих носителей в практической деятельности. В качестве демонстрации высокой концентрации информации на гибком магнитном диске (дискете) ПЭВМ емкостью 1,44 Мбайт укажем, что на нем можно записать около 150 тыс. знаков или примерно 1000 страниц текста. Еще большей емкостью обладают жесткие диски, CD- и DVD-диски. Такой источник информации может один содержать практически всю информацию о фирме или предприятии.

**Технические средства обработки информации.** Технические средства как источники конфиденциальной информации являются достаточно широкой и емкой в информационном плане группой источников. По специфике назначения и исполнения их можно разделить на две большие группы:

- технические средства обеспечения производственной и трудовой деятельности;
- технические средства автоматизированной обработки информации.

В группу средств обеспечения производственной и трудовой деятельности входят самые различные технические средства, такие, например, как телефонные аппараты и телефонная связь; телеграфная, фототе-

леграфная и факсимильная связь; системы радиосвязи (автономные, территориальные, релейные, спутниковые и др.); телевизионные (в том числе и средства промышленного телевидения); радиоприемники и радиотрансляционные системы; системы громкоговорящей связи, усилительные системы различного назначения; средства магнитной и видеозаписи; средства неполиграфического размножения документов (пишущие машинки, ксерокопировальные аппараты, факсы) и другие средства и системы. Все эти средства могут являться источниками преобразования акустических сигналов, содержащих коммерческие секреты, в электрические и электромагнитные поля, способные образовать электромагнитные каналы утечки охраняемых сведений.

Особую группу технических средств составляют автоматизированные системы обработки информации. Привлекательность ПЭВМ и информационных систем как источников конфиденциальной информации обусловлена рядом объективных особенностей, к числу которых относятся:

- резкое расширение сферы применения информационной и вычислительной техники (ПЭВМ, локальные и распределенные информационные сети национального и международного масштаба);
- увеличение объемов обрабатываемой и хранимой информации в локальных и распределенных банках данных;
- увеличение числа пользователей ресурсами ПЭВМ и сетей: многопользовательский режим удаленного доступа к базам данных.

Привлекательность заключается еще и в том, что АСОИ содержит весьма значительный ассортимент информации. В ее базах данных есть все о конкретном предприятии от досье на сотрудников до конкретной продукции, ее характеристиках, стоимости и другие сведения.

**Продукция.** Производство материальных благ является естественной деятельностью человечества в целях улучшения своей жизни и обеспечения других видов деятельности. И вполне естественно, что продукты труда выступают источниками информации, за которой весьма активно охотятся конкуренты. Особое внимание обращают конкуренты на новую продукцию, находящуюся в стадии подготовки к производству. Производство любой продукции определяется этапами «жизненного цикла»: идеей, макетом, опытным образцом, испытаниями, серийным производством, эксплуатацией, модернизацией и снятием с производства. Каждый из этих этапов сопровождается специфической информацией, проявляющейся разными физическими эффектами, которые в виде характеристик (демаскирующих признаков) могут раскрыть охраняемые сведения о производимом товаре.

Естественно, что злоумышленник стремится получить информацию о производимом товаре на более ранних стадиях его «жизненного цикла», что даст ему возможность своевременно принять необходимые меры для упреждения в выпуске своей продукции. При этом, очевидно, его продукция должна обладать привлекательными для потребителя параметрами: быть дешевле, надежнее, производительнее, оригинальнее, красивее и т. д. Ведь недаром же говорят об умении японцев подхватывать и запускать в массовое производство то, что изобретено в других странах.

**Промышленные и производственные отходы.** Отходы производства, что называется бросовый материал, могут многое рассказать об используемых материалах, их составе, особенностях производства, технологии. Тем более что они получаются почти безопасным путем на свалках, помойках, местах сбора металлолома, в ящиках отходов исследовательских лабораторий, в мусорных корзинах кабинетов. Как откровенничал один из опытных шпионов, «рекомендую обращать внимание на содержание мусорных корзин: стоит недорого, а среди смятых бумажек, испорченных документов и разных копирок, если искать, можно найти тысячедолларовый банкнот; я не раз их находил в виде черновиков, за которые мне платили тысячи». Не менее серьезными источниками конфиденциальной информации являются промышленные отходы: опилки, стружка, обрезки, испорченные заготовки, поломанные комплектующие и т. д. Анализ отходов поможет узнать об особенностях производства, технологии.

Каждый в отдельности, а в итоге в совокупности источники конфиденциальной информации содержат достаточно полные сведения о составе, состоянии и направлениях деятельности предприятия, что весьма интересует конкурентов. Ведь заманчиво знать, когда конкурент начнет разработку нового изделия, чем оно будет лучше старого, когда он выбросит новый товар на рынок, по какой цене и т. д. Зная это, можно успешно конкурировать с ним, приняв своевременные меры.

Источниками конфиденциальной информации в информационных системах являются люди, документы, публикации, технические носители, технические средства обработки информации, продукция, промышленные и производственные отходы.

## 3.5. Что приводит к неправомерному овладению конфиденциальной информацией в информационных системах

Другое толкование. «Одной из проблем защиты информации является классификация возможных каналов утечки информации. Под возможным каналом утечки информации мы будем понимать способ, позволяю-

щий нарушителю получить доступ к обрабатываемой или хранящейся в ПЭВМ информации». И далее: «К каналам утечки относятся:

- хищение носителей информации (магнитных лент, дисков, дискет и т. д.);
- чтение информации с экрана посторонним лицом (во время отображения информации на экране законным пользователем или при отсутствии его);
- чтение информации из оставленных без присмотра распечаток программ;
- подключение к устройствам ПЭВМ специально разработанных аппаратных средств, обеспечивающих доступ к информации;
- использование специальных технических средств для перехвата электромагнитных излучений технических средств ПЭВМ;
- несанкционированный доступ программ к информации;
- расшифровка программой зашифрованной информации;
- копирование программой информации с носителей» [24].

Довольно часто встречаются такие определения, как «промышленные шпионы... подслушивают, ведут наблюдение, досматривают почту...», «экономический шпионаж как сфера тайной деятельности по сбору, анализу, хранению и использованию... конфиденциальной информации», «выуживание информации, от примитивного прослушивания до космического подглядывания», «космический шпионаж не отменяет тысячелетиями опробованные способы выуживания секретов», «спецслужбы рассматривают, прощупывают прослушивают, зондируют земной шарик всевозможными способами начиная от простого изучения прессы и кончая сканированием земной толщи лазерными лучами из космоса».

Один из возможных перечней способов получения информации приведен ниже.

1. Сбор информации, содержащейся в СМИ, включая официальные документы, например судебные отчеты.
2. Использование сведений, распространяемых служащими конкурирующих фирм.
3. Биржевые отчеты и отчеты консультантов, финансовые отчеты и документы, находящиеся в распоряжении маклеров; выставочные экспонаты и проспекты, брошюры конкурирующих фирм; отчеты коммивояжеров своей фирмы.

4. Изучение продукции конкурирующих фирм; использование данных, полученных во время бесед со служащими конкурирующих фирм (без нарушения законов).
5. Замаскированные опросы и «выуживание» информации у служащих конкурирующих фирм на научно-технических конгрессах (конференциях).
6. Непосредственное наблюдение, осуществляемое скрытно.
7. Беседы о найме на работу со служащими конкурирующих фирм (хотя опрашивающий вовсе не намерен принимать данного человека на работу в свою фирму).
8. Так называемые ложные переговоры с фирмой-конкурентом относительно приобретения лицензии.
9. Наем на работу служащего конкурирующей фирмы для получения требуемой информации.
10. Подкуп служащего конкурирующей фирмы или лица, занимающегося ее снабжением.
11. Использование агента для получения информации на основе платежной ведомости фирмы-конкурента.
12. Подслушивание переговоров, ведущихся в фирмах-конкурентах.
13. Перехват телеграфных сообщений.
14. Подслушивание телефонных переговоров.
15. Кражи чертежей, образцов, документов и т. д.
16. Шпионаж и вымогательство.

Возникает закономерный вопрос, что из приведенных понятий можно рассматривать как способ несанкционированного доступа. Под способом вообще понимается порядок и приемы действий, приводящие к достижению какой-либо цели. Энциклопедическое понимание способа производства - исторически обусловленная форма производства материальных благ. Известно также определение способов военных действий как порядок и приемы применения сил и средств для решения задач в операции (бою). Наконец, способ доступа -совокупность приемов работы с данными во внешней памяти. В криминальной сфере отмечаются способы сокрытия доходов от налогообложения.

С учетом рассмотренного можно так определить способ несанкционированного доступа к источникам конфиденциальной информации: способ несанкционированного доступа - совокупность приемов и порядок

действий с целью получения (добывания) охраняемых сведений незаконным, противоправным путем.

С учетом этой формулировки рассмотрим на самом высоком уровне абстракции систематизированный перечень таких способов (табл. 2.3).

*Таблица 2.3. Обобщенная модель способов несанкционированного доступа к источникам конфиденциальной информации*

| *Источники информации* | *Способы доступа к информации* | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | *Инициативное сотрудничество* | *Склонение к сотрудничеству* | *Выпытывание* | *Подслушивание* | *Наблюдение* | *Хищение* | *Копирование* | *Подделка (модификация)* | *Уничтожение (порча, разрушение)* | *Незаконное подключение* | *Перехват* | *Негласное ознакомление* | *Фотографирование* | *Сбор и аналитическая обработка* | *Итого по источнику* |
| Люди | + | + | + | + | + | + | | + | + | | + | + | + | + | 10 |
| Документы | | | | | + | + | + | + | + | | + | + | + | + | 9 |
| Публикации | | | | | + | | | + | | | | + | | + | 3 |
| Технические носители | | | | | | + | + | + | + | | | | | + | 5 |
| Технические средства | | | | + | + | | | | + | + | + | | | + | 4 |
| Технические средства АСОИ | | | | + | + | + | + | + | + | + | + | + | + | | 10 |
| Продукция | | | | | + | + | + | + | + | | | + | + | | 7 |
| Отходы | | | | | + | + | | | | | | + | | + | 2 |
| *Всего* | 1 | 1 | 1 | 3 | 4 | 6 | 4 | 6 | 6 | 2 | 3 | 5 | 4 | 4 | 50 |

Способами несанкционированного доступа к конфиденциальной информации являются:

1. Инициативное сотрудничество.
2. Склонение к сотрудничеству.
3. Выведывание, выпытывание.
4. Подслушивание переговоров различными путями.
5. Хищение.
6. Копирование.
7. Подделка (модификация).
8. Уничтожение (порча, разрушение).
9. Незаконное подключение к каналам и линиям связи и передачи данных.
10. Негласное ознакомление со сведениями и документами.
11. Перехват.
12. Визуальное наблюдение.
13. Фотографирование.
14. Сбор и аналитическая обработка.

Развернутое содержание способов несанкционированного доступа приведено в [22, 31].

Этот перечень является независимым и непересекающимся на выбранном уровне абстракции. Согласившись с тем, что перечень источников конфиденциальной информации также независим и непересекаем, рассмотрим их взаимосвязи и взаимозависимости.

Даже беглый обзор позволяет заключить, что к определенным источникам применены и определенные способы. Как разнообразны источники, так и разнообразны способы несанкционированного доступа к ним. Мы допускаем возможность декомпозиции и способов несанкционированного доступа (НСД) и источников по их применимости в зависимости от определенных условий и ситуаций. Тем не менее, имея формальный набор источников и способов НСД к ним, возможно построить формальную модель взаимосвязи источников и способов на качественном уровне с определенной степенью условности. Такую модель можно было бы назвать обобщенной моделью способов несанкционированного доступа к источникам конфиденциальной информации. Вариант такой модели приведен в табл. 2.3. Что же показывает эта модель?

Не вдаваясь в сущность каждого способа, видно, что значительная их часть применима к таким источникам, как люди, технические средства

АСОИ и документы. Другие, как бы менее применяемые по количеству охватываемых источников, никак нельзя отнести к менее опасным. Степень опасности проникновения определяется не количеством, а принесенным ущербом.

Многообразие способов несанкционированного доступа к источникам конфиденциальной информации вызывает вопрос, каково их соотношение в практике деятельности спецслужб (рис. 2.9).


Рис. 2.9. Действия, приводящие к овладению информацией

На рис. 2.9 представлены действия, приводящие к НСД. Зарубежные литературные источники приводят отдельные показатели соотношения способов НСД, приведенные в табл. 2.4; полной картины пока нет.

*Таблица 2.4. Соотношение способов НСД*

| *Способ НДС* | *%* |
|---|---|
| Подкуп, шантаж, переманивание служащих, внедрение агентов | 43 |
| Подслушивание телефонных переговоров | 5 |
| Кража документов | 10 |
| Проникновение в ПЭВМ | 18 |
| Съем информации с каналов связи «втемную» | 24 |

Анализ приведенных данных показывает, что последние три группы реализуются в криминальной практике посредством использования тех или иных технических средств и составляют в общем составе 47 % от общего их числа. Это лишний раз подтверждает опасность технических каналов утечки информации в практике ведения предпринимательской деятельности.

### 3.6. Виды технических средств информационных систем

В процессе функционирования информационной системы происходит то или иное преобразование, вызванное необходимостью обеспечения управленческих решений.

Виды работ, которые можно выполнять с информацией, следующие:

- преобразование информации (изменение физического сигнала, формы представления, кода, языка, но без изменения содержания);
- перемещение информации в пространстве (передача);
- перемещение информации во времени (фиксация информации, запоминание с выдачей по запросу);
- обработка информации;
- размножение информации и др.

Выполнение названных работ обеспечивают специальные, ориентированные на эти работы средства, которые принято называть основными. Помимо основных технических средств, в процессе управления производством и трудовой деятельности используются различные технические средства вспомогательного, обеспечивающего назначения [32].

К ним относятся вспомогательные системы и аппараты, такие, как радиофикация, системы единого времени, магнитофоны и др. (табл. 2.5-2.6).

*Таблица 2.5. Технические средства обеспечения производственной деятельности*

| *Основные* | *Вспомогательные* |
|---|---|
| Средства передачи, обработки, накопления и хранения конфиденциальной информации | Средства обеспечения производственной и трудовой деятельности |
| Средства проводной и радиосвязи:<br>• телефонной,<br>• телеграфной,<br>• конференц-связи.<br>Средства вычислительной техники и передачи данных.<br>Звукоусилительные системы и аппаратура громкоговорящей связи.<br>Системы промышленного телевидения.<br>Средства изготовления, копирования и размножения документов.<br>Испытательная и измерительная техника:<br>• радиотелеметрические системы;<br>• измерительные комплекты;<br>• отдельные измерительные приборы | Системы радиофикации.<br>Системы единого времени.<br>Звукозаписывающая аппаратура.<br>Бытовая радиоприемная аппаратура.<br>Телевизионные системы.<br>Бытовые электроприборы:<br>• электрические часы,<br>• электрические звонки,<br>• настольные и потолочные светильники,<br>• холодильники,<br>• кондиционеры,<br>• вентиляторы.<br>Средства охранно-пожарной сигнализации |

*Таблица 2.6. Взаимосвязь способов НСД и каналов утечки информации*

| *Способы несанкционированного доступа* | *Типы технических каналов утечки информации* | | | |
|---|---|---|---|---|
| | *Визуально-оптические* | *Акустические* | *Электромагнитные (магнитные, электрические)* | *Материально-вещественные* |
| Подслушивание | | + | + | |
| Визуальное наблюдение | + | | | |
| Хищение | | | + | + |
| Копирование | | | + | + |
| Подделка | | | + | + |
| Незаконное подключение | | + | + | |
| Перехват | | + | + | |
| Фотографирование | + | | | |
| *Всего* | 2 | 3 | 6 | 3 |

Показательно, что наиболее опасными являются электромагнитные каналы утечки информации, охватываемые шестью способами НСД. Бо-

лее того, в обиход уверенно вошло такое понятие, как «магнитный терроризм» - воздействие на этот объект электромагнитным полем.

Любая ИС может оперативно и в полном объеме удовлетворять информационные потребности пользователей имея современные технические средства. Чем больше средств, тем успешнее работает ИС. Однако любые технические средства потенциально обладают техническими каналами утечки информации по своей природе. Это расширяет возможности не только в плане использования этих средств, но и в плане несанкционированного съема информации.

Если не уверен в безопасности, считай,
что опасность существует реально.
*Правило морского судоходства*

## 4. Угрозы информации

Угроза информации - возможность возникновения на каком-либо этапе жизнедеятельности системы такого явления или события, следствием которого могут быть нежелательные воздействия на информацию.

1. Виды угроз. Основные нарушения.
1.1. Физической целостности (уничтожение, разрушение элементов).
1.2. Логической целостности (разрушение логических связей).
1.3. Содержания (изменение блоков информации, внешнее навязывание ложной информации).
1.4. Конфиденциальности (разрушение защиты, уменьшение степени защищенности информации).
1.5. Прав собственности на информацию (несанкционированное копирование, использование).

2. Характер происхождения угроз.
2.1. Умышленные факторы:
2.1.1. Хищение носителей информации.
2.1.2. Подключение к каналам связи.
2.1.3. Перехват электромагнитных излучений (ЭМИ).
2.1.4. Несанкционированный доступ.
2.1.5. Разглашение информации.
2.1.6. Копирование данных.
2.2. Естественные факторы:
2.2.1. Несчастные случаи (пожары, аварии, взрывы).
2.2.2. Стихийные бедствия (ураганы, наводнения, землетрясения).
2.2.3. Ошибки в процессе обработки информации (ошибки пользователя, оператора, сбои аппаратуры).

Три наиболее выраженные угрозы:

- подверженность физическому искажению или уничтожению;
- возможность несанкционированной (случайной или злоумышленной) модификации;
- опасность несанкционированного (случайного и преднамеренного) получения информации лицами, для которых она не предназначена.

Источники угроз (понимается непосредственный исполнитель угрозы в плане ее негативного воздействия на информацию):

- люди;
- технические устройства;
- модели, алгоритмы, программы;
- технологические схемы обработки;
- внешняя среда.

Предпосылки появления угроз:

- объективные (количественная или качественная недостаточность элементов системы) - причины, не связанные непосредственно с деятельностью людей и вызывающие случайные по характеру происхождения угрозы;
- субъективные - причины, непосредственно связанные с деятельностью человека и вызывающие как преднамеренные (деятельность разведок иностранных государств, промышленный шпионаж, деятельность уголовных элементов и недобросовестных сотрудников), так и непреднамеренные (плохое психофизиологическое состояние, недостаточная подготовка, низкий уровень знаний) угрозы информации.

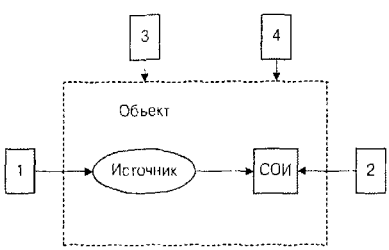



Рис. 2.10. Каналы НСД к информации

Несанкционированный доступ - получение лицами в обход системы защиты с помощью программных, технических и других средств, а также в силу случайных обстоятельств доступа к обрабатываемой и хранимой на объекте информации. На рис. 2.10 приведен общий вид каналов НСД к источнику информации и системе обработки информации (СОИ).

*Разглашение информации* ее обладателем есть умышленное или неосторожное действие должностных лиц и граждан, которым соответствующие сведения в установленном порядке были доверены по работе, приведшие к не вызванному служебной необходимостью оглашению охраняемых сведений, в также передача таких сведений по открытым техническим каналам или обработка на некатегорированных ЭВМ.

*Утечку информации* в общем плане можно рассматривать как бесконтрольный и неправомерный выход конфиденциальной информации за пределы организации или круга лиц, которым эта информация была доверена.

*Система защиты информации* - совокупность взаимосвязанных средств, методов и мероприятий, направленных на предотвращение уничтожения, искажения, несанкционированного получения конфиденциальных сведений, отображенных полями, электромагнитными, световыми и звуковыми волнами или вещественно-материальными носителями в виде сигналов, образов, символов, технических решений и процессов.

Система защиты информации является составной частью комплексной системы безопасности. На рис. 2.11 представлена трехмерная модель комплексной безопасности.

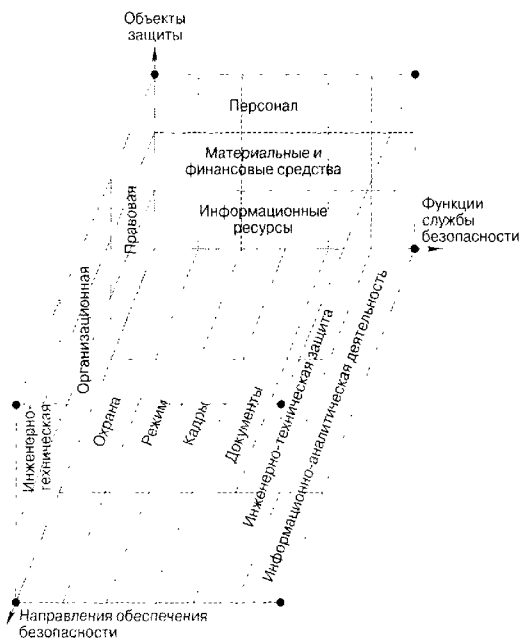



Рис. 2.11. Трехмерная модель комплексной безопасности

## 4.1. Классы каналов несанкционированного получения информации

Рассмотрим относительно полное множество каналов несанкционированного получения информации, сформированного на основе такого показателя, как степень взаимодействия злоумышленника с элементами объекта обработки информации и самой информацией.

К *первому классу* относятся каналы от источника информации при НСД к нему.

1. Хищение носителей информации.
2. Копирование информации с носителей (материально-вещественных, магнитных и т. д.).
3. Подслушивание разговоров (в том числе аудиозапись).
4. Установка закладных устройств в помещение и съем информации с их помощью.
5. Выведывание информации обслуживающего персонала на объекте.
6. Фотографирование или видеосъемка носителей информации внутри помещения.

Ко *второму классу* относятся каналы со средств обработки информации при НСД к ним.

1. Снятие информации с устройств электронной памяти.
2. Установка закладных устройств в СОИ.
3. Ввод программных продуктов, позволяющих злоумышленнику получать информацию.
4. Копирование информации с технических устройств отображения (фотографирование с мониторов и др.).

К *третьему классу* относятся каналы от источника информации без

1. Получение информации по акустическим каналам (в системах вентиляции, теплоснабжения, а также с помощью направленных микрофонов).
2. Получение информации по виброакустическим каналам (с использованием акустических датчиков, лазерных устройств).
3. Использование технических средств оптической разведки (биноклей, подзорных труб и т. д.).
4. Использование технических средств оптико-электронной разведки (внешних телекамер, приборов ночного видения и т. д.).

5. Осмотр отходов и мусора.
6. Выведывание информации у обслуживающего персонала за пределами объекта.
7. Изучение выходящей за пределы объекта открытой информации (публикаций, рекламных проспектов и т. д.).

К *четвертому классу* относятся каналы со средств обработки информации без НСД к ним.

1. Электромагнитные излучения СОИ (паразитные электромагнитные излучения (ПЭМИ), паразитная генерация усилительных каскадов, паразитная модуляция высокочастотных генераторов низкочастотным сигналом, содержащим конфиденциальную информацию).
2. Электромагнитные излучения линий связи.
3. Подключения к линиям связи.
4. Снятие наводок электрических сигналов с линий связи.
5. Снятие наводок с системы питания.
6. Снятие наводок с системы заземления.
7. Снятие наводок с системы теплоснабжения.
8. Использование высокочастотного навязывания.
9. Снятие с линий, выходящих за пределы объекта, сигналов, образованных на технических средствах за счет акустоэлектрических преобразований.
10. Снятие излучений оптоволоконных линий связи.
11. Подключение к базам данных и ПЭВМ по компьютерным сетям.

## 4.2. Причины нарушения целостности информации

1. Субъективные.

1.1. Преднамеренные.

1.1.1. Диверсия (организация пожаров, взрывов, повреждений электропитания и др.).

1.1.2. Непосредственные действия над носителем (хищение, подмена носителей, уничтожение информации).

1.1.3. Информационное воздействие (электромагнитное облучение, ввод в компьютерные системы разрушающих программных средств, воздействие на психику личности психотропным оружием).

1.2. Непреднамеренные.

1.2.1. Отказы обслуживающего персонала (гибель, длительный выход из строя).

1.2.2. Сбои людей (временный выход из строя).

1.2.3. Ошибки людей.

2. Объективные, непреднамеренные.

2.1. Отказы (полный выход из строя) аппаратуры, программ, систем питания и жизнеобеспечения.

2.2. Сбои (кратковременный выход из строя) аппаратуры, программ, систем питания и жизнеобеспечения.

2.3. Стихийные бедствия (наводнения, землетрясения, ураганы).

2.4. Несчастные случаи (пожары, взрывы, аварии).

2.5. Электромагнитная несовместимость.

## 4.3. Виды угроз информационным системам

Угрозы информационной системе можно рассматривать с позиций их воздействия на ее характеристики, такие, в частности, как готовность системы, ее надежность и конфиденциальность [34].

Готовность - способность ИС обеспечить законным пользователям условия доступа к ресурсам в соответствии с принятым режимом работы.

Надежность - способность системы обеспечивать информационные потребности только законным пользователям в рамках их интересов.

Конфиденциальность - способность системы обеспечивать целостность и сохранность информации ее законных пользователей.

Угрозы могут также классифицироваться и по природе возникновения - стихийные бедствия, несчастные случаи (чрезвычайные происшествия), различного рода ошибки или злоупотребления, сбои и отказы оборудования и др.

Кроме того, угрозы могут быть классифицированы по ориентации на угрозы персоналу, материальным и финансовым ресурсам и информации, как составным элементам информационной системы.

Неоднократно предпринимались попытки описать различные виды угроз и воздействий на информационные системы, дать характеристику степени опасности каждой из них. Однако большинство таких попыток сводилось к описанию угроз на достаточно высоком уровне абстракции, так как описать угрозы на конкретном, деятельном уровне просто не представляется возможным.

На стадии концептуальной проработки вопросов безопасности информационной системы представляется возможным рассмотрение общего состава потенциальных угроз. Конкретные перечни, связанные со спецификой и информационной системы, и условий требуют определенной детализации и характерны для этапа разработки конкретного проекта системы безопасности ИС.

В общем плане к угрозам безопасности относятся:

- похищения и угрозы похищения сотрудников, персонала, членов их семей и близких родственников;
- убийства, сопровождаемые насилием, издевательствами и пытками;
- психологический террор, угрозы, запугивание, шантаж, вымогательство;
- грабежи с целью завладения денежными средствами, ценностями и документами.

Преступные посягательства в отношении помещений (в том числе и жилых), зданий и персонала проявляются в виде:

- взрывов;
- обстрелов из огнестрельного оружия, сигнальных ракетниц, ручных гранатометов;
- минирования, в том числе с применением дистанционного управления;
- поджогов, бросков канистр и иных емкостей с легковоспламеняющейся жидкостью;
- нападения, вторжения, захваты, пикетирования, блокирования;
- актов вандализма, повреждения входных дверей, решеток, ограждений, витрин, мебели, а также транспортных средств, личных и служебных.

Цель подобных акций:

- откровенный террор в отношении коммерческого предприятия;
- нанесение серьезного морального и материального ущерба;
- срыв на длительное время нормального функционирования предприятия;
- вымогательство значительных сумм денег или каких-либо льгот (кредиты, отсрочка платежей и т. п.) перед лицом террористической угрозы [28].

Угрозы информационным ресурсам проявляются в овладении конфиденциальной информацией, ее модификации в интересах злоумышленника или ее разрушении с целью нанесения материального ущерба.

Осуществление угроз информационным ресурсам может быть произведено:

- через имеющиеся агентурные источники в органах государственного управления, коммерческих структур, имеющих возможность получения конфиденциальной информации;

- путем подкупа лиц, непосредственно работающих на предприятии или в структурах, непосредственно связанных с его деятельностью;
- путем перехвата информации, циркулирующей в средствах и системах связи и вычислительной техники, с помощью технических средств разведки и съема информации, несанкционированного доступа к информации и преднамеренных программно-математических воздействий на нее в процессе обработки и хранения;
- путем подслушивания конфиденциальных переговоров, ведущихся в служебных помещениях, служебном и личном автотранспорте, на квартирах и дачах;
- через переговорные процессы с иностранными или отечественными фирмами, используя неосторожное обращение с информацией;
- через «инициативников» из числа сотрудников, которые хотят заработать деньги и улучшить свое благосостояние или проявляют инициативу по другим моральным или материальным причинам.

К факторам, приводящим к информационным потерям и, как следствие, к различным видам убытков или ущерба, можно отнести следующие причины и действия.

1. *Материальный ущерб,* связанный с несчастными случаями, вызывает частичный или полный вывод из строя оборудования или информационного ресурса. Причинами этого могут быть:

- пожары, взрывы, аварии;
- удары, столкновения, падения;
- воздействия твердых, газообразных, жидких или смешанных химических или физических сред;
- поломка элементов машин различного характера: механического, электрического, электронного и электромагнитного;
- последствия природных явлений (наводнения, бури, молнии, град, оползни, землетрясения и т. д.).

2. *Кражу и преднамеренную порчу материальных средств.* Воруют главным образом небольшие по габаритам аппаратные средства (мониторы, клавиатуру, принтеры, модемы, кабели и оргтехнику), информационные носители (диски, дискеты, ленты, магнитные карты и др.) и различное другое имущество и ЗИП (документация, комплектующие и др.).

Посягательства и вредительские действия проявляются в самых различных формах: явные (например, оставленная отвертка внутри печа-

тающего устройства, в корпусе вентилятора процессора) или скрытые (например, вредные химические вещества в помещениях и аппаратуре).

3. *Аварии и выход из строя аппаратуры, программ и баз данных.* Остановка или нарушение деятельности информационных центров не такие уж редкие события, а продолжительность этих состояний в основном небольшая. Но иногда между тем прямые и косвенные последствия этих действий могут быть весьма значительными. Последствия этих действий к тому же не могут быть заранее предусмотрены и оценены.

4. *Убытки, связанные с ошибками накопления, хранения, передачи и использования информации.* Эти ошибки связаны с человеческим фактором, будь-то при использовании традиционных носителей информации (дискеты, ленты) или при диалоговом обмене в режиме удаленного доступа.

При традиционных носителях цена обычной ошибки, даже после уточнения, может достигнуть 0,5 %. Формальный и информационный контроль позволяют уменьшить величину ущерба, но тем не менее число таких ошибок не уменьшается. Их последствия редко бывают весьма значительными, однако представляют собой достаточно постоянный поток и приносят постоянные потери, обусловленные поиском, устранением и последующим повторением действий, а это невосполнимые потери времени и денег.

При диалоговом режиме дополнительно прибавляются ошибки восприятия, чтения, интерпретации содержания и соблюдения правил.

Ошибки передачи зависят от используемой техники. Они могут быть простыми при использовании средств почтовой связи и чисто техническими (телепередача). В обоих случаях могут быть потери, ошибки неумения, оплошности, наличие помех, сбои и искажения отдельных букв или сообщений. Ошибки подобного рода оцениваются как потери предприятия. И хотя их трудно определить и оценить, но учитывать необходимо. Не следует недооценивать эту категорию угроз, хотя к ним довольно быстро привыкают.

5. *Ошибки эксплуатации.* Эти ошибки могут приобретать различные формы: нарушение защиты, переполнение файлов, ошибки языка управления данными, ошибки при подготовке и вводе информации, ошибки операционной системы, ошибки программы, аппаратные ошибки, ошибочное толкование инструкций, пропуск операций и т. д.

Диапазон ошибок людей значителен. Иногда трудно установить различие между ошибкой, небрежностью, утомлением, непрофессионализмом и злоупотреблением.

6. *Концептуальные ошибки и ошибки внедрения.* Концептуальные ошибки могут иметь драматические последствия в процессе эксплуатации информационной системы.

Ошибки реализации бывают в основном менее опасными и достаточно легко устранимыми.

7. *Убытки от злонамеренных действий в нематериальной сфере.* Мошенничество и хищение информационных ресурсов - это одна из форм преступности, которая в настоящее время является довольно безопасной и может принести больший доход, чем прямое ограбление банка. Между тем, учитывая сложность информационных систем и их слабые стороны, этот вид действий считается достаточно легко реализуемым.

Нередко все начинается случайно, часто с небольшого правонарушения: обмана, воровства, только для того чтобы установить, что это не слишком трудное дело и в больших масштабах. Единственным препятствием остается только совесть. Мошенничество часто имеет внутренние побудительные мотивы или совершается в корыстных целях, по договоренности с третьими лицами (сотрудничество).

8. *Болтливость и разглашение.* Эти действия, последствия которых не поддаются учету, относятся к числу трудноконтролируемых и могут находиться в рамках от простого, наивного хвастовства до промышленного шпионажа в коммерческой деятельности - таков их диапазон.

9. *Убытки социального характера.* Речь идет об уходе или увольнении сотрудников, забастовках и других действиях персонала, приводящих к производственным потерям и неукомплектованности рабочих мест. Опасность этих действий существует почти всегда.

Особо опасный вид угроз представляет промышленный шпионаж как форма недобросовестной конкуренции.

*Промышленный шпионаж* - это наносящие владельцу коммерческой тайны ущерб незаконный сбор, присвоение и передача сведений, составляющих коммерческую тайну, а также ее носителей лицом, не уполномоченным на это ее владельцем.

## 4.4. Виды потерь

Информационный ущерб может рассматриваться и с точки зрения потерь, приводящих к какой-либо убыточности, в частности в тех случаях, когда они могут быть оценены.

1. *Потери, связанные с материальным ущербом.* Речь идет о компенсации или размещении утраченных или похищенных материальных средств. К этой сумме может добавиться целый ряд других, может быть даже более значительных:

- стоимость компенсации, возмещение другого косвенно утраченного имущества;
- стоимость ремонтно-восстановительных работ;
- расходы на анализ и исследование причин и величины ущерба;
- другие различные расходы.

2. *Дополнительные расходы,* связанные с персоналом, обслуживанием сети и расходы на восстановление информации, связанные с возобновлением работы сети по сбору, хранению, обработке и контролю данных.

К дополнительным расходам относятся также:

- поддержка информационных ресурсов и средств удаленного доступа;
- обслуживающий персонал, не связанный с информацией;
- специальные премии, расходы на перевозку и др.;
- другие виды расходов.

3. *Эксплуатационные потери,* связанные с ущемлением банковских интересов, или с финансовыми издержками, или с потерей клиентов.

Расходы на эксплуатацию соответствуют снижению общего потенциала предприятия, вызываемого следующими причинами:

- снижением банковского доверия;
- уменьшением размеров прибыли;
- потерей клиентуры;
- снижением доходов предприятия;
- другими причинами.

Естественно, что информационные потери увеличивают дополнительные расходы на их восстановление, что требует определенного времени. Временные задержки вызывают соответствующие претензии пользователей, потери интересов, а иногда и финансовые санкции.

4. *Утрата фондов или невосстанавливаемого имущества.* Утрата фондов соответствует в общем случае уменьшению финансовых возможностей (деньги, чеки, облигации, векселя, денежные переводы, боны, акции и т. д.).

Преступные действия могут быть предприняты и в отношении счетов третьей стороны (клиенты, поставщики, государство, лица наемного труда), а иногда даже и против капиталов. Потери собственности соответствуют утрате материальных ценностей как складированных, так и закупленных, а также недвижимости.

5. *Прочие расходы и потери,* в частности, связаны с моральной ответственностью.

Эта категория потерь по своему содержанию довольно разнообразна: травмы, телесные повреждения, моральный ущерб, судебные издержки, штрафы, расходы на обучение и различные эксперименты, другие виды гражданской ответственности. Сюда же можно отнести качественные потери и другие издержки.

Ущерб может быть прямой (расходы, связанные с восстановлением системы) и косвенный (потери информации, клиентуры).

В отдельных монографиях и статьях отечественных и зарубежных ученых излагаются некоторые результаты практических исследований по определению количественных значений различных угроз информационным системам. Не умаляя значения других авторов, исследовавших это направление, рассмотрим подход к оценке убытков информационным системам, проведенный Ж. Ламером [34]. В своей работе Ж. Ламер так оценивает убытки ИС. Размеры ущерба, нанесенного ИС за время с 1989-го по 1990 г., характеризуются количественными показателями, приведенными в табл. 2.7.

*Таблица 2. 7. Размеры ущерба информационным системам от различных видов угроз*

| *Вид угрозы* | *Содержание угрозы* | *Виды ущерба* | | | | *Размеры ущерба, млн. фр.* | |
|---|---|---|---|---|---|---|---|
| | | *Г* | *Д* | *Е* | *Ж* | *Всего* | *Процент к 1986 г.* |
| *А* | 1<br>2<br>3 | 420<br>50 | 940<br>45<br>1080 | - | 100 | 1460<br>95<br>1080 | +6<br>+12<br>+3 |
| *Итого* | | 470 | 2065 | - | 100 | 2635 | +21 |
| *Б* | 4<br>5<br>6 | - | 350<br>210<br>650 | 90<br>10<br>50 | 160<br>30<br>200 | 600<br>250<br>300 | -8<br>-17<br>+6 |
| *Итого* | | | 1250 | 150 | 390 | 1750 | -19 |
| *В* | 7<br>8<br>9<br>10 | - | 650<br>570<br>1250<br>50 | 1850<br>10 | 110<br>150 | 2650<br>670<br>1250<br>50 | +6<br>+16<br>+14<br>-33 |
| *Итого* | | | 2650 | 1860 | 260 | 4670 | +3 |
| *Всего* | | 470<br>+6 | 5775<br>-6 | 2010<br>+5,5 | 750<br>+5 | 9005<br>+0,5 | +5 |

*Примечания:*

А - происшествия. Это угроза материальным средствам информационной системы. Охватывает: 1 - материальный ущерб; 2 - кражи, хищения и другие виды действий; 3 - аварии, поломки, отказы, выход из строя аппаратных и программных средств и баз данных.

Б - ошибки и непредвиденные действия. Охватывает: 4 - ошибки ввода, хранения, обработки и передачи информации; 5 - ошибки функционирования системы; 6 - концептуальные ошибки и ошибки внедрения (реализации).

В - вредительство: 7 - экономический шпионаж; 8 болтливость и разглашение информации; 9 - копирование программ и операционных систем; 10 - саботаж, забастовки, уход (увольнение) сотрудников.

Виды ущерба: Г - материальный ущерб различного характера; Д - дополнительные расходы на возмещение убытков; Е - финансовые убытки; Ж - моральный ущерб и др.

Убытки от злонамеренных действий непрерывно возрастают и являются наиболее значительными.

Приведенные в таблице данные обладают определенной погрешностью (порядка 20 %), что связано в основном со сбором статистических данных.

В общем, 1990 г. отличался некоторым замедлением всех видов потерь, хотя ситуация в зависимости от различных причин довольно разнообразна (происшествия - +4,8 %, ошибки - -2,6 %, злоупотребления - +8,6 %).

Следует отменить, что ущерб, превышающий 10 млн. фр., увеличился (46 против 44), при этом зарегистрирован только один случай, сумма которого превышает 100 млн. франков (против четырех в 1989 г.).

Убытки, связанные с происшествиями (2-я строка), зависят от развития парка, в частности от увеличения техники и рабочих мест, а также от разнообразия причин: пожары - 42 %; задымления, коррозия, неисправности - 11 %; ущерб от подтоплений - 12%; выход из строя машин - 8 %; возгорание электросетей и приборов (от грозовых разрядов и перенапряжения) - 9 %; неполадки во внешней среде - 10 %; другие случаи - 8%.

Что касается 3-й строки, различие также довольно значительное. Типичные аварии оборудования - 18 %; неполадки во внешней среде - 9 %; специфические неисправности оборудования - 15 %; выход из строя операционной системы - 10 %; неисправности сетей - 11 %; перебои в снабжении водой - 5 %, перебои в электроснабжении - 3 %; перебои различного рода снабжения - 8 %; другие причины - 21 %.

Убытки, связанные с ошибками, несколько уменьшились. Это, в частности, относится к 4-й строке (несмотря на еще многочисленные ошибки маршрутизации потоков и ошибки, связанные с использованием сетей) и к 5-й сроке (здесь за счет увеличения доли автоматизации повысилось качество продукции). Вместе с тем можно отметить, что если увеличение обмена по каналам привело к улучшению показателей 4-й строки, то функциональные ошибки, которые не отражаются в этой таблице, скорее всего имеют тенденцию к росту.

Концептуальные и внедренческие ошибки (6-я строка). Причины носят одновременно структурный (привлечение к разработке сторонних организаций, абонементное обслуживание) и технический характер (физический износ постоянно растущего числа действующих систем, обусловливающий проблемы восстановления или адаптации новых, более сложных систем и т. д.).

Убытки, связанные со злоупотреблениями (7-я строка). Здесь довольно высокие показатели. По состоянию на 1989 г. они составляли: мошенничество - 67 % и саботаж - 33 %. В свою очередь, мошенничество подразделяется: на хищение фондов - 70 %, хищение материальных ценностей - 30 %. Последние могут быть проанализированы по отношению к социально-экономическому сектору: I - банки, страхование, социальное обеспечение, финансы - 38 %; II - промышленность, сельское хозяйство - 28 %; III - транспорт, торговля, другие услуги - 34 %. Саботаж подразделяется, в свою очередь: на фальсификацию данных или программ - 20 %; частичный вывод из строя или частичное блокирование - 49 %; полный вывод из строя или полное блокирование - 31 %. Убытки, связанные с вирусами, трудно поддаются оценке. В общем, они меньше 100 млн. фр. Хотя случаи их появления увеличиваются как в сетях мини-ЭВМ, так и в больших системах.

Убытки от разглашения и промышленного шпионажа (8-я строка) весьма значительны. Сегодня шпионаж не ограничивается только областью промышленности, а становится преимущественно экономическим. Особенно прогрессируют секторы торговли и финансов.

Показатели 9-й строки вновь увеличились после их падения в 1988 г. Это объясняется увеличением пиратских действий и в особенности ростом числа случаев подделки.

10-я строка имеет явную тенденцию к уменьшению приносимого ущерба.

В [4] анализируются угрозы автоматизированным информационным системам коммерческих банков. Результаты исследований, проведенных Datapro Information Service Group на основе анкетирования 1153 банков,

приведены в табл. 2.8. (В 1991, 1992, и 2001 гг. в опросе участвовало соответственно 1102, 1153 и 1121 респондент.)

*Таблица 2.8. Угрозы автоматизированным информационным системам, %*

| *Вид угрозы* | *Содержание угрозы* | *1991* | *1992* | *2001* |
|---|---|---|---|---|
| Потеря связи | Стихийные бедствия | 14 | 8 | 8 |
| | Небрежность пользователей | _ | 15 | 17 |
| | Неисправность учрежденческих АТС | _ | 21 | 25 |
| | Неисправность в сетях передачи данных | _ | 46 | 46 |
| | Ошибки программных средств | . | 39 | 55 |
| | Другие причины | 42 | 36 | 31 |
| Компьютерные преступления | Программными средствами (включая вирусы) | 22 | 44 | 64 |
| | Раскрытие пароля | 28 | 30 | 32 |
| | Внутренние угрозы системе | 4 | 5 | 2 |
| | Внешние угрозы системе | 2 | 2 | 2 |
| | Возгорание компьютера | 2 | 1 | 1 |
| | Утечка информации | 9 | 11 | 17 |
| Несанкционированный доступ | | 19 | 22 | 34 |
| Стихийные бедствия | Подтопление и другие причины | 3 | 3 | 3 |

Угрозы данным информационным системам, выраженные как причины потери данных в ИС [3], приведены на рис. 2.12. Анализ крупных убытков^ особенно тех, которые могут поставить под угрозу само существование предприятия, показывает, что, кроме основных причин, нанесению ущерба способствовали и такие факторы, как:

- отсутствие взаимодействия между ответственными за безопасность лицами;
- несоответствие технических средств реальным потребностям безопасности;
- установка средств безопасности без глубокого изучения конкретных условий и особенностей.

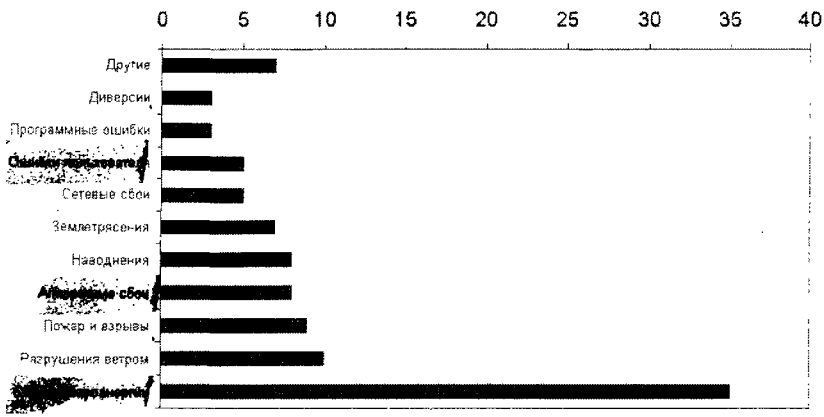



Рис. 2.12. Причины потери данных

Понять это, кроме технических аспектов, часто второстепенных и не представляющих собой значительных проблем на практике, - значит ОВЛАДЕТЬ основами управления безопасностью.

Основные причины убытков связаны не столько с недостаточностью средств безопасности как таковых, сколько с отсутствием взаимосвязи между ними.

## 4.5. Информационные инфекции

В течение последнего времени множатся примеры систем, подвергнувшихся информационным инфекциям. Все говорят о том, что в будущем логические бомбы, вирусы, черви и другие инфекции явятся главной причиной компьютерных преступлений. Совсем недавно речь шла в основном о случаях с малыми системами. Между тем отмечаются случаи прямых атак и на большие системы со стороны сети или перехода вирусов от микроЭВМ к центральным («переходящий» вирус, поддерживаемый совместимостью операционных систем и унификацией наборов данных).

В настоящее время инфекции в информационных системах становятся обычными и имеют неодинаковые последствия в каждом конкретном случае. В основном это потери рабочего времени.

Число атак больших систем (по сети и реже через магнитные носители) растет. Речь идет, в частности, о логических бомбах, разрушающих набор данных (в том числе и тех, которые считаются защищенными, поскольку инфекция сохраняется долгое время) или парализующих систему.

Участились случаи, когда предприятие полностью лишается одного или нескольких наборов данных, а иногда даже программ, что может в самом худшем случае привести к катастрофическим потерям.

Угроза таких атак может быть реальной или выражаться в виде шантажа или вымогательства фондов. Мотивы при этом могут быть самые различные: от личных интересов до преступной конкуренции (случаи уже ординарные).

Угрозы информационных инфекций опасны не только персональным ЭВМ. Они не менее опасны большим системам и информационным сетям самого различного уровня.

Различные виды злонамеренных действий в нематериальной сфере (разрушение или изменение данных или программ) могут быть подразделены на два крупных класса:

- физический саботаж (фальсификация данных, изменение логики обработки или защиты);
- информационные инфекции (троянский конь, логическая бомба, черви и вирусы), являющиеся программами, далекими от того, чтобы принести полезные результаты пользователю; они предназначены для того, чтобы расстроить, изменить или разрушить полностью или частично элементы, обеспечивающие нормальное функционирование системы.

Информационные инфекции специфически ориентированы и обладают определенными чертами: противоправны (незаконны), способны самовостанавливаться и размножаться; а также имеют определенный инкубационный период - замедленное время начала действия.

Информационные инфекции имеют злонамеренный характер: их действия могут иметь разрушительный результат (например, уничтожение набора данных), реже физическое уничтожение (например, резкое включение и выключение дисковода), сдерживающее действие (переполнение канала ввода-вывода, памяти) или просто видоизменяющее влияние на работу программ.

Самовосстановление и размножение приводит к заражению других программ и распространению по линиям связи. Это влияние трудно ограничить, так как недостаточно выявить только один экземпляр вируса: зараженными могут быть не только копии, но и любые другие программы, вступившие в связь с ней.

Замедленное действие проявляется в том, что работа программы начинается при определенных условиях: дата, час, продолжительность, наступление события и т. д. Такое действие называют логической бомбой.

Логические бомбы могут быть «запрятаны» служащим, например программистом; обычно бомба представляет собой часть программы, которая запускается всякий раз, когда вводится определенная информация. Такая ловушка может сработать не сразу. Например, она может сработать от ввода данных, вызывающих отработку секции программы, которая портит или уничтожает информацию [10].

Логические бомбы, как вытекает из их названия, используются для искажения или уничтожения информации, реже с их помощью совершается кража или мошенничество. Манипуляциями с логическими бомбами обычно занимаются чем-то недовольные служащие, собирающиеся покинуть данную организацию, но это могут быть и консультанты, служащие с определенными политическими убеждениями, инженеры, которые при повторных обращениях могут попытаться вывести систему из строя.

Реальный пример логической бомбы: программист, предвидя свое увольнение, вносит в программу заработной платы определенные изменения, работа которых начнется, если его фамилия исчезнет из набора данных о персонале фирмы.

Троянский конь - это часть программы, которая при обращении способна, например, вмешаться в инструкцию передачи денежных средств или в движение акций, а затем уничтожить все улики. Ее можно применить также в случае, когда один пользователь работает с программой, которая предоставляет ресурсы другому пользователю. Известен случай, когда преступная группа смогла договориться с программистом торговой фирмы, работающим над банковским программным обеспечением, о том, чтобы он ввел подпрограмму, которая предоставит этим преступникам доступ в систему после ее установки с целью переместить денежные вклады.

Известен также случай, когда фирма, разрабатывающая программное обеспечение для банковских систем, стала объектов домогательств другой фирмы, которая хотела выкупить программы и имела тесную связь с преступным миром. Преступная группа, если она удачно определит место для внедрения троянского коня (например, включит его в систему очистки с автоматизированным контролем, выдающую денежные средства), может безмерно обогатиться.

Червь представляет собой паразитный процесс, который потребляет (истощает) ресурсы системы. Программа обладает свойством перевоплощаться и воспроизводиться в диспетчерах терминалов. Она может также приводить к разрушению программ.

Вирус представляет собой программу, которая обладает способностью размножаться и самовосстанавливаться. Некоторые вирусы помечают программы, которые они заразили, с помощью пометы с тем, чтобы

не заражать несколько раз одну и ту же программу. Эта помета используется некоторыми антивирусными средствами. Другие средства используют последовательность характерных для вирусов кодов.

Большинство известных вирусов обладают замедленным действием. Они различаются между собой способами заражать программы и своей эффективностью. Существует три основные категории вирусов:

- Системные вирусы, объектом заражения которых являются исключительно загрузочные секторы (BOOT).
- Почтовые вирусы, объектом заражения которых являются электронные сообщения.
- Программные вирусы, заражающие различные программы функционального назначения. Программные вирусы можно подразделить на две категории в соответствии с воздействием, которое они оказывают на информационные программы. Эта классификация позволяет разработать процедуры обеспечения безопасности применительно к каждому виду вирусов.

Восстанавливающийся вирус внедряется внутрь программы, которую он частично разрушает. Объем инфицированной программы при этом не изменяется. Это не позволяет использовать этот параметр для обнаружения заражения программы. Однако инфицированная программа не может больше нормально работать. Это довольно быстро обнаруживает пользователь.

Вирус, внедряемый путем вставки, изменяет программу не разрушая ее. Всякий раз, когда задействуется программа, вирус проявляет себя позже, после окончания работы программы. Программа кажется нормально работающей, что может затруднить своевременное обнаружение вируса. Однако увеличение объема программы позволяет довольно быстро обнаружить инфицированную программу (табл. 2.9).

*Таблица 2.9. Анализ проявления каждого из видов инфекций*

| *Вид инфекции* | *Характер действия* | | |
|---|---|---|---|
| | *незаконный* | *с замедлением* | *с самовосстановлением* |
| Троянский конь | Всегда | Редко, но возможно | Никогда |
| Логическая бомба | Всегда | Часто, но необязательно | Никогда |
| Червь | Всегда | Возможно | Всегда |
| Вирус | Всегда | Очень часто | Всегда |

Строки в табл. 2.9 следуют в хронологическом порядке: первые логические инфекции имели место на основе троянских коней, затем идут логические бомбы и, наконец, черви и вирусы. Хронологический порядок довольно хорошо отражает, кроме того, степень сложности: в то время как знание одного из распространенных языков программирования, например Си или Паскаля, достаточно для написания троянского коня или логической бомбы, знание Ассемблера почти всегда необходимо для написания червя или вируса.

Табл. 2.10 иллюстрирует уровни заражения, создаваемого информационными инфекциями.

*Таблица 2.10. Уровни заражения, создаваемого червем и вирусом*

| *Объект заражения* | *Червь* | *Вирус* |
|---|---|---|
| Оперативная память | Да | Да |
| Оперативная память ЭВМ в составе сети | Да | Возможно |
| Накопитель на жестком магнитном диске (НЖМД) | Нет | Да |
| Накопитель на гибком магнитном диске (НГМД) | Нет | Да |
| Внешние накопители ЭВМ в составе сети | Исключено | Возможно |

## 4.6. Убытки, связанные с информационным обменом

Установить информационный обмен между несколькими партнерами - это значит договориться о технических (нормализация функций и используемых данных, интеграция и автоматизация процессов, спецификация станций и сетей и т. д.) и юридических (ответственность сторон, право проверки передаваемой информации и др.) условиях передачи данных. К этому следует добавить еще и требования сокращения времени передачи документов, снижение стоимости, улучшение качества информационного обслуживания.

Убытки в системе обмена данными могут иметь внешние и внутренние причины, часто взаимосвязанные и взаимообусловливаемые, причиненные теми или иными угрозами, покушениями или другими факторами.

На рис. 2.13 представлена обобщенная схема злонамеренных действий.

### *4.6.1. Остановки или выходы из строя*

Речь идет о простой остановке или выходе из строя системы (физическая поломка, отказ или авария оборудования или программных средств, случайные или более или менее частые в течение определенного времени). Причины могут быть многочисленными.

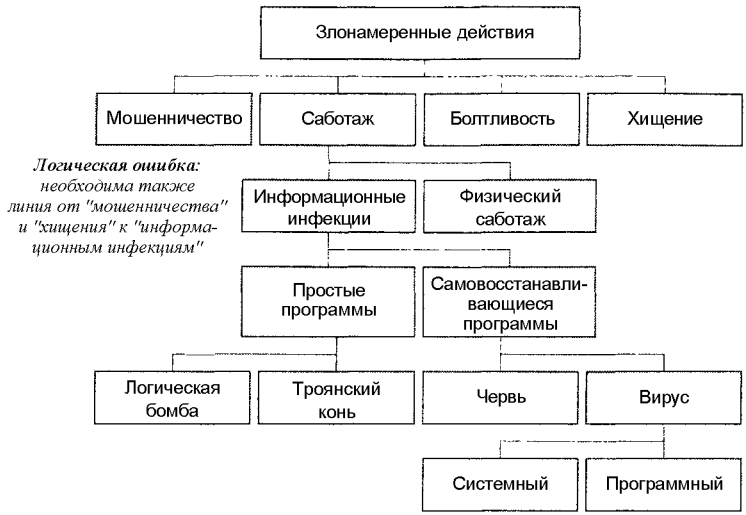



Рис. 2.13. Обобщенная схема злонамеренных действий

1. Происшествия, аварии, отказы системы, случайные или преднамеренные, могут нарушить готовность системы передачи данных.
2. Перерывы в работе узлов или магистральных линий связи. Речь идет о собственных средствах или о сетях передачи данных или центра вашего абонента. Причины могут быть разные: забастовки, случайное повреждение оборудования, происшествия (стихийные бедствия), физическое стирание информации и др. Продолжительность прерывания работы зависит от многих причин и от возможностей защиты и организации восстановления.
3. Помехи. Помехи в системе связи могут значительно затруднить информационный обмен и привести к ошибкам и потере информации.

### *4.6.2. Потери информации*

В процессе передачи данные могут быть утрачены, что создает проблему готовности (полная утрата), целостности (частичная утрата) или направлены не по адресу (ошибки маршрутизации), что приводит к нарушению конфиденциальности. Причины могут корениться в сетях передачи данных или в узлах связи. В данном случае источниками могут быть оборудование, протоколы обмена или люди (ошибки или злонамеренные действия). В числе последних могут быть, в частности, логические бомбы, вирусы, которые наносят удар прежде всего по целостности, а затем уже по готовности системы.

### *4.6.3. Изменение информации*

Этот вид бедствия затрагивает и содержание, и последовательность информации (изменение порядка и формы сообщения). В основе этого может быть ошибка или злонамеренное действие. Сознательное изменение информации может привести к ее утрате, задержке, модификации или служить основой для мошенничества (хищение материальных и финансовых ценностей).

Информация может быть изменена во время передачи (при вводе), при передачи или при приеме. В любом случае изменение информации может быть результатом либо некомпетентности, либо злоумышленных действий.

### *4.6.4. Неискренность*

Передающий отрицает факт передачи или принимающий не подтверждает факт приема сообщения. Это может быть результатом ошибки или чаще всего нечестного поступка. Бедствие произошло, но ответственность на себя никто не берет. Это приводит к росту злоумышленных действий.

### *4.6.5. Маскарад*

Выдача себя за другого пользователя, чтобы снять с себя ответственность или же использовать его полномочия с целью формирования ложной информации, изменения законной информации, применения ложного удостоверения личности для получения несанкционированного доступа, санкционирования ложных обменов информацией или же их подтверждения. Для этого могут использоваться чужие идентификаторы и пароли или вноситься изменения в процесс передачи информации. Существует много способов, позволяющих убедиться в законности информационного обмена в интересах его защиты. Это может быть запрос приемной стороны на подтверждение опознавательных элементов (идентификаторов, контрольных сумм и др.). Следует учитывать возможность атак, предпринимаемых злоумышленниками во время обмена информацией (пиратство, перехват элементов подлинности, маскарад и др.). Пират может выступать инициатором запроса на подтверждение подлинности сообщения. Например, пират становится посредником между А и В. Он говорит А, что он В; запрашивает у А подтверждение подлинности как В; он говорит В, что он А и что он желает обменяться опознавательными элементами. Далее следует информационный обмен.

### *4.6.6. Перехват информации*

Информация может быть перехвачена при передаче путем подключения или за счет наводок или излучения. Подключение может быть физическим или программным в зависимости от места расположения пункта перехвата. Информация может быть перехвачена не только на узлах связи, но и на кабелях (подключение, наводки, излучение).

### *4.6.7. Вторжение в информационную систему*

Информационный обмен можно рассматривать как «окно», через которое можно проникнуть к информационным массивам системы, поэтому следует изучать угрозы, которые могут возникнуть, если окно «не очень хорошо закрыто». Речь идет о сценарии несанкционированного доступа к информации посредством информационного обмена. Это одна из серьезных опасностей, поскольку она может угрожать как данным, так и функциональным элементам. Вторжение может совершаться по заранее разработанному сценарию. Одной из возможных причин, мотивирующих вторжение, может быть разглашение конфиденциальной информации, в частности паролей или идентификаторов. Подобную информацию, однако, можно получить и более простыми способами: болтливостью, подкупом, шантажом..., которые совершенно не связаны с информационным обменом в составе сети.

В общем плане угроза вторжения определяется степенью открытости системы по отношению к доступу со стороны сети.

Основные рубежи на пути вторжения. Первый рубеж - организационные и структурные элементы (выбор сети, разграничение доступа и др.). Второй рубеж образуют в основном структурные (связь «ПК - сервер») и технические, (неприступность системы, элементов и ресурсов) компоненты системы информационного обмена.

По своему характеру вторжения в линии связи информационных систем по отношению к информационному обмену могут быть пассивными или активными [21] (рис. 2.14).

Пассивное проникновение - это подключение к линиям связи или прием электромагнитных излучений этих линий в любой точке системы лицом, не являющимся пользователем ЭВМ. Активное проникновение в систему представляет собой прямое использование информации из файлов, хранящихся в запоминающих устройствах. Такое проникновение реализуется обычными процедурами доступа:


Рис. 2.14. Методы вторжения в линии связи

- использованием известного способа доступа к системе или ее частям с целью задания запрещенных вопросов, обращения к файлам, содержащим интересующую информацию;
- маскировкой под истинного пользователя после получения характеристик (идентификаторов) доступа;
- использованием служебного положения, т. е. незапланированного просмотра (ревизии) информации файлов.

Активное проникновение в систему может осуществляться скрытно, т. е. в обход контрольных программ обеспечения сохранности информации.

Наиболее характерные приемы проникновения.

1. Использование точек входа, установленных в системе программистами (обслуживающим персоналом), или точек, обнаруженных при проверках цепей системного контроля.
2. Подключение к сети связи специального терминала, обеспечивающего вход в систему под видом законного пользователя ЭВМ, с последующим восстановлением связи по типу ошибочного сообщения, а также в момент, когда законный пользователь не проявляет активности, но продолжает занимать канал связи.
3. Аннулирование сигнала пользователя о завершении работы с системой и последующее продолжение работы от его имени.

Подобные попытки проникновения могут быть вызваны не только простым удовлетворением любопытства квалифицированного программиста (пользователя), но и преднамеренным получением конфиденциальной информации.

## 4.7. Модель нарушителя информационных систем

Попытка получить несанкционированный доступ к информационной системе или вычислительной сети с целью ознакомиться с ними, оставить записку, выполнить, уничтожить, изменить или похитит программу или иную информацию квалифицируется как компьютерное пиратство. Как явление подобные действия прослеживаются в последние 15 лет, но при этом наблюдается тенденция к их стремительному росту по мере увеличения числа бытовых ПК [21, 33].

Рост компьютерных нарушений ожидается в тех странах, где они широко рекламируются с помощью фильмов и книг, а дети в процессе игр рано начинают знакомиться с компьютерами. Вместе с тем растет число и более серьезных нарушений, связанных с умышленными действиями. Так, например, известны случаи внедрения в военные системы НАТО, США, нарушения телевизионной спутниковой связи, вывода из строя электронных узлов регистрации на бензоколонках, использующих высокочастотные усилители; известны попытки перевода в Швейцарию евробонов на сумму 8,5 млн. долл. и разрушения европейской коммуникационной сети связи. Из этого следует, что не только компьютеры, но и другие электронные системы являются объектами злоумышленных действий.

Авторам хотелось бы разделить два определения: хакер (hacker) и кракер (cracker). Основное отличие состоит в постановке целей взлома компьютерных систем: первые ставят исследовательские задачи по оценке и нахождению уязвимостей с целью последующего повышения надежности компьютерной системы. Кракеры же вторгаются в систему с целью разрушения, кражи, порчи, модификации информации и совершают правонарушения с корыстными намерениями быстрого обогащения. Далее по тексту в некоторых случаях будем объединять их понятием «взломщик». Очевидно, что при несанкционированном доступе к информации наиболее губительным будет появление кракера. Иногда в литературе можно встретить термин крекер.

Однако компьютерные пираты (кракеры) не интересуются, насколько хорошо осуществляется в целом контроль в той или иной системе; они ищут единственную лазейку, которая приведет их к желанной цели. Для получения информации они проявляют незаурядную изобретательность,

используя психологические факторы, детальное планирование и активные действия. Кракеры совершают компьютерные преступления, считая, что это более легкий путь добывания денег, чем ограбление банков. При этом они пользуются такими приемами, как взяточничество и вымогательство, о которых заурядный владелец ЭВМ, возможно, читал, но никогда не предполагал, что сам станет объектом таких действий. Однако изобилие примеров говорит о том, что это не так. Объектами кракерских атак становятся как фирмы и банки, так и частные лица. Вот всего лишь несколько примеров.

**«Забавы хакеров».** «Недавно компьютерная сеть г. Северска (Томская область) подверглась массированной атаке доморощенных хакеров. В результате межрайонному отделу налоговой полиции был перекрыт доступ в Интернет. Это вторжение в городскую компьютерную сеть было не только зафиксировано налоговыми полисменами, но и задокументировано на магнитных носителях для дальнейшего использования в качестве доказательства в случае возбуждения уголовного дела» [38].

«Суд **над томскими хакерами».** 16.02.2002 г. «Двух жителей Томска, рассылавших через Интернет компьютерные вирусы, судят в районном суде города. Их уголовное дело состоит из семи томов. С помощью популярной программы ICQ злоумышленники распространяли по сети файлы, зараженные вирусной программой типа «троянский конь». В активированном виде вирус позволял хакерам получить доступ к ресурсам зараженного компьютера, завладеть чужими паролями и контролировать ввод данных с клавиатуры. Как сообщили в областном УФСБ, все началось в апреле 2000 г. с жалобы жителя Томска в ОАО «Томсктелеком» на многократное увеличение месячной платы за пользование сетью Интернет. С 200 руб. сумма таинственным образом возросла в 5 раз, превысив сначала одну, а потом 2 тыс. руб. в месяц. Пострадавший рассказал, что недавно он получил по почте ICQ странное электронное письмо. Обследование компьютера потерпевшего выявило наличие вируса в системе. Вскоре был установлен номер телефона, с которого незаконно подключались к Интернету. От действий подсудимых компьютерных воров пострадало в городе еще более десяти человек. В Томской области это первое доведенное до суда уголовное дело такого рода» [39 www.dni.ru/news/society/2002/2/16/6047.html].

**«Криминал» О. Никитский.** Гор. Омск. «Два года назад в Омске при помощи поддельной карты были ограблены банкоматы Омскпромстройбанка системы «Золотая корона». Однако разработчики платежной системы смогли тогда убедить общественность, что речь идет о случайном доступе, не связанном со взломом системы защиты. Сегодня же, два

года спустя, в Омске состоялся новый судебный процесс - над молодым человеком, который сумел подделать микропроцессорную карту ОАО «Омская электросвязь» и тем самым окончательно развенчал миф о неуязвимости смарт-технологий.

Согласно решению суда, эмуляторы (поддельные образцы) пластиковых карт, с помощью которых была ограблена «Золотая корона», изготовил 23-летний Е. Монастырев, ведущий специалист отдела вычислительной техники Томского АКБ «Нефтеэнергобанк». По мнению следователей, при помощи служебного оборудования он изготовил поддельные карты, с помощью которых в омских банкоматах неизвестные сообщники сняли 25 тыс. долл. Программист получил 2 года. Экспертизу материалов дела проводило ФАПСИ.

В суде города рассматривается дело о подделки телефонных карт, которые работают по тому же принципу, что и банковские, хотя немного проще устроены: в зависимости от продолжительности разговора процессор телефона-автомата изменяет количество тарифных единиц, записанных в микропроцессоре карты. «При использовании телефонной карты находящаяся на ней информация об отсутствии тарифных единиц не поступала в телефонный аппарат, что позволяло пользоваться услугами связи без оплаты» - такое заключение вынесло следствие. После нейтрализации самоучки доход от продажи карт вырос на 500 тыс. руб. Ущерб от деятельности афериста составил 3 млн. руб.» [40].

Удивительно мало фирм и людей верит в то, что они могут пострадать от кракеров, и еще меньше таких, кто анализировал возможные угрозы и обеспечил защиту. Большинство менеджеров под действием средств массовой информации считают компьютерными нарушителями только школьников и применяют против них такое средство защиты, как пароли. При этом они не осознают более серьезной опасности, которая исходит от профессиональных или обиженных программистов, поскольку не понимают мотивов, которыми руководствуются эти люди при совершении компьютерных пиратств.

Для предотвращения возможных угроз фирмы должны не только обеспечить защиту операционных систем, программного обеспечения и контроля доступа, но и попытаться выявить категории нарушителей и те методы, которые они используют.

В зависимости от мотивов, целей и методов действия всех взломщиков можно разбить на несколько групп начиная с дилетантов и кончая профессионалами. Их можно представить четырьмя группами:

- начинающим взломщиком;
- освоившим основы работы на ПЭВМ и в составе сети;

- классным специалистом;
- специалистом высшего класса.

В табл. 2.11 представлены группы взломщиков в связке с их возможностями по реализации злонамеренных целей.

*Таблица 2.11. Модель нарушителя в ИС*

| *Группа* | *Возможности проникновения* | | | |
|---|---|---|---|---|
| | Запуск задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации | Создание и запуск собственных программ с новыми функциями по обработке информации | Возможность управления функционированием ИС, т. е. воздействие на базовое ПО, на состав и конфигурацию ее оборудования | Полное и всестороннее воздействие на средства ИС, вплоть до включения в состав ИС своих средств и ПО |
| Начинающий взломщик | + | | | |
| Освоивший основы работы на ПЭВМ и в составе сети | + | + | | |
| Классный специалист | + | + | + | |
| Специалист высшего класса | + | + | + | + |

Нарушитель является специалистом высшей квалификации, знает все про информационные системы, и в частности о составе и средствах ее защиты. Модель нарушителя определяет:

- категории лиц, в числе которых может оказаться нарушитель;
- возможные цели нарушителя и их градации по степени важности и опасности;
- предположения о его квалификации;
- оценка его технической вооруженности;
- ограничения и предположения о характере его действий.

Диапазон побудительных мотивов получения доступа к системе довольно широк: от желания испытать эмоциональный подъем при игре с компьютером до ощущения власти над ненавистным менеджером. Занимаются этим не только новички, желающие позабавиться, но и профессиональные программисты. Пароли они добывают либо в результате догадки, либо путем обмена с другими взломщиками.

Часть из них, однако, начинает не только просматривать файлы, но и проявлять интерес к их содержимому, а это уже представляет серьезную угрозу, поскольку в данном случае трудно отличить безобидное баловство от умышленных действий.

До недавнего времени вызывали беспокойство случаи, когда недовольные руководителем служащие, злоупотребляя своим положением, портили системы, допуская к ним посторонних или оставляя их в рабочем состоянии без присмотра. Побудительными мотивами таких действий являются:

- реакция на выговор или замечание со стороны руководителя;
- недовольство тем, что фирма не оплатила сверхурочные часы работы (хотя чаще всего сверхурочная работа возникает из-за неэффективного использования рабочего времени);
- злой умысел в качестве, например, реванша с целью ослабить фирму как конкурента какой-либо вновь создаваемой фирмы.

Недовольный руководителем служащий создает одну из самых больших угроз вычислительным системам коллективного пользования; это обусловлено еще и тем, что агентства по борьбе со взломщиками с большей охотой обслуживают владельцев индивидуальных компьютеров.

Профессиональные взломщики - это компьютерные фанаты, прекрасно знающие вычислительную технику и системы связи. Они затратили массу времени на обдумывание способов проникновения в системы и еще больше, экспериментируя с самими системами. Для вхождения в систему профессионалы чаще всего используют некоторую систематику и эксперименты, а не рассчитывают на удачу или догадку. Их цель - выявить и преодолеть систему защиты, изучить возможности вычислительной установки и затем удалиться, самоутвердившись в возможности достижения цели.

Благодаря высокой квалификации эти люди понимают, что степень риска мала, так как отсутствуют мотивы разрушения или хищения. Действительно, задержанные и привлекавшиеся к суду нарушители чаще всего упрекали свое начальство в дурном с ними отношении и оправды-

вали себя своей незащищенностью. Некоторые из них предлагали услуги в качестве консультантов фирмам, где накопились подобные проблемы.

Все это свидетельствует о том, насколько опасно наивное отношение ко взломщикам, которые, с одной стороны, по-детски хотят продемонстрировать свое умение внедряться в системы, а также ошибки и глупость фирм, не имеющих мощных средств защиты, и, с другой стороны, в случае их выявления хотят понести такое наказание, как если бы они не преследовали какого-либо злого умысла.

Такие личности, когда ими руководят недовольство и гнев, часто отыгрываются на других и относятся к той категории людей, которые никогда не настаивают на проведении проверок устройств защиты.

К категории взломщиков-профессионалов обычно относят: преступные группировки, преследующие политические цели; лиц, стремящихся получить информацию в целях промышленного шпионажа, и, наконец, группировки отдельных лиц, стремящихся к наживе. Приведем некоторые примеры их деятельности. Заместитель директора одной из фирм, имея доступ к сети информационного обмена, «спускал пары», посылая оскорбительные записки клиентам или перетасовывал телексы; своими действия он фактически парализовал работу станции телексной связи. Также, злоупотребляя возможностями центральной телексной связи, мошенники смогли похитить 13,8 млн. долл., пересылавшихся телеграфом. В результате прослушивания телефонных разговоров было похищено 780 тыс. ф. ст. Была предпринята попытка передачи евробонов на сумму 8,5 млн. долл. на один из личных счетов в Швейцарии.

Все описанные компьютерные махинации были тщательно спланированы и совершены со знанием дела. Мотивом нарушений служили большие деньги, которые можно было получить, практически не рискуя. Вообще профессиональные пираты стремятся свести риск к минимуму. Для этого они привлекают к соучастию работающих или недавно уволившихся с фирмы служащих, поскольку для постороннего риск быть обнаруженным при проникновении в банковские системы весьма велик. Сложность и высокое быстродействие банковских вычислительных систем, постоянное совершенствование методов ведения и проверки документов и отчетности делают практически невозможным для постороннего лица перехватить то или иное сообщение или внедриться в систему с целью похитить данные. Существует и дополнительный риск: изменение одного компонента может привести к сбою в работе другого и послужить сигналом к объявлению тревоги.

Чтобы уменьшить риск, взломщики обычно завязывают контакты со служащими, у которых есть финансовые или семейные проблемы. Так сотни лет используется шпионаж как метод, вынуждающий людей идти

на риск и преступления за минимальное вознаграждение или вовсе без него. Большинство людей могут ни разу в жизни так и не столкнуться со взломщиками, но бывает, что служащий, не осознавая своих слабостей, например пристрастившись к алкоголю или азартным играм, незаметно для себя становится должником какого-либо букмекера, который, возможно, связан с преступной организацией. Такой служащий может сболтнуть лишнее на какой-нибудь вечеринке, не предполагая, что его собеседник является профессиональным агентом.

Для осуществления несанкционированного доступа в информационную систему требуется, как правило, провести два подготовительных этапа:

- собрать сведения о системе;
- выполнить пробные попытки вхождения в систему.

**Сбор сведений.** В зависимости от личности взломщика и его наклонностей возможны различные направления сбора сведений:

- подбор соучастников;
- анализ периодических изданий, ведомственных бюллетеней и документации;
- перехват сообщений электронной почты;
- подслушивание разговоров, телексов, телефонов;
- перехват информации и электромагнитного излучения;
- организация краж;
- вымогательство и взятки.

Многие владельцы систем часто не представляют, какую кропотливую подготовительную работу должен провести нарушитель, чтобы проникнуть в ту или иную компьютерную систему. Поэтому они самонадеянно полагают, что то единственное, что необходимо сделать, - это защитить файл, указав ему пароль, и забывают, что любая информация о тех или иных слабых местах системы может помочь взломщику найти лазейку и обойти пароль, получив доступ к файлу. Таким образом, информация становится легкодоступной, если взломщик знает, где и что смотреть. Так, даже простая брошюра, описывающая возможности системы, может оказаться весьма полезной взломщику, который не знаком с системой, и может послужить ключом для вхождения в систему.

Полная картина вырисовывается в процессе постепенного и тщательного сбора информации. И если начинающие взломщики должны прило-

жить к этому все свое умение, то профессионалы достигают результатов гораздо быстрее.

**Подбор соучастников.** Подбор соучастников основан на подслушивании разговоров в барах, фойе отелей, ресторанах, такси, подключении к телефонам и телексам, изучении содержимого потерянных портфелей и документов. Большую и полезную информацию можно извлечь, если представляется возможность подсесть к группе программистов, например в баре. Этот способ часто используют репортеры и профессиональные агенты.

**Извлечение информации из периодических изданий.** Взломщики могут почерпнуть много полезной информации из газет и других периодических изданий.

**Перехват сообщений электронной почты.** Обычно для подключения к электронной почте используется бытовой компьютер с модемом для связи с государственной телефонной сетью.

Телефонный канал доступа в такую систему обычно свободен, хотя в последнее время системные операторы требуют установки устройств регистрации пользователей электронной почты. Вплоть до недавнего времени многие справочные системы были оснащены блоками, через которые взломщики могли извлекать большие объемы данных, а также идентификаторы и пароли пользователей.

Недавние случаи арестов и судебного преследования кракеров в США и Великобритании позволили выявить, насколько усложнились способы извлечения информации. Сейчас нет ничего необычного в том, что блоки, установленные кракерами, могут быть зашифрованы и только отдельные члены преступных группировок могут считывать с них информацию.

**Завязывание знакомств.** Для установления контактов с целью получить информацию о вычислительной системе или выявить служебные пароли взломщики могут использовать разнообразные приемы. Например, знакомясь, они представляются менеджерами; используют вопросники, раздавая их в фойе фирмы и детально расспрашивая сотрудников о компьютерной системе; звонят оператору ЭВМ в обеденное время с просьбой напомнить якобы забытый пароль; прогуливаются по зданию, наблюдая за доступом к системе; устанавливают контакты с незанятыми в данный момент служащими охраны, которым посетители при входе в здание фирмы должны предъявлять идентификационный код или пароль.

Более злонамеренным, но, возможно, и более успешным является метод «охоты за мозгами», когда на фирму приходит человек, якобы же-

лающий работать системным программистом или инженером по линиям связи, и просит дать ему консультацию. Удивительно, как много информации может передать вовне служащий, не имеющий перспективы роста, но считающий себя достойным более важной и высокооплачиваемой должности; он может раскрыть коды пользователей, пароли, указать слабые места в сетях связи.

**Анализ распечаток.** Некоторые взломщики получили доступ к ЭВМ просто изучая распечатки, и это один из наиболее эффективных и наименее рискованных путей получения конфиденциальной информации. Многочисленные фирмы все еще теряют информацию со своих компьютерных систем, во-первых, ошибочно думая, что она не содержит конфиденциальной информации, и, во-вторых, ошибочно полагая, что все черновые распечатки добросовестно уничтожаются. Именно таким способом взломщики смогли получить весьма полную картину организации компьютерной системы, используя выброшенные распечатки и невостребованные протоколы работы системы, которые сотрудникам вычислительного центра представлялись безобидными бумажками.

**Перехват сообщений в каналах связи.** Долгое время считалось, что о перехвате сообщений может идти речь лишь в связи с деятельностью военных или секретных служб. Благодаря тому что число фирм, оснащенных вычислительной техникой, постоянно растет, перехват сообщений стал весьма реальной угрозой и для коммерческого мира. Спектр возможных перехватов весьма широк - перехват устных сообщений с использованием радиопередатчиков, микрофонов и микроволновых устройств; подслушивание сообщений, передаваемых по телефону, телексу и другим каналам передачи данных; контроль за электромагнитным излучением от дисплеев; перехват спутниковых или микроволновых передач.

Установкой радиопередатчиков, микрофонов и микроволновых устройств или прослушиванием линий связи обычно занимаются профессиональные взломщики, а также предприимчивые любители и специалисты по связи. В последнее время число случаев установки таких устройств возросло. Излюбленными точками бесконтрольного доступа являются телефонные линии.

Существует риск при использовании трехуровневых систем связи, поскольку абонент не в состоянии контролировать работу инженеров и доступ в здание и к оборудованию. Передача данных с коммутацией пакетов или с использованием широкополосных линий связи со скоростями в тысячу и миллионы бод вызывает интерес у взломщиков и может быть перехвачена, чтобы выкрасть передаваемые сообщения, модифицировать их содержимое, задержать или удалить.

Не следует недооценивать тех трудностей, которые возникают при перехвате больших потоков слабосвязанной информации и при попытках объединить ее в нечто напоминающее исходное сообщение. Для этого может потребоваться достаточно мощный мини-компьютер, устройство для выделения сигналов отдельных каналов и терминал, на который поступают двоичные цифровые сигналы; хотя это весьма сложно, но возможно.

**Кражи.** Администраторы и менеджеры фирм получили возможность брать работу домой или при необходимости связываться и передавать информацию по телефонным каналам в банк данных фирмы. Коммивояжеры могут совершать сделки, используя терминалы в номерах отелей, или получать доступ к информации непосредственно из салона автомобиля. Это создает почву для осуществления краж в домах, автомобилях, отелях с целью получить информацию для последующего вхождения в вычислительную систему.

**Взятки и вымогательство.** Преступный мир традиционно играет на человеческих слабостях и несчастьях, таких, как чрезмерное увлечение азартными играми, семейные неурядицы, трудноразрешимые финансовые проблемы, долги, оплата медицинских счетов и т. п.

Часто посещая бары, казино, скачки, информаторы, нанятые кракерами, быстро выявляют людей, готовых идти на контакт. К сожалению, большинство фирм не предусматривает ни штата сотрудников по безопасности, ни каких-либо дисциплинарных процедур, чтобы обнаружить, помешать или снизить риск от действий служащих, попавших под влияние кракеров.

Получив необходимый объем предварительной информации, компьютерный кракер делает следующий шаг - осуществляет непосредственное вторжение в систему. Используемые им при этом средства будут зависеть от количества информации, имеющейся в его распоряжении. Чтобы осуществить несанкционированное вхождение в систему, кракеру требуется знать номер телефона или иметь доступ к линии связи, иметь протоколы работы, описания процедур входа в систему, код пользователя и пароль. Если кракер не знает телефонного адреса порта, он должен либо узнать его, завязывая знакомства, либо воспользоваться автонабирателем.

Реальный пример проникновения кракера в информационную систему ВВС США приведен с подробностями в журнале «Computer World» (1994. № 37) в статье «Арестован хакер, вторгшийся в компьютерную сеть ВВС США».

Прихожу домой.
Ем, пью, сплю за ваш счет.
Работаю круглосуточно.
*Объявление*

## 5. Методы и модели оценки уязвимости информации

Уязвимость информации есть событие, возникающее как результат такого стечения обстоятельств, когда в силу каких-то причин используемые в автоматизированных системах обработки данных средства защиты не в состоянии оказать достаточного противодействия проявлению дестабилизирующих факторам и нежелательного их воздействия на защищаемую информацию. Модель уязвимости информации в автоматизированных системах обработки данных в общем виде показана на рис. 2.15.

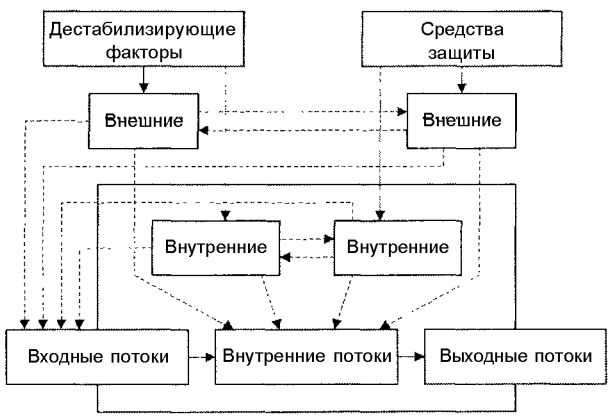



Рис. 2.15. Общая модель воздействия на информацию

Данная модель детализируется при изучении конкретных видов уязвимости информации: нарушения физической или логической целостности, несанкционированной модификации, несанкционированного получения, несанкционированного размножения.

При детализации общей модели основное внимание акцентируется на том, что подавляющее большинство нарушений физической целостности информации имеет место в процессе ее обработки на различных участках технологических маршрутов. При этом целостность информации зависит не только от процессов, происходящих на объекте, но и от целостности информации, поступающей на его вход. Основную опасность представляют случайные дестабилизирующие факторы (отказы, сбои и ошибки компонентов автоматизированных систем обработки данных),

которые потенциально могут проявиться в любое время, и в этом отношении можно говорить о регулярном потоке этих факторов. Из стихийных бедствий наибольшую опасность представляют пожары, опасность которых в большей или меньшей степени также является постоянной. Опасность побочных явлений практически может быть сведена к нулю путем надлежащего выбора места для помещений автоматизированной системы обработки данных и их оборудования. Что касается злоумышленных действий, то они связаны главным образом с несанкционированным доступом к ресурсам автоматизированной системы обработки данных. При этом наибольшую опасность представляет занесение вирусов.

В соответствии с изложенным общая модель процесса нарушения физической целостности информации на объекте автоматизированной системы обработки данных представлена на рис. 2.16.

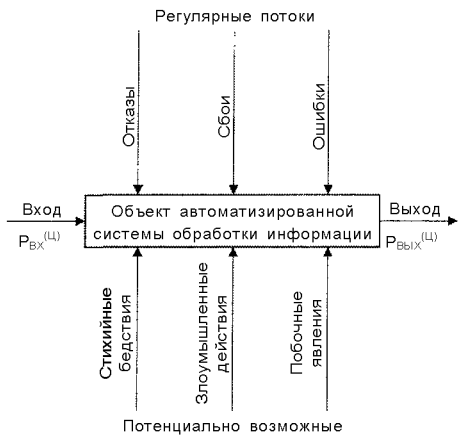



Рис. 2.16. Общая модель процесса нарушения физической целостности информации

С точки зрения несанкционированного получения информации принципиально важным является то обстоятельство, что в современных автоматизированных системах обработки данных оно возможно не только путем непосредственного доступа к базам данных, но и многими путями, не требующими такого доступа. При этом основную опасность представляют злоумышленные действия людей. Воздействие случайных факторов непосредственно не ведет к несанкционированному получению информации, оно лишь способствует появлению каналов несанкционированного получения информации, которыми может воспользоваться злоумышленник. Структурированная схема потенциально возможных злоумышленных действий в автоматизи-

ленных действий в автоматизированных системах обработки данных для самого общего случаю представлена на рис. 2.17.

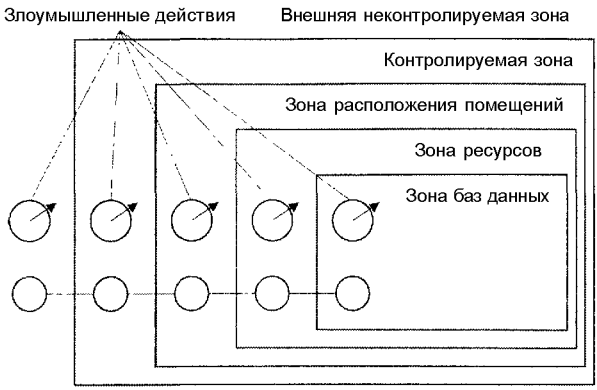



Рис. 2.17. Структурированная схема потенциально возможных злоумышленных действий в автоматизированных системах обработки данных

Обозначенные на рис. 2.17 зоны определяются следующим образом.

1. Внешняя неконтролируемая зона - территория вокруг автоматизированной системы обработки данных, на которой персоналом и средствами автоматизированной системы обработки данных не применяются никакие средства и не осуществляются никакие мероприятия для защиты информации.
2. Контролируемая зона - территория вокруг помещений автоматизированной системы обработки данных, которая непрерывно контролируется персоналом или средствами автоматизированной системы обработки данных.
3. Зона помещений автоматизированной системы обработки данных - внутреннее пространство тех помещений, в которых расположена система.
4. Зона ресурсов автоматизированной системы обработки данных - та часть помещений, откуда возможен непосредственный доступ к ресурсам системы.
5. Зона баз данных - та часть ресурсов системы, с которой возможен непосредственный доступ к защищаемым данным.

Злоумышленные действия с целью несанкционированного получения информации в общем случае возможны в каждой из перечисленных зон.

При этом для несанкционированного получения информации необходимо одновременное наступление следующих событий: нарушитель должен Получить доступ в соответствующую зону; во время нахождения нарушителя в зоне в ней должен проявиться (иметь место) соответствующий канал несанкционированного получения информации; соответствующий канал несанкционированного получения информации должен быть доступен нарушителю соответствующей категории; в канале несанкционированного получения информации в момент доступа к нему нарушителя должна находиться защищаемая информации.

Рассмотрим далее трансформацию общей модели уязвимости с точки зрения несанкционированного размножения информации. Принципиальными особенностями этого процесса являются:

- любое несанкционированное размножение есть злоумышленное действие;
- несанкционированное размножение может осуществляться в организациях-разработчиках компонентов автоматизированной системы обработки данных, непосредственно в автоматизированной системе обработки данных и сторонних организациях, причем последние могут получать носитель, с которого делается попытка снять копию как законным, так и незаконным путем.

Попытки несанкционированного размножения информации у разработчика и в автоматизированной системе обработки данных есть один из видов злоумышленных действий с целью несанкционированного ее получения и поэтому имитируются приведенной моделью. Если же носитель с защищаемой информацией каким-либо путем (законным или незаконным) попал в стороннюю организацию, то для его несанкционированного копирования могут использоваться любые средства и методы, включая и такие, которые носят характер научных исследований и опытно-конструкторских разработок.

В процессе развития теории и практики защиты информации сформировалось три методологических подхода к оценке уязвимости информации: эмпирический, теоретический и теоретико-эмпирический.

## 5.1. Эмпирический подход к оценке уязвимости информации

Сущность эмпирического подхода заключается в том, что на основе длительного сбора и обработки данных о реальных проявлениях угроз информации и о размерах того ущерба, который при этом имел место, чисто эмпирическим путем устанавливаются зависимости между потенциально возможным ущербом и коэффициентами, характеризующими

частоту проявления соответствующей угрозы и значения имевшего при ее проявлении размера ущерба.

Наиболее характерным примером моделей рассматриваемой разновидности являются модели, разработанные специалистами американской фирмы IBM. Рассмотрим развиваемые на этих моделях подходы.

Исходной посылкой при разработке моделей является почти очевидное предположение: с одной стороны, при нарушении защищенности информации наносится некоторый ущерб, с другой - обеспечение защиты информации сопряжено с расходованием средств. Полная ожидаемая стоимость защиты может быть выражена суммой расходов на защиту и потерь от ее нарушения. Совершенно очевидно, что оптимальным решением было бы выделение на защиту информации средств минимизирующих общую стоимость работ по защите информации.

Для того чтобы воспользоваться данным подходом к решению проблемы, необходимо знать (или уметь определять), во-первых, ожидаемые потери при нарушении защищенности информации, а во-вторых, зависимость между уровнем защищенности и средствами, затрачиваемыми на защиту информации.

Решение первого вопроса, т. е. оценки ожидаемых потерь при нарушении защищенности информации, принципиально может быть получено лишь тогда, когда речь идет о защите промышленной, коммерческой и им подобной тайны, хотя и здесь встречаются весьма серьезные трудности. Что касается оценки уровня потерь при нарушении статуса защищенности информации, содержащей государственную, военную и им подобную тайну, то здесь до настоящего времени строгие подходы к их получению не найдены. Данное обстоятельство существенно сужает возможную область использования моделей, основанных на рассматриваемых подходах.

Для определения уровня затрат $R_i$, обеспечивающих требуемый уровень защищенности информации, необходимо по крайней мере знать, во-первых, полный перечень угроз информации, во-вторых, потенциальную опасность для информации для каждой из угроз и, в-третьих, размеры затрат, необходимых для нейтрализации каждой из угроз.

Поскольку оптимальное решение вопроса о целесообразном уровне затрат на защиту состоит в том, что этот уровень должен быть равен уровню ожидаемых потерь при нарушении защищенности, достаточно определить только уровень потерь. Специалистами фирмы IBM предложена следующая эмпирическая зависимость ожидаемых потерь от $i$-й угрозы информации:

$$R_i = 10^{(S_i - 4)},$$

где $S_i$ - коэффициент, характеризующий возможную частоту возникновения соответствующей угрозы; $V_i$ - коэффициент, характеризующий значение возможного ущерба при ее возникновении. Предложенные специалистами значения коэффициентов следующие:

значения коэффициента $S_i$.

| *Ожидаемая (возможная) частота появления угрозы* | *Предполагаемое значение* $S_i$ |
|---|---|
| Почти никогда | 0 |
| 1 раз в 1000 лет | 1 |
| 1 раз в 100 лет | 2 |
| 1 раз в 10 лет | 3 |
| 1 раз в год | 4 |
| 1 раз в месяц (примерно, 10 раз в год) | 5 |
| 1-2 раза в неделю (примерно 100 раз в год) | 6 |
| 3 раза в день (1000 раз в год) | 7 |

возможные значения коэффициента $V_i$.

| *Значение возможного ущерба при проявлении угрозы, долл.* | *Предполагаемое значение* $V_i$ |
|---|---|
| 1 | 0 |
| 10 | 1 |
| 100 | 2 |
| 1000 | 3 |
| 10 000 | 4 |
| 100 000 | 5 |
| 1 000 000 | 6 |
| 10 000 000 | 7 |

Суммарная стоимость потерь определяется формулой

$$R = \sum_{\forall i} R_i.$$

Таким образом, если бы удалось собрать достаточное количество фактических данных о проявлениях угроз и их последствиях, то рассмотренную модель можно было бы использовать для решения достаточно широкого круга задач защиты информации, причем нетрудно видеть, что модель позволяет не только находить нужные решения, но и оценивать их точность. По России такая статистика в настоящее время практически

отсутствует. В США же, например, сбору и обработке указанных данных большое внимание уделяет целый ряд учреждений (Станфордский исследовательский институт и др.). В результате уже получены достаточно представительные данные по целому ряду угроз, которые могут быть положены в основу ориентировочных расчетов и для других стран.

## 5.2. Система с полным перекрытием

Естественным продолжением моделей оценки угроз автоматизированных систем обработки данных являются модели нейтрализации этих угроз, т. е. модели защиты. Наиболее общей моделью защиты является модель с так называемой системой с полным перекрытием.

При построении данной модели в качестве исходной взята естественная посылка, состоящая в том, что в механизме защиты должно содержаться по крайней мере одно средство для перекрытия любого потенциально возможного канала утечки информации. Методика формального описания такой системы заключается в следующем:

- составляется полный перечень объектов системы, подлежащих защите;
- составляется полный перечень потенциально возможных угроз информации, т. е. возможных вариантов злоумышленных действий;
- определяется количественная мера соответствующей угрозы для соответствующего объекта;
- формируется множество средств защиты информации в вычислительной системе;
- определяется количественная мера возможности противодействия. Если она превышает уровень угрозы, то система защиты достаточна.

Очевидно, что если множество $M$ таково, что устраняются все ребра графа, то такая система является системой с полным перекрытием.

Одной из разновидностей теоретически строгих моделей являются модели систем разграничения доступа к ресурсам автоматизированной системы обработки данных.

В самом общем виде существо этих моделей может быть представлено следующим образом. Автоматизированная система обработки данных является системой множественного доступа, т. е. к одним и тем же ее ресурсам (техническим средствам, программам, массивам данных) имеет законное право обращаться некоторое число пользователей (абонентов). Если какие-либо из указанных ресурсов являются защищаемыми, то доступ к ним должен осуществляться лишь при предъявлении соответствующих полномочий. Система разграничения доступа и должна стать тем

механизмом, который регулирует такой доступ. Требования к этому механизму на содержательном уровне состоят в том, что, с одной стороны, не должен быть разрешен доступ пользователям (или их процессам), не имеющим на это полномочий, а с другой - не должно быть отказано в доступе пользователям (или их процессам), имеющим соответствующие полномочия.

## 5.3. Практическая реализация модели «угроза - защита»

В качестве примера практической реализации модели «угроза - защита» рассмотрим табл. 2.12, где представлена информация ООО «ТехИнформКонсалтинг», г. Москва, для случая широкомасштабного внедрения в России акцизных марок с объемной криптоголографической защитой. В ней отчетливо выделяются как технические, так и организационные методы защиты информации.

*Таблица 2.12. Перечень возможных вариантов угроз и защиты от них*

| *Угроза* | *Защита* |
|---|---|
| Подделка информации в марках | 1. Информация в марках защищается путем применения электронной цифровой подписи (ЭЦП), что не позволяет производить марки с произвольной информацией, а также вносить в нее исправления.<br>2. Используемое в системе средство криптографической защиты информации (СКЗИ) «ВЕРБА-OW» имеет сертификат ФАПСИ № СФ/114-0174 от 10.04.1997 г., что гарантирует его надежность и обеспечивает юридическую значимость защищенной информации |
| Копирование информации в марках | 1. Так как система ведет учет продукции с точностью до одной единицы и каждая марка подписывается ЭЦП, то информация на каждой марке является уникальной и не подлежит массовому копированию. Так, например, для копирования партии марок в количестве 10 тыс. шт. трудозатраты составляют примерно 2 рабочих человеком месяца при условии автоматизации этого процесса и работы без остановки в течение всего рабочего дня. Без автоматизации процесса время копирования марок увеличивается на несколько порядков.<br>2. Так как в системе вся информация по проведенным проверкам экспортируется в центральную базу данных, то дублирование марок легко выявляется на этапе анализа результатов их проверок |

*Окончание табл. 2.12*

| *Угроза* | *Защита* |
|---|---|
| Кража готовых марок | В случае кражи партии готовых марок информация о них заносится в центральную базу данных. При проведении проверок продукция, маркированная этими марками, легко выявляется |
| Перепродажа готовых марок | При печати марок на них наносится информация, полностью описывающая данную конкретную единицу продукции, включая наименование, производителя, дату производства, тару, маркирующую организацию, сопроводительные документы и т. д., защищенную от подделки и модификации ЭЦП. На основании этой информации при проведении проверки легко выявляется несоответствие между марками, маркированной продукцией и сопроводительными документами |
| Сговор с разработчиками | 1. Проверка подлинности и авторства информации в защитных марках осуществляется с помощью электронной цифровой подписи. Так как разработчики не имеют доступа к используемым закрытым ключам ЭЦП, то сговор по подделке марок невозможен.<br>2. Отсутствие закладок в используемых программах может гарантироваться путем их сертификации в Государственной технической комиссией при Президенте РФ (ФСТЭК России) |
| Сговор с инспектором | Для исключения фактов искажения или несообщения инспектором результатов проверки марок в системе предусмотрена специальная «фискальная» память, в которую заносится вся информация о проведенных проверках. Далее эта информация экспортируется в центральную базу данных для анализа |
| Сговор с персоналом инспекции для модификации центральной базы данных системы | Для защиты информации от несанкционированного доступа центральная база данных разработана на СУБД Oracle 8, что обеспечивает высокую надежность хранения и защиты информации, а также масштабируемость системы. СУБД Oracle 8 имеет сертификат Государственной технической комиссией при Президенте РФ № 168 по классу защищенности 1В |

Мудрец ищет всего в себе,
безумец - всего в другом.
*Конфуций*

## 6. Рекомендации по использованию моделей оценки уязвимости информации

Как правило, модели позволяют определять текущие и прогнозировать будущие значения всех показателей уязвимости информации для любых компонентов автоматизированной системы обработки данных, любой их комбинации и для любых условий жизнедеятельности автоматизированной системы обработки данных. Некоторые замечания по использованию.

1. Практически все модели строятся в предположении независимости тех случайных событий, совокупности которых образуют сложные процессы защиты информации в современных автоматизированных системах обработки данных.
2. Для обеспечения работы моделей необходимы большие объемы таких исходных данных, подавляющее большинство которых в настоящее время отсутствует, а формирование сопряжено с большими трудностями.

Определим замечание первое - допущение независимости случайных событий, происходящих в системах защиты информации. Основными событиями, имитируемыми в моделях определения показателей уязвимости, являются: проявление дестабилизирующих факторов, воздействие проявившихся дестабилизирующих факторов на защищаемую информацию и воздействие используемых средств защиты на дестабилизирующие факторы. При этом обычно делаются следующие допущения.

1. Потенциальные возможности проявления каждого дестабилизирующего фактора не зависят от проявления других.
2. Каждый из злоумышленников действует независимо от других, т. е. не учитываются возможности формирования коалиции злоумышленников.
3. Негативное воздействие на информацию каждого из проявившихся дестабилизирующих факторов не зависит от такого же воздействия других проявившихся факторов.
4. Негативное воздействие дестабилизирующих факторов на информацию в одном каком-либо компоненте автоматизированной системы обработки данных может привести лишь к поступлению на входы

связанных с ним компонентов информации с нарушенной защищенностью и не оказывает влияния на такое же воздействие на информацию в самих этих компонентах.

5. Каждое из используемых средств защиты оказывает нейтрализующее воздействие на дестабилизирующие факторы и восстанавливающее воздействие на информацию независимо от такого же воздействия других.
6. Благоприятное воздействие средств защиты в одном компоненте автоматизированной системы обработки данных лишь снижает вероятность поступления на входы связанных с ним компонентов информации с нарушенной защищенностью и не влияет на уровень защищенности информации в самих этих компонентах.

В действительности же события, перечисленные выше являются зависимыми, хотя степень зависимости различна: от незначительной, которой вполне можно пренебречь, до существенной, которую следует учитывать. Однако для решения данной задачи в настоящее время нет необходимых предпосылок, поэтому остаются лишь методы экспертных оценок.

Второе замечание касается обеспечения моделей необходимыми исходными данными. Ранее уже неоднократно отмечалось, что для практического использования моделей определения показателей уязвимости необходимы большие объемы разнообразных данных, причем подавляющее большинство из них в настоящее время отсутствует.

Сформулируем теперь рекомендации по использованию моделей, разработанных в рамках рассмотренных ранее допущений, имея в виду, что это использование, обеспечивая решение задач анализа, синтеза и управления в системах защиты информации, не должно приводить к существенным погрешностям.

**Первая** и основная рекомендация сводится к тому, что моделями должны пользоваться квалифицированные специалисты-профессионалы в области защиты информации, которые могли бы в каждой конкретной ситуации выбрать наиболее эффективную модель и критически оценить степень адекватности получаемых решении.

**Вторая** рекомендация заключается в том, что модели надо использовать не просто для получения конкретных значений показателей уязвимости, а для оценки поведения этих значений при варьировании существенно значимыми исходными данными в возможных диапазонах их изменений. В этом плане модели определения значений показателей уязвимости могут служить весьма ценным инструментом при проведении деловых игр по защите информации.

**Третья** рекомендация сводится к тому, что для оценки адекватности моделей, исходных данных и получаемых решений надо возможно шире привлекать квалифицированных и опытных экспертов.

**Четвертая** рекомендация заключается в том, что для эффективного использования моделей надо непрерывно проявлять заботу об исходных данных, необходимых для обеспечения моделей при решении задач защиты. Существенно важным при этом является то обстоятельство, что подавляющее количество исходных данных обладает высокой степенью неопределенности. Поэтому надо не просто формировать необходимые данные, а перманентно их оценивать и уточнять.

Легче зажечь одну маленькую
свечу, чем клясть темноту.
*Конфуций*

# 7. Методы определения требований к защите информации

В самом общем виде и на чисто прагматическом уровне требования к защите могут быть определены как предотвращение угроз информации, по крайней мере тех из них, проявление которых может привести к существенно значимым последствиям. Но поскольку, как рассматривалось раньше, защита информации есть случайный процесс (показатели уязвимости носят вероятностный характер), то и требования к защите должны выражаться терминами и понятиями теории вероятностей.

По аналогии с требованиями к надежности технических систем, обоснованными в классической теории систем, требования к защите могут быть сформулированы в виде условия

$$P_з \geq P_{зт},$$

где $P_З$ - вероятность защищенности информации; $P_{ЗТ}$ - требуемый уровень защищенности. С требованиями, выраженными в таком виде, можно оперировать с использованием методов классической теории систем при решении задач защиты всех классов: анализа, синтеза и управления.

Однако из предыдущих разделов известно, что решение проблем защиты информации сопряжено с исследованиями и разработкой таких систем и процессов, в которых и конкретные методы, и общая идеология классической теории могут быть применены лишь с большими оговорками. Для повышения степени адекватности применяемых моделей реальным процессам необходим переход от концепции создания инструмен-

тальных средств получения необходимых решений на инженерной основе к концепции создания методологического базиса и инструментальных средств для динамического оптимального управления соответствующими процессами.

С учетом данного подхода в самом общем виде и на содержательном уровне требования к защите информации могут быть сформулированы в следующем виде.

Конкретные требования к защите, обусловленные спецификой автоматизированной обработки информации, определяются совокупностью следующих факторов:

- характером обрабатываемой информации;
- объемом обрабатываемой информации;
- продолжительностью пребывания информации в АСОИ;
- структурой автоматизированной системы обработки данных;
- видом защищаемой информации;
- технологией обработки информации;
- организацией информационно-вычислительного процесса в автоматизированной системе обработки данных;
- этапом жизненного цикла автоматизированной системы обработки данных.

По характеру (с точки зрения требуемой защиты) информацию можно разделить на общедоступную, конфиденциальную, служебную, секретную и совершенно секретную.

Соответствующие рекомендации по предъявлению требований к защите могут быть следующими.

1. При обработке общедоступной информации никаких специальных мер защиты от НДС не требуется.

2. Требования к защите конфиденциальной информации определяет пользователь, устанавливающий статус конфиденциальности.

3. При обработке служебной информации к ней должен быть обеспечен свободный доступ пользователям учреждения-владельца этой информации (по общему списку); доступ же пользователей, не включенных в общий список, должен осуществляться по разовым санкциям, выдаваемым пользователям, включенным в список.

4. При обработке секретной информации в зависимости от ее объема и характера может быть предъявлен один из следующих вариантов требований:

- персональное разграничение - для каждого элемента информации составляется список пользователей, имеющих к нему право доступа;
- коллективное разграничение - структура баз защищаемых данных организуется в соответствии со структурой подразделений, участвующих в обработке защищаемой информации; пользователи каждого подразделения имеют право доступа к только к «своим» данным.

5. При обработке совершенно секретной информации список лиц, имеющих право доступа, должен составляться для каждого самостоятельного элемента информации с указанием дней и времени доступа, а также перечня разрешенных процедур.

Требования, связанные с размещением защищаемой информации, могут заключаться в следующем.

При обработке информации, размещенной только в оперативном запоминающем устройстве (ОЗУ), должны обеспечиваться требуемые уровень защиты и надежность в центральном вычислителе и на коммуникациях ввода-вывода данных. При обработке информации, размещенной на одном внешнем носителе, дополнительно к предыдущему должна обеспечиваться защита в соответствующем внешнем запоминающем устройстве (ВЗУ) и коммуникациях, связывающих это устройство с процессором.

При обработке информации, размещенной на нескольких внешних носителях, дополнительно к предыдущему должна обеспечиваться необходимая изоляция друг от друга данных, размещенных на различных носителях при одновременной их обработке.

При обработке информации, размещенной на очень большом количестве носителей, дополнительно к предыдущему должна обеспечиваться защита в хранилищах носителей и на коммуникациях, связывающих хранилища с помещениями, в которых установлены ВЗУ.

С точки зрения продолжительности пребывания защищаемой информации в автоматизированной системе обработки данных требования к защите формулируются следующим образом:

- Информация разового использования подлежит защите в процессе подготовки, ввода, решения задач и выдачи результатов решения. После этого защищаемая информация должна быть уничтожена во всех устройствах автоматизированной системы обработки данных.
- Информация временного хранения дополнительно к предыдущему подлежит защите в течение объявленного времени хранения, после чего должна быть уничтожена во всех устройствах автоматизированной системы обработки данных и на всех носителях, используемых

для ее хранения. Продолжительность хранения задается или длиной промежутка времени, или числом сеансов решения соответствующих функциональных задач.

- Информация длительного хранения подлежит постоянной защите, уничтожение ее должно выполнятся по определенным командам.

Требования, определяемые структурой автоматизированной системы обработки данных, могут быть сформулированы в следующем виде.

Информация должна защищаться во всех структурных элементах автоматизированной системы обработки данных, причем специфические требования к защите информации в структурных элементах различного типа сводятся к следующему.

1. В терминалах пользователей:

- защищаемая информация может находиться только во время сеанса решения задач, после чего подлежит уничтожению;
- устройства отображения и фиксации информации должны располагаться так, чтобы исключить возможность просмотра отображаемой (выдаваемой) информации со стороны;
- информация, имеющая ограничительный гриф, должна выдаваться (отображаться) совместно с этим грифом;
- должны быть предусмотрены возможности быстрого (аварийного) уничтожения информации, находящейся в терминале (в том числе и на устройствах отображения).

2. В устройствах группового ввода-вывода (УГВВ):

- в простых УГВВ и в сложных с малым объемом запоминающего устройства (ЗУ) защищаемая информация может находиться только во время решения задач, после чего подлежит уничтожению; в сложных с большим объемом ЗУ информация может храниться в ВЗУ, однако продолжительность хранения должна быть ограниченной;
- устройства отображения и фиксации информации должны располагаться так, чтобы исключить возможность просмотра отображаемой (выдаваемой) информации со стороны;
- информация, имеющая ограничительный гриф, должна выдаваться (отображаться) совместно с этим грифом;
- в УГВВ с возможностями универсального процессора при каждом обращении к защищаемой информации должны осуществляться процедуры:

- установления подлинности (опознавания) вступающих в работу терминалов и пользователей;
- проверки законности каждого запроса на соответствие предоставленным пользователю полномочиям;
- проверки адреса выдачи информации, имеющей ограничительный гриф, и наличия этого грифа;
- контроля обработки защищаемой информации;
- регистрации запросов и всех нарушений правил защиты;

- при выдаче информации в линии связи должны осуществляться:
  - проверка адреса выдачи информации;
  - маскировка (закрытие) содержания защищаемой информации, выдаваемой в линии связи, проходящей по неконтролируемой территории;
- должны быть предусмотрены возможности аварийного уничтожения информации как в ОЗУ, так и в ВЗУ, а также подачи команды на аварийное уничтожение информации в сопряженных с УГВВ терминалах.

3. В аппаратуре и линиях связи:

- защищаемая информация должна находиться только в течение сеанса; в ЗУ аппаратуры связи могут храниться только служебные части передаваемых сообщений;
- линии связи, по которым защищаемая информация передается в явном виде, должны находиться под непрерывным контролем во время передачи информации;
- перед началом каждого сеанса передачи защищаемой информации должна осуществляться проверка адреса выдачи данных;
- при передаче большого объема защищаемой информации проверка адреса передачи должна периодически производиться в процессе передачи (через заданный промежуток времени или после передачи заданного числа знаков сообщения);
- при наличии в составе аппаратуры связи процессоров и ЗУ должна вестись регистрация данных о всех сеансах передачи защищаемой информации;
- должны быть предусмотрены возможности аварийного уничтожения информации, находящейся в аппаратуре связи.

4. В центральном вычислителе:

- защищаемая информация в ОЗУ может находиться только во время сеансов решения соответствующих задач, в ВЗУ - минимальное время, определяемое технологией решения соответствующей прикладной задачи в автоматизированной системе обработки данных;
- устройства отображения и фиксации информации должны располагаться так, чтобы исключить возможность просмотра отображаемой (выдаваемой) информации со стороны;
- информация, имеющая ограничительный гриф, должна выдаваться (отображаться) совместно с этим грифом;
- при обработке защищаемой информации должно осуществляться установление подлинности всех участвующих в обработке устройств и пользователей и ведение протоколов их работы;
- всякое обращение к защищаемой информации должно проверяться на санкционированность;
- при обмене защищаемой информации, осуществляемом с использованием линий связи, должна осуществляться проверка адреса корреспондента;
- должны быть предусмотрены возможности аварийного уничтожения всей информации, находящейся в центральном вычислителе, и подачи команды на аварийное уничтожение информации в сопряженных устройствах.

5. В ВЗУ:

- сменные носители информации должны находиться на устройствах управления в течение минимального времени, определяемого технологией автоматизированной обработки информации;
- устройства управления ВЗУ, на которых установлены носители с защищаемой информацией, должны иметь замки, предупреждающие несанкционированное изъятие или замену носителя;
- должны быть предусмотрены возможности автономного аварийного уничтожения информации на носителях, находящихся на ВЗУ.

6. В хранилище носителей:

- все носители, содержащие защищаемую информацию, должны иметь четкую и однозначную маркировку, которая, однако, не должна раскрывать содержания записанной на них информации;
- носители, содержащие защищаемую информацию, должны храниться таким образом, чтобы исключались возможности несанкционированного доступа к ним;

- при выдаче и приемке носителей должна осуществляться проверка личности получающего (сдающего) и его санкции на получение (сдачу) этих носителей;
- должны быть предусмотрены возможности аварийного уничтожения информации на носителях, находящихся в хранилищах.

7. В устройствах подготовки данных:

- защищаемая информация должна находиться только в течение времени ее подготовки;
- устройства подготовки должны быть размещены так, чтобы исключались возможности просмотра обрабатываемой информации со стороны;
- а специальных регистрационных журналах должны фиксироваться время обработки информации, исполнители, идентификаторы использованных носителей, и возможно, другие необходимые данные;
- распределение работ между операторами должно быть таким, чтобы минимизировать осведомленность их о содержании обрабатываемой информации;
- должны быть предусмотрены возможности аварийного уничтожения информации, находящейся в подразделениях подготовки данных.

8. Требования к защите информации, обусловливаемые территориальной распределенностью автоматизированной системы обработки данных, заключаются в следующем:

- в компактных автоматизированных системах обработки данных (размещенных в одном помещении) достаточно организовать и обеспечить требуемый уровень защиты в пределах того помещения, в котором размещены элементы автоматизированной системы обработки данных;
- в слабораспределенных автоматизированных системах обработки данных (размещенных в нескольких помещениях, но на одной и той же территории) дополнительно к предыдущему должна быть обеспечена требуемая защита информации в линиях связи, с помощью которых сопрягаются элементы автоматизированной системы обработки данных, расположенные в различных помещениях, для чего должны быть или постоянный контроль за этими линиями связи, или исключена передача по ним защищаемой информации в явном виде;
- в сильнораспределенных автоматизированных системах обработки данных (размещенных на нескольких территориях) дополнительно

к предыдущему должна быть обеспечена требуемая защита информации в линиях связи большой протяженности, что может быть достигнуто предупреждением передачи по ним защищаемой информации в открытом виде.

Требования, обусловливаемые видом защищаемой информации, могут быть сформулированы в таком виде:

1. К защите документальной информации предъявляются следующие требования:

- должна обеспечиваться защита как оригиналов документов, так и сведений о них, накапливаемых и обрабатываемых в автоматизированной системе обработки данных;
- применяемые средства и методы защиты должны выбираться с учетом необходимости обеспечения доступа пользователям различных категорий:
  - персонала делопроизводства и библиотеки оригиналов;
  - специалистов подразделения первичной обработки документов;
  - специалистов функциональных подразделений автоматизируемых органов.

2. При обработке фактографической быстроменяющейся информации должны учитываться следующие требования:

- применяемые средства и методы защиты не должны существенно влиять на оперативность обрабатываемой информации;
- применяемые средства и методы защиты должны выбираться с учетом обеспечения доступа к защищаемой информации строго ограниченного круга лиц.

3. К защите фактографической исходной информации предъявляются следующие требования:

- каждому пользователю должны быть обеспечены возможности формирования требований к защите создаваемых им массивов данных в пределах предусмотренных в автоматизированной системе обработки данных возможностей защиты;
- в системе защиты должны быть предусмотрены средства, выбираемые и используемые пользователями для защиты своих массивов по своему усмотрению.

4. К защите фактографической регламентной информации предъявляются следующие требования:

- применяемые средства и методы защиты должны быть рассчитаны на длительную и надежную защиту информации;
- должен обеспечиваться доступ (в пределах полномочий) широкого круга пользователей;
- повышенное значение приобретают процедуры идентификации, опознавания, проверки полномочий, регистрации обращений и контроля выдачи.

Требования, обусловливаемые технологическими схемами автоматизированной обработки информации, сводятся к тому, что в активном состоянии автоматизированной системы обработки данных должна обеспечиваться защита на всех технологических участках автоматизированной обработки информации и во всех режимах.

С точки зрения организации вычислительного процесса в автоматизированной системе обработки данных требуемая защита должна обеспечиваться при любом уровне автоматизации обработки информации, при всех способах взаимодействия пользователей со средствами автоматизации и при всех режимах работы комплексов средств автоматизации.

Специфические требования к защите для различных уровней автоматизации обработки информации состоят в следующем:

- при автономном решении отдельных задач или их комплексов основными макропроцессами автоматизированной обработки, в ходе которых должен обеспечиваться необходимый уровень защиты, являются:
  - сбор, подготовка и ввод исходных данных, необходимых для решения задач;
  - машинное решение задач в автономном режиме;
  - выдача результатов решения;
- в случае полусистемной обработки дополнительно к предыдущему на участках комплексной автоматизации должна быть обеспечена защита в ходе осуществления следующих макропроцессов:
  - автоматизированного сбора информации от датчиков и источников информации;
  - диалогового режима работы пользователей ЭВМ;
- в случае системной обработки дополнительно к предыдущему должна быть обеспечена защита в ходе таких макропроцессов:
  - приема потока запросов и входной информации;
  - формирования пакетов и очередей запросов;

- диспетчеризации в ходе выполнения запросов;
- регулирования входного потока информации.

В зависимости от способа взаимодействия пользователя с комплексом средств автоматизации предъявляются следующие специфические требования:

- при автоматизированном вводе информации должны быть обеспечены условия, исключающие несанкционированное попадание информации одного пользователя (абонента) в массив другого, причем должны быть обеспечены возможности фиксирования и документального закрепления момента передачи информации пользователя банку данных автоматизированной системы обработки данных и содержания этой информации;
- при неавтоматизированном вводе должна быть обеспечена защита на неавтоматизированных коммуникациях «пользователь - автоматизированная система обработки данных», на участках подготовки данных и при вводе с местных устройствах группового ввода-вывода;
- при пакетном выполнении запросов пользователей должно исключаться размещение в одном и том же пакете запросов на обработку информации различных ограничительных грифов;
- при обработке запросов пользователей в реальном масштабе времени данные, поступившие от пользователей, и данные, подготовленные для выдачи пользователям, в ЗУ автоматизированной системы обработки данных должны группироваться с ограничительным грифом, при этом в каждой группе должен быть обеспечен уровень защиты, соответствующий ограничительному грифу данной группы.

В зависимости от режимов функционирования комплексов средств автоматизации предъявляются следующие специфические требования:

- в однопрограммном режиме работы в процессе выполнения программы должны предупреждаться:
  - несанкционированное обращение к программам;
  - несанкционированный ввод данных для решаемой задачи;
  - несанкционированное прерывание выполняемой программы;
  - несанкционированная выдача результатов решения;
- в мультипрограммном режиме сформулированные раньше требования относятся к каждой из выполняемых программ и дополнительно должно быть исключено несанкционированное использование данных одной программы другой программой;

- в мультипроцессорном режиме сформулированные выше требования должны обеспечиваться одновременно во всех участвующих в решении задачи процессорах, кроме того, должно быть исключено несанкционированное вклинивание в вычислительный процесс при распараллеливании и при диспетчеризации мультипроцессорного выполнения программ.

Требования, обусловливаемые этапом жизненного цикла автоматизированной системы обработки данных, формулируются так:

- на этапе создания автоматизированной системы обработки данных должно быть обеспечено соответствие возможностей защиты требованиям к защите информации, сформулированным в задании на проектирование, кроме того, должно быть исключено несанкционированное включение элементов (блоков) в компоненты автоматизированной системы обработки данных (особенно системы защиты);
- на этапе функционирования автоматизированной системы обработки данных в пассивном ее состоянии должна быть обеспечена надежная защита хранящейся информации и исключены возможности несанкционированных изменений компонентов системы;
- на этапе функционирования автоматизированной системы обработки данных в активном ее состоянии дополнительно к сформулированным раньше требованиям должна быть обеспечена надежная защита информации во всех режимах автоматизированной ее обработки.

Так могут быть представлены общие рекомендации по формированию требований к защите информации. Нетрудно видеть, что приведенные раньше требования хотя и содержат полезную информацию, но недостаточны для выбора методов и средств защиты информации в конкретной автоматизированной системе обработки данных.

Последовательность решения задачи должна быть следующей.

1. Разработка методов оценки параметров защищаемой информации.
2. Формирование перечня и классификация факторов, влияющих на требуемый уровень защиты информации.
3. Структуризация возможных значений факторов.
4. Структуризация поля потенциально возможных вариантов сочетаний значений факторов (вариантов условий защиты).
5. Оптимальное деление поля возможных вариантов на типовые классы.
6. Структурированное описание требований к защите в пределах выделенных классов.

Безопасность информации - это состояние
защищенности информации, обрабатываемой
средствами вычислительной техники
или автоматизированной системы,
от внутренних и внешних угроз.
*Руководящие документы ФСТЭК*

## 8. Анализ существующих методик определения требований к защите информации

Проблема определения требований к защите информации в автоматизированных системах ее обработки возникла практически одновременно с самой проблемой защиты, т. е. когда средства электронно-вычислительной техники (ЭВТ) стали применяться для обработки конфиденциальной информации. При этом оказалось, что для ее решения нет сколько-нибудь адекватного аналога, поскольку в условиях бумажной информатики вопросы защиты информации решались преимущественно организационными средствами. Система защиты строилась таким образом, чтобы возможности несанкционированного получения защищаемой информации практически были исключены. В условиях же автоматизированной обработки существует большое количество таких каналов несанкционированного получения информации, которые не могут быть перекрыты без применения специфических технических и программно-аппаратных средств. Соответственно возникла необходимость определения требований к системам защиты, содержащим указанные средства. Задача оказалась достаточно сложной, в силу чего регулярная методика ее решения до настоящего времени не разработана.

В сложившейся ситуации наиболее подходящим оказался подход, основанный на выделении некоторого количества типовых систем защиты с четким обозначением тех механизмов защиты, которые должна содержать каждая из типовых систем, и разработке рекомендаций по их использованию.

Для оценки реального состояния безопасности информационной системы применяются различные критерии. Анализ отечественного и зарубежного опыта показал определенную общность подхода к определению состояния безопасности в разных странах. Ее сущность состоит в следующем. Для предоставления пользователю возможности оценки вводится некоторая система показателей и задается иерархия классов безопасности. Каждому классу соответствует определенная совокупность обязательных функций. Степень реализации выбранных критериев показывает

текущее состояние безопасности. Последующие действия сводятся к сравнению реальных угроз с реальным состоянием безопасности.

Если реальное состояние перекрывает угрозы в полной мере, система безопасности считается надежной и не требует дополнительных мер. Такую систему можно отнести к классу систем с полным перекрытием угроз и каналов утечки информации. В противном случае система безопасности нуждается в дополнительных мерах защиты.

Показатель защищенности ИС - характеристика средств системы, влияющая на защищенность и описываемая определенной группой требований, варьируемых по уровню и глубине в зависимости от класса защищенности.

Рассмотрим некоторые подходы к оценке безопасности ИС.

## 8.1. Требования к безопасности информационных систем в США

Вопросами стандартизации и разработки нормативных требований на защиту информации в США занимается Национальный центр компьютерной безопасности Министерства обороны США (NCSC - National Computer Security Center).

Этот центр в 1983 г. издал «Критерии оценки безопасности компьютерных систем» (Trasted Computer Systems Evaluation Criteria - TCSEC). Этот документ часто называют «Оранжевой книгой». Данная разработка широко использовалась вплоть до принятия международного стандарта по безопасности информационных технологий ISO 15408. «Оранжевая книга» была утверждена в 1985 г. в качестве правительственного стандарта. Она содержит основные требования и специфицирует классы для оценки уровня безопасности компьютерных систем. Используя эти критерии, NCSC тестирует эффективность механизмов контроля безопасности. Следует подчеркнуть, что критерии делают безопасность величиной, допускающей ее измерение, и позволяют оценить уровень безопасности той или иной системы. Подобная возможность эмпирического анализа степени безопасности систем привела к международному признанию федерального стандарта США. NCSC считает безопасной систему, которая «посредством специальных механизмов защиты контролирует доступ к информации таким образом, что только имеющие соответствующие полномочия лица или процессы, выполняющиеся от их имени, могут получить доступ на чтение, запись, создание или удаление информации».

**Стандарт США «Критерии оценки гарантированно защищенных вычислительных систем в интересах Министерства обороны США».**

Наиболее известным документом, четко определяющим критерии, по которым должна оцениваться защищенность вычислительных систем, и те механизмы защиты, которые должны использоваться в системах обработки секретной конфиденциальной - в более общей постановке информации, является так называемая «Оранжевая книга», представляющая собой стандарт США «Критерии оценки гарантированно защищенных вычислительных систем в интересах Министерства обороны США» (Trusted Computer Systems Evaluation Criteria - TCSEC), принятый в 1983 г. Его принятию предшествовали 15-летние исследования, проводившиеся специально созданной рабочей группой и Национальным бюро стандартов США.

Стандартом предусмотрено 6 фундаментальных требований, которым должны удовлетворять те вычислительные системы, которые используются для обработки конфиденциальной информации. Требования разделены на три группы: стратегия, подотчетность, гарантии - в каждой группе по два требования следующего содержания:

**1. Стратегия**

**Требование 1** - стратегия обеспечения безопасности: необходимо иметь явную и хорошо определенную стратегию обеспечения безопасности.

**Требование 2** - маркировка: управляющие доступом метки должны быть связаны с объектами.

**2. Подотчетность**

**Требование 3** - идентификация: индивидуальные субъекты должны идентифицироваться.

**Требование 4** - подотчетность: контрольная информация должна храниться отдельно и защищаться так, чтобы со стороны ответственной за это группы имелась возможность отслеживать действия, влияющие на безопасность.

**3. Гарантии**

**Требование 5** - гарантии: вычислительная система в своем составе должна иметь аппаратные/программные механизмы, допускающие независимую оценку на предмет достаточного уровня гарантий того, что система обеспечивает выполнение изложенных выше требований с 1 -го по 4-е.

**Требование 6** - постоянная защита: гарантированно защищенные механизмы, реализующие перечисленные требования, должны быть постоянно защищены от «взламывания» и/или несанкционированного внесения изменений.

В зависимости от конкретных значений, которым отвечают автоматизированные системы, они разделены на 4 группы - D, C, B, A, которые названы так:

- **D** - минимальная защита;
- **C** - индивидуальная защита;
- **B** - мандатная защита;
- **A** - верифицированная защита.

Группы систем делятся на классы, причем все системы, относимые к группе D, образуют один класс D, к группе C - два класса C1 и C2, к группе B - три класса B1, B2 и B3, к группе A - один класс A1 с выделением части систем вне класса.

Ниже рассмотрим названия и краткую характеристику перечисленных классов.

- **D** - минимальная защита - системы, подвергнутые оцениванию, но не отвечающие требованиям более высоких классов.
- **C1** - защита, основанная на индивидуальных мерах, - системы, обеспечивающие разделение пользователей и данных. Они содержат внушающие доверие средства, способные реализовать ограничения по доступу, накладываемые на индивидуальной основе, т. е. позволяющие пользователям иметь надежную защиту их информации и не дающие другим пользователям считывать или разрушать их данные. Допускается кооперирование пользователей по уровням секретности.
- **C2** - защита, основанная на управляемом доступе, - системы, осуществляющие не только разделение пользователей, как в системах C1, но и разделение их по осуществляемым действиям.
- **B1** - защита, основанная на присваивании имен отдельным средствам безопасности, - системы, располагающие всеми возможностями систем класса C, и дополнительно должны быть формальные модели механизмов обеспечения безопасности, присваивания имен защищаемым данным, включая и выдаваемые за пределы системы, и средства мандатного управления доступом ко всем поименованным субъектам и объектам.
- **B2** - структурированная защита - системы, построенные на основе ясно определенной и формально задокументированной модели, с мандатным управлением доступом ко всем субъектам и объектам, располагающие усиленными средствами тестирования и средствами управления со стороны администратора системы.

- **B3** - домены безопасности - системы, монитор обращений которых контролирует все запросы на доступ субъектов к объектам, не допускающие несанкционированных изменений. Объем монитора должен быть небольшим вместе с тем, чтобы его состояние и работу можно было сравнительно легко контролировать и тестировать. Кроме того, должны быть предусмотрены сигнализация о всех попытках несанкционированных действий и восстановление работоспособности системы.
- **A1** - верификационный проект - системы, функционально эквивалентные системам класса B3, но верификация которых осуществлена строго формальными методами. Управление системой осуществляется по строго определенным процедурам. Обязательно введение администратора безопасности.

Эти основные требования конкретизируются в показателях защищенности, которые приведены в табл. 2.13.

*Таблица 2.13. Показатели защищенности ИС на основе технологии IBM*

| *Показатель защищенности* | *A1* | *B3* | *B2* | *B1* | *C2* | *C1* | *Наименование подгруппы показателей* |
|---|---|---|---|---|---|---|---|
| Избирательная политика безопасности | | | | | + | + | Политика безопасности |
| Полномочная политика безопасности | | | | | + | | |
| Повторное использование объектов | | | | | | | |
| Изоляция модулей | | | | | | | |
| Маркировка документов | | | | | | | |
| Защита ввода и вывода на отчуждаемый физический носитель информации | | | | | | | |
| Сопоставление пользователя с устройством | | | | | | | |
| Избирательный контроль доступа | | | | | | | |
| Мандатный контроль доступа | | | | | | | |
| Указатели метки | | | | | | | |
| Указатели целостности | | | | | | | |

*Окончание табл. 2.13*

| *Показатель защищенности* | *A1* | *B3* | *B2* | *B1* | *C2* | *C1* | *Наименование подгруппы показателей* |
|---|---|---|---|---|---|---|---|
| Идентификация и аутентификация | | | | | + | + | Статистика |
| Регистрация | | | | | + | | |
| Взаимодействие пользователя с комплексом средств защиты (КСЗ) | | | | | | | |
| Гарантии проектирования | | | | | + | + | Гарантии |
| Гарантии архитектуры | | | | | | + | |
| Надежное восстановление | | | | | + | + | |
| Целостность КСЗ | | | | | | | |
| Контроль модификации | | | | | | | |
| Контроль дистрибуции | | | | | | | |
| Тестирование | | | | | | | |
| Контроль полномочий | | | | | | | Документация |
| Контроль безопасности | | | | | | | |
| Руководство пользователя по безопасности | | | | | | + | |
| Инструкция по КСЗ | | | | | + | + | |
| Тестовая документация | | | | | | + | |
| Конструкторская документация | | | | | | + | |

*Примечание.* Ниже дано пояснение применяемых обозначений.

| | |
|---|---|
| | Не соответствует требованиям, предъявляемым к этому классу |
| | Нет дополнительных требований к этому классу |
| | Нет требований к этому классу |
| + | Соответствует или превышает требования к этому классу |

Разработаны также основные требования к проектной документации.

В части стандартизации аппаратных средств информационных систем и телекоммуникационных сетей в США разработаны правила стандарта Transient Electromagnetic Pulse Emanations Standart (TEMPEST).

Этот стандарт предусматривает применение специальных мер защиты аппаратуры от паразитных излучений электромагнитной энергии, перехват которой может привести к овладению охраняемыми сведениями.

Стандарт TEMPEST обеспечивает радиус контролируемой зоны перехвата порядка 1 м. Это достигается специальными схемотехническими, конструктивными и программно-аппаратными решениями, в том числе:

- применением специальной низкопотребляющей малошумящей элементной базы;
- специальным конструктивным исполнением плат и разводкой сигнальных и земляных электрических цепей;
- использованием экранов и RC-фильтров, ограничивающих спектры сигналов в цепях интерфейсных соединений;
- применением специальных мер, обеспечивающих защиту от НСД (съемный жесткий диск, магнитные парольные карты, специальные замковые устройства, программно-аппаратные средства защиты информации и шифрования).

Снижение мощности побочных электромагнитных излучений и наводок (ПЭМИН) монитора достигается рядом конструктивно-технологических решений, примененных в ПЭВМ:

- видеомонитор с задней стороны полностью заключен в металлический экран;
- плата видеоусилителей видеомонитора заключена в дополнительный экран;
- на соединительные кабели видеомонитора установлены ферритовые фильтры;
- сигнальные цепи выполнены экранированным кабелем;
- сигналы на интерфейсные разъемы системного блока подаются через LC-фильтры, ограничивающие спектр сигналов сверху;
- корпус системного блока металлический с токопроводящим покрытием, что обусловливает достаточную локализацию ПЭМИН.

*Таблица 2.14. Основные требования к проектной документации (приводятся частично)*

| *Описание техническая характеристика защиты* | *Класс защищенности* | | | | | |
|---|---|---|---|---|---|---|
| | *C1* | *C2* | *B1* | *B2* | *B3* | *A1* |
| Концепция защиты | + | + | + | + | + | + |
| Каким образом концепция защиты реализуется в ТСВ* | + | + | + | + | + | + |
| Модульный принцип ТСВ, если принцип модульный | + | + | + | | | |

*Продолжение табл. 2.14*

| *Описание техническая характеристика защиты* | *Класс защищенности* | | | | | |
|---|---|---|---|---|---|---|
| | *C1* | *C2* | *B1* | *B2* | *B3* | *A1* |
| Устройства сопряжения между модулями ТСВ, если принцип модульный | | | | | | |
| Какова защита самого ТСВ | + | + | + | | | |
| Предписание оператор концепции защиты системы | + | + | + | + | + | + |
| Модель концепции защиты системы | | | + | + | + | + |
| Аргументация достаточности модели концепции защиты в целях усиления этой концепции | | | + | + | + | + |
| Идентифицирование механизмов защиты ТСВ | | | + | + | + | + |
| Аргументация соответствия механизмов ТСВ модели концепции защиты системы | | | + | + | + | + |
| Модульный принцип ТСВ | | | | + | + | + |
| Устройства сопряжения между модулями ТСВ | | | | + | + | + |
| Формальная внешняя модель концепции защиты | | | | + | + | + |
| Аргументация достаточности модели концепции защиты для ее усиления | | | | + | + | + |
| Схематическое отображение технических требований высшего уровня, изложенных в описательной форме, в устройстве сопряжения ТСВ | | | | + | + | + |
| Каким образом ТСВ обеспечивает выполнение концепции обращения к монитору управляющей программы | | | | + | + | + |
| Почему ТСВ является препятствием для вмешательства самовольного изменения процессов в систему | | | | + | + | + |
| Почему ТСВ нельзя обойти | | | | + | + | + |
| Почему ТСВ обеспечивает правильное выполнение задач | | | | + | + | + |
| Какова структура ТСВ, которая способствует контрольному испытанию системы защиты | | | | + | + | + |

*Окончание табл. 2.14*

| *Описание техническая характеристика защиты* | *Класс защищенности* | | | | | |
|---|---|---|---|---|---|---|
| | *C1* | *C2* | *B1* | *B2* | *B3* | *A1* |
| Какова структура TCB, которая способствует усилению минимальных преимуществ | | | | + | + | + |
| Результаты анализа защищенных каналов | | | | + | + | + |
| Альтернативные варианты | | | | + | + | + |
| Результаты проверки, которые можно использовать при эксплуатации известных защитных каналов ЗУ | | | | + | + | + |

* TCB (Trusted computer base) - доверенная вычислительная среда

## 8.2. Требования к безопасности информационных систем в России

Аналогичный подход реализован и в руководящем документе Государственной технической комиссией при Президенте РФ «Классификация автоматизированных систем и требований по защите информации», выпущенном в 1992 г. Требования всех приведенных ниже документов обязательны для исполнения только для тех государственных либо коммерческих организаций, которые обрабатывают информацию, содержащую государственную тайну. Для остальных коммерческих структур документы носят рекомендательный характер. В данном документе выделено 9 классов защищенности автоматизированных систем от несанкционированного доступа к информации, а для каждого класса определен минимальный состав необходимых механизмов защиты и требования к содержанию защитных функций каждого из механизмов в каждом из классов систем.

Классы систем разделены на три группы, причем основным критерием деления на группы приняты специфические особенности обработки информации, а именно:

третья группа - системы, в которых работает один пользователь, допущенный ко всей обрабатываемой информации, размещенной на носителях одного уровня конфиденциальности; к группе отнесены два класса, обозначенные 3Б и 3А;

вторая группа - системы, в которых работает несколько пользователей, которые имеют одинаковые права доступа ко всей информации, об-

рабатываемой и/или хранимой на носителях различного уровня конфиденциальности; к группе отнесены два класса, обозначенные 2Б и 2А;

первая группа - многопользовательские системы, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности, причем различные пользователи имеют разные права на доступ к информации; к группе отнесено 5 классов: 1Д, 1Г, 1В, 1Б и 1А.

Требования к защите растут от систем класса 3Б к классу 1 А.

Все механизмы защиты разделены на 4 подсистемы следующего назначения:

- управления доступом;
- регистрации и учета;
- криптографического закрытия;
- обеспечения целостности.

Состав перечисленных подсистем приведен в табл. 2.15.

*Таблица 2.15. Классы подсистем защищенности*

| *Подсистема и ее характеристики* | *Классы систем* | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | *3Б* | *3А* | *2Б* | *2А* | *1Д* | *1Г* | *1В* | *1Б* | *1А* |
| 1. Подсистема управления доступом | + | + | + | + | + | + | + | + | + |
| 1.1. Идентификация, проверка подлинности и контроль доступа субъектов в систему: к терминалам, ЭВМ, каналам связи, внешним устройствам ЭВМ | - | - | - | + | - | + | + | + | + |
| к томам, каталогам, файлам, записям, полям записей | - | - | - | + | - | + | + | + | + |
| 1.2. Управление потоками информации | - | - | - | + | - | + | + | + | + |
| 2. Подсистема регистрации и учета | + | + | + | + | + | + | + | + | + |
| 2.1. Регистрация и учет: входа субъектов доступа в системы узла сети и выхода их из нее | - | | - | | - | | | | |
| выдачи печатных графических выходных документов | | + | | + | | + | + | + | + |

*Продолжение табл. 2.15*

| *Подсистема и ее характеристики* | *Классы систем* | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | *3Б* | *3А* | *2Б* | *2А* | *1Д* | *1Г* | *1В* | *1Б* | *1А* |
| запуска-завершения программ процессов заданий, задач | - | - | - | + | - | + | + | + | + |
| доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи; | - | - | - | + | - | + | + | + | + |
| доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей; | - | - | - | + | - | + | + | + | + |
| изменения полномочий субъектов доступа | - | - | - | - | - | + | + | + | + |
| создаваемых защищаемых объектов доступа | - | - | - | + | - | - | + | + | + |
| 2.2. Учет носителей информации | + | + | + | + | + | + | + | + | + |
| 2.3. Очистка, обнуление, обезличивание освобождаемых областей оперативной памяти ЭВМ и внешних накопителей | - | + | - | + | - | + | + | + | + |
| 3. Криптографическая подсистема | + | + | + | + | + | + | + | + | + |
| 3.1. Шифрование конфиденциальной информации | + | + | + | + | + | + | + | + | + |
| 3.2. Шифрование информации, принадлежащей различным субъектам доступа, группам субъектов на различных ключах | - | - | - | - | - | - | - | - | + |
| 3.3. Использование аттестованных сертифицированных криптографических средств | - | - | - | + | - | - | - | + | + |

*Окончание табл. 2.15*

| *Подсистема и ее характеристики* | *Классы систем* | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | *3Б* | *3А* | *2Б* | *2А* | *1Д* | *1Г* | *1В* | *1Б* | *1А* |
| 4. Подсистема обеспечения целостности | + | + | + | + | + | + | + | + | + |
| 4.1. Обеспечение целостности программных средств и обрабатываемой информации | + | + | + | + | + | + | + | + | + |
| 4.2. Физическая охрана средств вычислительной техники и носителей информации | + | + | + | + | + | + | + | + | + |
| 4.3. Наличие администратора службы защиты информации в автоматизированной системе обработки данных | - | - | - | + | - | - | + | + | + |
| 4.4. Периодическое тестирование средств защиты информации несанкционированного доступа | + | + | + | + | + | + | + | + | + |
| 4.5. Наличие средств восстановления средств защиты информации несанкционированного доступа | + | + | + | + | + | + | + | + | + |
| 4.6. Использование сертифицированных средств защиты | - | + | - | + | - | - | + | + | + |

Содержание средств для каждой группы систем приведено в документе. Приведенная в руководящем документе Гостехкомиссии методика распространяется на защиту от несанкционированного доступа к информации, находящейся непосредственно в ЗУ ЭВМ и на сменных машиночитаемых носителях. Значительно раньше, в 1978 г., Гостехкомиссией были выпущены руководящие документы, определяющие требования к защите информации в автоматизированных системах от утечки по побочным электромагнитным излучениям и наводкам. При разработке названных требований учитывались следующие факторы:

1. Доля грифованной информации в общем объеме обрабатываемой информации.
2. Интенсивность обработки грифованной информации, выражаемая относительной долей времени ее обработки в течение суток.
3. Условия расположения аппаратуры автоматизированной системы.

Наличие рассмотренных методик и закрепление их в официальных документах создает достаточно надежную базу для защиты информации на регулярной основе. Однако нетрудно видеть, что с точки зрения современной постановки задачи защиты информации имеющиеся методики являются недостаточными по ряду причин, а именно:

1) методики ориентированы на защиту информации только в средствах ЭВТ, в то время как имеет место устойчивая тенденция органического сращивания автоматизированных и традиционных технологий обработки информации;
2) учитываются далеко не все факторы, оказывающие существенное влияние на уязвимость информации, а поэтому и подлежащие учету при определении требований к защите;
3) в научном плане они обоснованы недостаточно за исключением требований к защите информации от утечки по техническим каналам.

## 8.3. Классы защищенности средств вычислительной техники от несанкционированного доступа

В ч. 2 руководящих документах Гостехкомиссии устанавливается классификация средств вычислительной техники (СВТ) по уровню защищенности от несанкционированного доступа к информации на базе перечня показателей защищенности и совокупности описывающих их требований. Под средствами вычислительной техники понимаются совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Показатели защищенности содержат требования по защите СВТ от несанкционированного доступа к информации и применяются к общесистемным программным средствам и операционным системам с учетом архитектуры компьютера. Классы защищенности СВТ описываются совокупностью требований. Совокупность всех средств защиты составляет комплекс средств защиты.

Изложенные ниже требования к показателям защищенности предъявляются к общесистемным программным средствам и операционным системам.

В зависимости от реализованных моделей защиты и надежности их проверки классы подразделяются на 4 группы. Первая группа включает только один седьмой класс - минимальная защищенность.

Вторая группа характеризуется избирательной защитой и включает шестой и пятый классы. Избирательная защита предусматривает кон-

троль доступа поименованных субъектов к поименованным объектам системы. При этом для каждой пары «субъект - объект» должны быть определены разрешенные типы доступа. Контроль доступа применяется к каждому объекту и к каждому субъекту - индивиду или группе равноправных индивидов.

Третья группа характеризуется полномочной защитой и включает четвертый, третий и второй классы. Полномочная защита предусматривает присвоение каждому субъекту и объекту системы классификационных меток, указывающих место субъекта объекта в соответствующей иерархии. Классификационные метки на объекты устанавливаются пользователем системы или специально выделенным субъектом. Обязательным требованием для классов, входящих в эту группу, является реализация диспетчера доступа в иностранной литературе - reference monitor, монитор ссылок. Контроль доступа должен осуществляться применительно ко всем объектам при явном и скрытом доступе со стороны любого из субъектов. Решение о санкционированности запроса на доступ должно приниматься только при одновременном разрешении его и избирательными и полномочными правилами разграничения доступа.

Четвертая группа характеризуется верифицированной защитой и содержит только первый класс.

Для присвоения класса защищенности система должна иметь:

- руководство администратора по системе;
- руководство пользователя;
- тестовую и конструкторскую документацию.

Перечень показателей по классам защищенности СВТ приведен в табл. 2.16.

*Таблица 2.16. Показатели защищенности СВТ от НСД*

| *Показатель защищенности* | *6* | *5* | *4* | *3* | *2* | *1* |
|---|---|---|---|---|---|---|
| Дискреционный принцип контроля доступа | + | + | + | = | + | = |
| Мандатный принцип контроля доступа | - | - | + | = | = | = |
| Очистка памяти | - | + | + | + | = | = |
| Изоляция модулей | - | - | + | = | + | = |
| Маркировка документов | - | - | + | = | = | = |
| Защита ввода и вывода на отчуждаемый физический носитель информации | - | - | + | = | = | = |
| Сопоставление пользователя с устройством | - | - | + | = | = | = |
| Идентификация и аутентификация | + | = | + | = | = | = |

*Окончание табл. 2.16*

| *Показатель защищенности* | *6* | *5* | *4* | *3* | *2* | *1* |
|---|---|---|---|---|---|---|
| Гарантии проектирования | - | + | + | + | + | + |
| Регистрация | - | + | + | + | - | = |
| Взаимодействие пользователя с комплексом средств защиты (КСЗ) | - | - | - | + | = | = |
| Надежное восстановление | - | - | - | + | = | = |
| Целостность КСЗ | - | + | + | + | = | = |
| Контроль модификации | - | - | - | - | + | = |
| Контроль дистрибуции | - | - | - | - | + | = |
| Гарантии архитектуры | - | - | - | - | - | + |
| Тестирование | + | + | + | + | + | = |
| Руководство пользователя | + | = | = | = | = | = |
| Руководство по КСЗ | + | + | = | + | + | = |
| Текстовая документация | + | + | + | + | + | = |
| Конструкция проектная документация | + | + | + | + | + | + |

*Примечание.* «-» - нет требований к данному классу; «+» - новые или дополнительные требования; «=» - требования совпадают с требованиями к СВТ предыдущего класса.

В данном документе к каждому требованию приведены подробные развернутые комментарии.

В качестве примера рассмотрим требования к подсистеме обеспечения целостности класса 2А.

- Должна быть обеспечена целостность программных средств системы защиты информации (СЗИ) от несанкционированного доступа НСД, целостность обрабатываемой информации, а также неизменность программной среды. При этом:
  - целесообразность СЗИ НСД проверяется при загрузке системы по наличию имен идентификаторов компонентов СЗИ;
  - целостность программной среды обеспечивается отсутствием в системе средств разработки и отладки программ;
- Должна осуществляться физическая охрана средств устройств и носителей информации, предусматривающая постоянное наличие охраны территории и здания, где размещается система, с помощью технических средств охраны и специального персонала, использование строгого пропускного режима, специальное оборудование помещений.

- Должен быть предусмотрен администратор служба защиты информации, ответственный за ведение, нормальное функционирование и контроль работы СЗИ НСД.
- Должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала системы с помощью тест-программ, имитирующих попытки НСД.
- Должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности.
- Должны использоваться сертифицированные средства защиты.

Тщательный анализ таких требований позволит оценить реальную безопасность ИС с отнесением ее к определенному классу защищенности.

Методика оценки безопасности и США и России практически ориентированы на оценку безопасности на качественном уровне.

Определенный интерес для читателей представит опыт французских исследователей по оценке безопасности ИС с использованием некоторых количественных нормативов, что для практического применения более конкретно и обозримо.

Класс защищенности ИС - определенная совокупность требований по защите средств ИС от НСД к информации.

## 8.4. Оценка состояния безопасности ИС Франции

Были опубликованы результаты нескольких опросов оценки уровня безопасности предприятий. Опросная анкета содержала 27 характерных факторов безопасности ИС (табл. 2.17) и была распространена на 172 предприятиях: 73 в секторе I - банки, страховые общества, финансовые органы; 54 в секторе II - промышленность, сельское хозяйство, энергетика и 45 в секторе III - транспорт, торговля, сфера услуг и др. [34].

*Таблица 2.17. Факторы безопасности ИС Франции*

| *Код* | *Содержание* | *Сфера безопасности* |
|---|---|---|
| 101 | Общая организация | Общая организация безопасности |
| 102 | Постоянные виды контроля | |
| 103 | Регламентация и аудит | |
| 201 | Социально-экономические факторы | Социально-экономическая безопасность |

*Окончание табл. 2.17*

| *Код* | *Содержание* | *Сфера безопасности* |
|---|---|---|
| 301 | Внешняя окружающая среда | Физическая безопасность |
| 302 | Контроль доступа | |
| 303 | Загрязнение | |
| 304 | Правила безопасности | |
| 305 | Противопожарная безопасность | |
| 306 | Защита от подтопления | |
| 307 | Безопасность функционирования информационной техники | |
| 308 | Средства восстановления и резервирования | Организационная безопасность |
| 309 | Протоколы обмена | |
| 310 | Подготовка персонала | |
| 311 | Планирование безопасности | |
| 401 | Безопасность оборудования и баз данных | Логическая, телекоммуникационная и эксплуатационная безопасность |
| 402 | Безопасность телекоммуникаций | |
| 403 | Защита данных | |
| 501 | Архивация/дезархивация | Функциональная безопасность |
| 502 | Получение и передача данных | |
| 503 | Охрана | |
| 504 | Надежность функционирования | |
| 505 | Обеспечение | |
| 601 | Процедуры проверки | Управление безопасностью |
| 602 | Методики контроля | |
| 603 | Взаимосвязь методов контроля | |
| 604 | Программно-математическая безопасность | |

Общие факторы связаны с организацией предприятия *101, 102, 103, 201.* Социально-экономические факторы *201* остаются довольно благоприятными. Различия в показателях других факторов значительные. Наиболее слабой остается общая организация безопасности *101* - структура ответственных участков, правовая и страховая защита. Самые низкие показатели в секторе I: сложность финансовых механизмов значительно затрудняет реализацию мер обеспечения безопасности. Постоянные виды контроля *102* имеют высокие показатели. Регламентация и аудит *103* имеют средние показатели.

Физическая безопасность *301, 302, 303, 304, 305, 306, 307.* Традиционно противопожарная безопасность *304* и *305* находится на довольно высоком уровне, в то время как защита от подтопления *306* недостаточна. Отмечается слабость безопасности внешней зоны и зданий *301,* хотя они представляют собой первый рубеж безопасности предприятия. Контроль доступа, пропускной режим также недостаточен, особенно в промышленности.

Защита информации от искажений *303* тоже недостаточна. Наконец, безопасность оборудования внешней среды *307* только на среднем уровне: довольно хорошая для сектора I и весьма низкая для сектора II.

Организационная безопасность *308, 309, 310, 401, 402, 403, 501, 502, 503, 504, 505.*

Средства восстановления и резервирования *308* медленно совершенствуются для больших и средних машин. Безопасность коммуникаций *402* и данных *403* неодинакова: в большей степени аппаратура, средства, но недостаточно взаимоувязаны. Защита *503* всегда на должном уровне только против саботажа в нематериальной среде.

Управление безопасностью *601, 602, 603, 604.* Процедуры контроля *601* слишком просты. Методики *602* являются часто формальными, обеспечены аппаратурой и необходимой документацией; не увязаны с принципом «безопасность - надежность». Мероприятия *603* и *604* пока еще слабо реализуются из-за недостаточной взаимоувязки и не соответствуют затратам.

Саботаж в нематериальной сфере весьма распространен, начиная с фальсификации программ и данных до тотального саботажа путем применения логических бомб и различных вирусов. Этот вид угроз отмечается во всех обследованных центрах. Убытки главным образом касаются уничтожения содержания и формы данных, потери целостности, программ и документов.

В основном эти угрозы направлена на дезорганизацию защиты: атаки на операционную систему, модификация данных, изменение языка управления данными, стирание данных на магнитных носителях и др. Действия совершает в основном в вычислительных центрах внутренний персонал, а иногда наблюдаются и вне ВЦ пиратские действия в сети теледоступа.

Физические угрозы определяются как конфигурацией, так и расположением зданий и осложняются их рассредоточением, делением помещений на отдельные кабинеты, рассредоточением средств пожаротушения и защиты. Меры по восстановлению зависят от наличия резерва.

Что касается угроз внешней среды, то она является физически опасной в части необходимости создания искусственного климата и защиты

электросетей. Последствия в основном ограниченные, однако часто отмечаются довольно значительные задержки в возобновлении снабжения некоторыми материалами, в особенности для электрооборудования большой мощности, использующего необычные электрические частоты.

Угрозы телекоммуникационным средствам касаются внутреннего телекоммуникационного оборудования: распределительных щитов, кабелей, автоматических коммутаторов, соединительных коробок, концентраторов, контроллеров линий связи, модемов и т. д. Серьезную опасность представляет выход из строя узлов связи. Отмечен максимальный перерыв в связи до трех недель. Восстановление определяется возможностями переключения на другие центры, наличием резервных линий и средств.

**Забастовки.** Отмечен случай, когда эксплуатационный персонал не имел возможности доступа в центр в течение двух недель. Нанесенный ущерб находится в прямой зависимости от времени.

Уход ведущих специалистов по эксплуатации сетей, управлению данными, безопасностью и т. д. особенно опасен для малых центров. Самый серьезный случай - уход руководителей проектов или соответствующих функционеров, которые аккумулируют уникальные знания и практический опыт.

**Хищения.** Имеются многочисленные сценарии и разнообразные формы; нередко обычны для информатики манипуляция с библиотекой данных, программами, управлением заданиями, изменение системы, подключение к сети и т. д., но значительная часть нарушений довольно неординарного характера: неправомерное обслуживание или незаконная эксплуатация, мошенничество в отношении логического или программного контроля и т. д. Основа сценариев мошенничества находится на уровне практического применения, и преступниками являются в первую очередь сотрудники предприятия или пользователи. Случаи хищения информации также разнообразны: часто простые листинги, магнитные носители, запросы с экрана, узурпация права доступа и т. д., а иногда более сложные - сетевые. Они относятся в первую очередь к предприятиям с высокой технологией, распределительным организациям, биржевой деятельности, организациям-экспортерам и многим видам специфической деятельности во всех секторах.

Нарушение конфиденциальности, случаи пиратства отмечаются только тогда, когда программный продукт представляет собой «секрет производства» или если предприятие является его владельцем, автором.

**Ошибки.** Они весьма разнообразны и многочисленны. Часто совершаются злонамеренно. Среди них ошибки хранения и передачи данных,

а также программ, ошибки интерпретации или использования, концептуальные ошибки или ошибки реализации, функциональные или эксплуатационные ошибки.

**Аварии.** Что касается аварий оборудования или основных элементов системы, то они являются малораспространенными и определяются надежностью аппаратуры. При выходе ее из строя продолжительность простоя может оказаться довольно значительной. Внешние аварии электрических сетей и водоснабжения являются более серьезными и более продолжительными. Они могут иметь внутреннее происхождение, но самые серьезные из них обусловлены внешними причинами. Восстановление зависит от автономности средств группы электропитания, резервов топлива и воды для электросети и водоснабжения и т. д.

Что касается посягательств, то их последствия в среднем одинаковы или более слабы, чем для стихийных бедствий, за исключением случаев, когда несколько преступников одновременно атакуют различные жизненно важные точки.

Кражи материальных ценностей. Воруют ПЭВМ, печатающие устройства, телексы, факсы, мультиплексоры, аппаратуру контроля и измерения и другие элементы и материалы.

Основу ущерба составляют материальные потери и в значительной части потери информационных материалов, хранящихся на жестких магнитных дисках.

Результаты опроса о величине нанесенного ущерба представлены в табл. 2.18. Убытки являются весьма значительными, и можно удивляться тому, что угрозы, случаясь редко, не бывают сразу, одновременно. Это ослабляет их удары.

*Таблица 2.18. Материальные убытки по видам угроз, млн. франков*

| *Ранг* | *Вид угрозы* | *Средняя сумма* | *Максимальная сумма* |
|---|---|---|---|
| 1 | Тотальный саботаж в нематериальной сфере | 422 | 3 000 |
| 2 | Хищение, мошенничество | 319 | 25 000 |
| 3 | Физическая угроза | 189 | 1 000 |
| 4 | Угроза конфиденциальности | 68 | 800 |
| 5 | Забастовки | 56 | 900 |
| 6 | Внешняя среда | 48 | 300 |
| 7 | Телекоммуникации | 22 | 120 |
| 8 | Концептуальные ошибки | 9 | 15 |

*Окончание табл. 2.18*

| *Ранг* | *Вид угрозы* | *Средняя сумма* | *Максимальная сумма* |
|---|---|---|---|
| 9 | Ошибки хранения | 7 | 10 |
| 10 | Ошибки эксплуатации | 7 | 10 |
| 11 | Аварии оборудования | 7 | 35 |
| 12 | Ошибки передачи | 6 | 12 |
| 13 | Внешние аварии | 3 | 5 |
| 14 | Уход персонала | 2 | 5 |
| 15 | Кража материальных ценностей | 1 | 5 |

Большинство крупных предприятий подвергаются риску, превышающему 1 млрд. фр. Уровень риска большинства из них, как правило, превышает их возможности в случаях неожиданных ситуаций.

### *8.4.1. Состояние безопасности малых информационных систем*

Результаты анкетирования состояния безопасности малых информационных систем приведены в табл. 2.19.

*Таблица 2.19. Результаты анкетирования состояния безопасности малых информационных систем, %*

| *Код* | *Факторы* | *Секторы* | | | | | |
|---|---|---|---|---|---|---|---|
| | | *финансовый* | | *промышленный* | | *услуг* | |
| | | *да* | *нет* | *да* | *нет* | *да* | *нет* |
| 01 | Уровень организации безопасности | 75,2 | 24,2 | 73,9 | 26,1 | 82,5 | 17,502 |
| 02 | Меры доверия | 81,8 | 18,2 | 78,3 | 21,7 | 55,0 | 45,0 |
| 03 | Определение владельцев информации и классификация | 21,2 | 78,8 | 39,3 | 60,7 | 42,5 | 57,5 |
| 04 | Внутренний аудит | 60,6 | 39,4 | 43,5 | 56,5 | 63,0 | 37,0 |
| 05 | Внешний аудит | 48,5 | 51,5 | 39,1 | 60,9 | 15,0 | 85,0 |
| 06 | Безопасность зданий | 54,5 | 45,5 | 47,8 | 52,2 | 67,5 | 32,5 |
| 07 | Безопасность вспомогательных служб | 30,3 | 69,7 | 34,8 | 65,2 | 17,5 | 82,5 |
| 08 | Физические системы контроля доступа | 93,9 | 6,1 | 78,2 | 21,7 | 90,0 | 10,0 |
| 09 | Биометрические системы контроля доступа | 0,0 | 100,0 | 0,0 | 100,0 | 0,0 | 100,0 |

*Окончание табл. 2.19*

| Код | Факторы | Секторы | | | | | |
|---|---|---|---|---|---|---|---|
| | | финансовый | | промышленный | | услуг | |
| | | да | нет | да | нет | да | нет |
| 10 | Обеспечение чистоты воздуха | 18,2 | 81,8 | 8,7 | 91,3 | 5,0 | 95,0 |
| 11 | Инструкции по безопасности | 66,7 | 33,3 | 60,9 | 39,1 | 85,0 | 10,0 |
| 12 | Автоматическое тушение пожара | 90,9 | 9,1 | 82,6 | 17,4 | 57,5 | 42,5 |
| 13 | Система охраны | 87,9 | 12,1 | 52,2 | 47,8 | 75,0 | 25,0 |
| 14 | Эвакуация | 81,8 | 18,2 | 47,8 | 52,2 | 70,0 | 30,0 |
| 15 | Резервное электропитание | 81,8 | 18,2 | 39,1 | 60,9 | 60,0 | 40,0 |
| 16 | Оказание помощи | 54,5 | 45,5 | 56,5 | 43,5 | 67,5 | 32,5 |
| 17 | Логический контроль доступа | 75,8 | 24,2 | 65,1 | 34,8 | 75,0 | 25,0 |
| 18 | Безопасность сети | 51,5 | 48,5 | 60,9 | 39,1 | 60,0 | 40,0 |
| 19 | Шифрование | 24,2 | 75,8 | 4,3 | 95,7 | 5,0 | 95,0 |
| 20 | Аудит | 63,6 | 39,4 | 65,2 | 34,8 | 62,5 | 37,5 |
| 21 | Безопасность носителей | 33,3 | 66,7 | 21,7 | 78,3 | 37,5 | 62,5 |
| 22 | Внешняя защита | 93,9 | 6,1 | 91,3 | 8,7 | 85,0 | 15,0 |
| 23 | Борьба с саботажем в нематериальной сфере | 12,1 | 87,9 | 17,4 | 82,6 | 0,0 | 100,0 |
| 24 | Непрерывность и целенаправленность эксплуатации | 70,8 | 29,2 | 62,5 | 37,5 | 40,0 | 60,0 |
| 25 | Надежность эксплуатации | 63,6 | 36,4 | 60,9 | 39,1 | 70,0 | 30,0 |
| 26 | Использование защищенной аппаратуры | 21,2 | 78,8 | 30,4 | 69,6 | 25,0 | 75,0 |
| 27 | Спецификация безопасности | 30,3 | 69,7 | 30,4 | 69,6 | 0,0 | 100,0 |
| 28 | Состояние контроля | 27,3 | 72,7 | 56,5 | 43,5 | 65,0 | 35,0 |
| 29 | Взаимоувязка мер контроля | 57,6 | 42,4 | 73,9 | 26,1 | 67,5 | 32,5 |
| 30 | Аутентификация | 63,6 | 36,4 | 60,9 | 39,1 | 75,0 | 25,0 |

Результаты опроса и анализа безопасности ПК еще более тревожные (табл. 2.20).

*Таблица 2.20. Котировка факторов*

| *№ фактора* | *Факторы* | *Котировка* |
|---|---|---|
| *Организационная и экономическая среда* | | |
| 101 | Общая организация | 1,70 |
| 102 | Виды контроля | 1,75 |
| 103 | Регламентация и аудит | 1,90 |
| 201 | Социально-экономические | 2,78 |
| *Физическая безопасность* | | |
| 301 | Внешняя окружающая среда | 2,75 |
| 302 | Контроль доступа | 1,82 |
| 303 | Загрязнение | 1,64 |
| 304 | Правила безопасности | 1,87 |
| 305 | Противопожарная безопасность | 2,49 |
| 306 | Защита от затопления | 2,30 |
| 307 | Безопасность работы информац. техники | 2,56 |
| *Общая информационная безопасность* | | |
| 308 | Средства резервирования и восстановления | 2,25 |
| 309 | Протоколы обмена | 2,84 |
| 310 | Подготовка персонала | 1,11 |
| 311 | Планирование безопасности | 1,21 |
| 401 | Безопасность оборудования и базового программного обеспечения | 1,58 |
| 402 | Телекоммуникационная безопасность | 1,83 |
| 403 | Защита данных | 0,65 |
| *Эксплуатационная безопасность* | | |
| 501 | Архивация/дезархивация | 1,62 |
| 502 | Прием и передача данных | 1,28 |
| 503 | Охрана | 1,28 |
| 504 | Надежность функционирования | 1,10 |
| 505 | Обеспечение | 2,67 |
| *Функциональная безопасность* | | |
| 601 | Процедуры проверки | 0,59 |
| 602 | Программные методы контроля | 1,57 |
| 603 | Взаимосвязь методов контроля | 1,57 |
| 604 | Программно-математическая безопасность | 2,46 |

Безопасность ПК чрезвычайно низкая: пользователи плохо информированы, слишком озабочены своей независимостью.

### *8.4.2. Анализ состояния безопасности систем обмена данными*

Результаты опроса о состоянии безопасности информационного обмена с помощью телекоммуникаций по состоянию на 1990 г. приведены в табл. 2.21.

*Таблица 2.21. Анализ рисков, связанных с использованием информационного обмена, %*

| *Сектор* | *1990* | | *2001* | |
|---|---|---|---|---|
| | *Да* | *Нет* | *Да* | *Нет* |
| Финансовый | 43 | 57 | *11* | 23 |
| Промышленный | 30 | 70 | 53 | 47 |
| Обслуживания | 0 | 100 | 38 | 62 |
| В общем | 26 | 74 | 43 | 57 |

Анализ возможных рисков и убытков, показывает, что существенная динамика происходит в финансовом секторе и секторе обслуживания (табл. 2.22) [41].

*Таблица 2.22. Классификация информации, %*

| *Сектор* | *1990* | | *2001* | |
|---|---|---|---|---|
| | *Да* | *Нет* | *Да* | *Нет* |
| Финансовый | 14 | 86 | 82 | 18 |
| Промышленный | 20 | 80 | 69 | 31 |
| Обслуживания | 0 | 100 | 53 | 47 |
| В общем | 13 | 87 | 45 | 55 |

Важность качественной классификации информации является необходимой предпосылкой для использования средств безопасности адекватно эффективности и стоимости. Это часто недооценивается.

Сопоставление того, что следовало бы сделать в области безопасности систем обмена данными, с тем, что делается в настоящее время, показывает, что безопасность телекоммуникаций в большинстве случаев представляет ахиллесову пяту.

Когда классификация проведена, она широко используется для определения архитектуры информационной системы и для реализации программ, которые будут управлять информационным обменом (табл. 2.23-2.28).

*Таблица 2.23. Использование классификации в интересах архитектурной концепции системы, %*

| Сектор | 1990 | | 2001 | |
|---|---|---|---|---|
| | Да | Нет | Да | Нет |
| Финансовый | 11 | 89 | 47 | 53 |
| Промышленный | 20 | 80 | 46 | 54 |
| Обслуживания | 0 | 100 | 12 | 88 |
| В общем | 12 | 88 | 35 | 65 |

Анализ показывает, что большое внимание защите важной информации уделяет финансовый сектор.

*Таблица 2.24. Защита важной информации в режиме «абонент - абонент», %*

| Сектор | 1990 | | 2001 | |
|---|---|---|---|---|
| | Да | Нет | Да | Нет |
| Финансовый | 57 | 43 | 87 | 13 |
| Промышленный | 40 | 60 | 62 | 38 |
| Обслуживания | 0 | 100 | 12 | 88 |
| В общем | 35 | 65 | 43 | 57 |

*Таблица 2.25. Наличие системы «идентификация/подтверждение подлинности» каждого пользователя, %*

| Сектор | 1990 | | 2001 | |
|---|---|---|---|---|
| | Да | Нет | Да | Нет |
| Финансовый | 57 | 43 | 89 | 11 |
| Промышленный | 80 | 20 | 100 | 0 |
| Обслуживания | 33 | 67 | 50 | 50 |
| В общем | 61 | 39 | 78 | 22 |

Сопоставление двух последних аспектов свидетельствует о более широком использовании систем «идентификация/подтверждение подлинности» для внешних корреспондентов по сравнению с внутренними пользователями. Такая подозрительность по отношению к внешним пользователям противоречит действительности, которая свидетельствует, что две трети ущербов, имеющих злонамеренный характер, исходит от персонала предприятия.

*Таблица 2.26. Наличие системы «идентификация/подтверждение подлинности» внешних корреспондентов, %*

| Сектор | 1990 | | 2001 | |
|---|---|---|---|---|
| | Да | Нет | Да | Нет |
| Финансовый | 72 | 28 | 86 | 14 |
| Промышленный | 90 | 10 | 95 | 5 |
| Обслуживания | 17 | 83 | 50 | 50 |
| В общем | 65 | 35 | 80 | 20 |

*Таблица 2.27. Использование системы подписных номеров, %*

| Сектор | 1990 | | 2001 | |
|---|---|---|---|---|
| | Да | Нет | Да | Нет |
| Финансовый | 15 | 85 | 69 | 31 |
| Промышленный | 20 | 80 | 36 | 64 |
| Обслуживания | 0 | 100 | 0 | 100 |
| В общем | 13 | 87 | 28 | 72 |

*Таблица 2.28. Использование электронной подписи, %*

| Сектор | 1990 | | 2001 | |
|---|---|---|---|---|
| | Да | Нет | Да | Нет |
| Финансовый | 15 | 85 | 41 | 53 |
| Промышленный | 20 | 80 | 25 | 75 |
| Обслуживания | 0 | 100 | 0 | 100 |
| В общем | 4 | 96 | 11 | 89 |

## 8.5. Факторы, влияющие на требуемый уровень защиты информации

Таким образом, можно классифицировать факторы, влияющие на уровни защиты информации.

**Группа 1** - обусловливаемые характером обрабатываемой информации:

1. Степень секретности.
2. Объемы.
3. Интенсивность обработки.

**Группа 2** - обусловливаемые архитектурой автоматизированной системы обработки данных:

1. Геометрические размеры.

2. Территориальная распределенность.
3. Структурированность компонентов.

**Группа 3** - обусловливаемые условиями функционирования автоматизированной системы обработки данных:

1. Расположение в населенном пункте.
2. Расположение на территории объекта.
3. Обустроенность.

**Группа 4** - обусловливаемые технологией обработки информации.

1. Масштаб.
2. Стабильность.
3. Доступность.
4. Структурированность.

**Группа 5** - обусловливаемые организацией работы автоматизированной системы обработки данных:

1. Общая постановка дела.
2. Укомплектованность кадрами.
3. Уровень подготовки и воспитания кадров.
4. Уровень дисциплины.

## 8.6. Критерии оценки безопасности информационных технологий

В 2002 г. Гостехкомиссия России утвердила руководящий документ (РД) «Критерии оценки безопасности информационных технологий. (Общие критерии)».

Этот РД содержит систематизированный каталог требований к безопасности информационных технологий (ИТ), порядок и методические рекомендации по его использованию при задании требований, разработке, оценке и сертификации продуктов и систем ИТ по требованиям безопасности информации.

Этот документ не отменяет ранее принятые РД. Он разработан в развитие РД Гостехкомиссии России по защите информации от несанкционированного доступа и соответствует ГОСТ Р ИСО/МЭК 15408-2002 «Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий».

Разработка настоящего руководящего документа была направлена на обеспечение практического использования ГОСТ Р ИСО/МЭК 15408-2002 в деятельности заказчиков, разработчиков и пользователей продуктов и систем ИТ при формировании ими требований, разработке, приобретении и применении продуктов и систем ИТ, предназначенных для обработки, хранения или передачи информации, подлежащей защите в соответствии с требованиями нормативных правовых документов или требованиями, устанавливаемыми собственником информации. Руководящий документ предназначен также для органов сертификации и испытательных лабораторий, аккредитованных в системе сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00 (Гостехкомиссии России), для использования при проведении оценки и сертификации безопасности ИТ.

Основной целью РД является повышение доверия к безопасности продуктов и систем ИТ. Положения РД направлены на создание продуктов и систем ИТ с уровнем безопасности, адекватным имеющимся по отношению к ним угрозам и проводимой политике безопасности с учетом условий применения, что должно обеспечить оптимизацию продуктов и систем ИТ по критерию «эффективность - стоимость».

Под безопасностью ИТ в этом РД понимается состояние ИТ, определяющее защищенность информации и ресурсов ИТ от действия объективных и субъективных, внешних и внутренних, случайных и преднамеренных угроз, а также способность ИТ выполнять предписанные функции без нанесения неприемлемого ущерба субъектам информационных отношений.

Доверие к безопасности ИТ обеспечивается как реализацией в них необходимых функциональных возможностей, так и осуществлением комплекса мер по обеспечению безопасности при разработке продуктов и систем ИТ, проведением независимых оценок их безопасности и контролем ее уровня при эксплуатации.

Требования к безопасности конкретных продуктов и систем ИТ устанавливаются, исходя из имеющихся и прогнозируемых угроз безопасности, проводимой политики безопасности, а также с учетом условий их применения. При формировании требований должны в максимальной степени использоваться компоненты требований, представленные в настоящем РД. Допускается также использование и других требований безопасности, при этом уровень детализации и способ выражения требований, представленных в настоящем РД, должны использоваться в качестве образца. Требования безопасности могут задаваться заказчиком в техническом задании на разработку продуктов и систем ИТ или формироваться разработчиком при создании им продуктов ИТ самостоятельно.

Требования безопасности, являющиеся общими для некоторого типа продуктов или систем ИТ, могут оформляться в виде представленной в настоящем РД структуры, именуемой «профилем защиты». Профили защиты, прошедшие оценку в установленном порядке, регистрируются и помещаются в каталог оцененных профилей защиты.

Оценка и сертификация безопасности ИТ проводится на соответствие требованиям, представляемым разработчиком продукта или системы ИТ в задании по безопасности. Требования заданий по безопасности продуктов и систем ИТ, предназначенных для использования в областях применения, регулируемых государством, должны соответствовать требованиям установленных профилей защиты.

РД состоит из трех частей.

Ч. 1 определяет виды требований безопасности (функциональные и требования доверия), основные конструкции представления требований безопасности (профиль защиты, задание по безопасности) и содержит основные методические положения по оценке безопасности ИТ.

Ч. 2 содержит универсальный систематизированный каталог функциональных требований безопасности и предусматривает возможность их детализации и расширения по определенным правилам.

Ч. 3 содержит систематизированный каталог требований доверия к безопасности и оценочные уровни доверия, определяющие меры, которые должны быть приняты на всех этапах жизненного цикла продуктов или систем ИТ для обеспечения уверенности в том, что они удовлетворяют предъявленным к ним функциональным требованиям.

Требования безопасности, содержащиеся в настоящем РД, могут уточняться и дополняться по мере совершенствования правовой и нормативной базы, развития ИТ и совершенствования методов обеспечения безопасности. Внесение изменений в РД осуществляется в порядке, устанавливаемом Гостехкомиссией России.

В табл. 2.29 приведен путеводитель по общим критериям, позволяющий потребителям, разработчикам и экспертам ориентироваться в содержании РД.

*Таблица 2.29. Путеводитель по общим критериям ориентировки в РД*

| *Часть* | *Потребители* | *Разработчики* | *Эксперты* |
|---|---|---|---|
| 1 | Общие сведения по применению. Руководство по структуре профилей защиты | Общие сведения и справочное руководство для разработки требований и формулирования спецификаций безопасности для объектов оценки (ОО) | Общие сведения по применению. Руководство по структуре профилей защиты и заданий по безопасности |

*Окончание табл. 2.29*

| *Часть* | *Потребители* | *Разработчики* | *Эксперты* |
|---|---|---|---|
| 2 | Руководство и справочник при формулировании требований к функциям безопасности | Справочник при интерпретации функциональных требований и формулировании функциональных спецификаций для ОО | Официальное описание критериев оценки для определения эффективности выполнения ОО требуемых функций безопасности |
| 3 | Руководство при определении требуемого уровня гарантии | Справочник при интерпретации описаний требований гарантии и определении подходов к обеспечению гарантии для ОО | Официальное описание критериев оценки при определении гарантии для ОО и при оценке профилей защиты и заданий по безопасности |

Рассматриваемый РД использует следующую терминологию.

**Активы (Assets)** - информация или ресурсы, которые должны быть защищены средствами ОО.

**Атрибут безопасности (Security attribute)** - информация, связанная с субъектами, пользователями и/или объектами, которая применяется для реализации политики безопасности (ПБ) ОО.

**Аутентификационные данные (Authentication data)** - данные, используемые для подтверждения подлинности пользователя.

**Базовая стойкость функции безопасности (СФБ) (SOF-basic)** - уровень стойкости функции безопасности ОО, на котором в соответствии с результатами анализа обеспечивается адекватная защита от случайного нарушения безопасности ОО нарушителями с низким потенциалом нападения.

**Внешний объект ИТ (External IT entity)** - любые продукты или система ИТ, доверенные или нет, находящиеся вне ОО и взаимодействующие с ОО.

**Внутренний канал связи ОО (Internal communication channel ТОЕ)** - канал связи между отдельными частями ОО.

**Выбор (Selection)** - выделение одного или нескольких элементов из списка в компоненте.

**Высокая СФБ (SOF-high)** - уровень стойкости функции безопасности ОО, на котором в соответствии с результатами анализа обеспечивается адекватная защита от тщательно спланированного и организованного нарушения безопасности ОО нарушителями с высоким потенциалом нападения.

**Гарантия (Assurance)** - основание для уверенности в том, что объект соответствует заданным целям безопасности.

**Данные комплексной системы безопасности (КСБ) (TSF data)** - данные, созданные ОО или созданные для ОО, которые могут повлиять на его функционирование.

**Данные пользователя (User data)** - данные, созданные пользователем или для пользователя, которые не влияют на функционирование КСБ.

**Доверенный канал (Trusted channel)** - средства взаимодействия между КСБ и удаленным доверенным продуктом ИТ, обеспечивающие необходимую степень уверенности в выполнении ПБ ОО.

**Доверенный маршрут (Trusted path)** - средства взаимодействия между пользователем и КСБ, обеспечивающие необходимую степень уверенности в выполнении ПБ ОО.

**Зависимость (Dependency)** - такое соотношение между требованиями, при котором требование, от которого зависят другие требования, должно быть полностью выполнено, чтобы и другие требования могли быть реализованы.

**Задание по безопасности (Security Target)** - совокупность требований безопасности и спецификаций, которую необходимо использовать в качестве основы для оценки конкретного ОО.

**Идентификатор (Identity)** - представление уполномоченного пользователя (например, строка символов), однозначно его идентифицирующее. Таким представлением может быть полное или сокращенное имя этого пользователя или его псевдоним.

**Интерфейс комплекса средств обеспечения безопасности ОО (TOE Security Functions Interface)** - совокупность интерфейсов, как интерактивных (человекомашинные интерфейсы), так и программных (интерфейсы прикладных программ), с использованием которых осуществляется доступ к ресурсам ОО под контролем КСБ или получение от КСБ какой-либо информации.

**Итерация (Iteration)** - более чем однократное использование компонента при различном выполнении операций.

**Класс (Class)** - совокупность семейств, объединенных общим назначением.

**Комплекс средств обеспечения безопасности ОО (TOE Security Functions)** - совокупность всех аппаратных, программных и программно-аппаратных средств ОО, обеспечивающих адекватную реализацию ПБ ОО.

**Компонент (Component)** - наименьшая совокупность элементов, которая может быть выбрана для включения в профиль защиты (ПЗ), задание по безопаности (ЗБ) или пакет.

**Механизм проверки правомочности обращений (Reference validation mechanism)** - реализация монитора обращений, обладающая сле-

дующими свойствами: защищенностью от проникновения; постоянной готовностью; простотой, достаточной для проведения полного анализа и тестирования.

**Модель политики безопасности ОО (TOE security policy model)** - структурированное представление ПБ, которая должна быть реализована ОО.

**Монитор обращений (Reference monitor)** - концепция абстрактной машины, реализующей политику управления доступом ОО.

**Назначение (Assignment)** - спецификация заданного параметра в компоненте.

**Неформальный (Informal)** - выраженный на естественном языке.

**Область действия КСБ (TSF Scope of Control)** - совокупность возможных взаимодействий с ОО или внутри его, которые подчинены правилам ПБ ОО.

**Объект (Object)** - сущность в пределах области действия комплексной системы безопасности (ОДКСБ), которая содержит или принимает информацию и над которой субъекты выполняют операции.

**Объект оценки (Target of Evaluation)** - подлежащие оценке продукт ИТ или система с руководствами администратора и пользователя (с документацией).

**Оператор-пользователь (Human user)** - любое лицо, взаимодействующее с ОО.

**Орган оценки (Evaluation authority)** - организация, которая посредством системы оценки осуществляет применение общих критериев (ОК) для определенной сферы, устанавливает стандарты и контролирует качество оценок, проводимых в данной сфере другими организациями.

**Оценка (Evaluation)** - установление соответствия ПЗ, ЗБ или ОО определенным критериям.

**Пакет (Package)** - неоднократно используемая совокупность функциональных компонентов или компонентов гарантии (например, оценочного уровня доверия (ОУД)), объединенных для достижения определенных целей безопасности.

**Передача в пределах ОО (Internal TOE transfers)** - передача данных между отдельными частями ОО.

**Передача за пределы области действия КСБ (Transfers outside TSF control)** - передача данных сущностям, не контролируемым КСБ.

**Передача между КСБ (Inter-TSF transfers)** - передача данных между ОО и КСБ других доверенных продуктов ИТ.

**Политика безопасности организации (Organisational security policies)** - совокупность правил, процедур, практических приемов или

руководящих принципов в области безопасности, которыми руководствуется организация в своей деятельности.

**Политика безопасности ОО (TOE Security Policy)** - совокупность правил, регулирующих управление, защиту и распределение активов внутри ОО.

**Политика функции безопасности (Security Function Policy)** - политика безопасности, реализуемая некоторой функцией безопасности (ФБ) (некоторым СБ).

**Полуформальный (Semiformal)** - выраженный на языке с ограниченным синтаксисом и заданной семантикой.

**Пользователь** (User) - любая сущность (оператор-пользователь или внешний объект ИТ) за пределами ОО, которая взаимодействует с ОО.

**Потенциал нападения (Attack potential)** - предполагаемая возможность успеха в случае реализации нападения, выраженная в терминах квалификации, ресурсов и мотивации нарушителя.

**Продукт (Product)** - совокупность программных, программно-аппаратных и/или аппаратных средств ИТ, предоставляющая определенные функциональные возможности и предназначенная как для непосредственного использования, так и для включения в различные системы.

**Профиль защиты (Protection Profile)** - не зависящая от реализации (не связанная с реализацией) совокупность требований безопасности для некоторой категории ОО, отвечающей специфическим потребностям потребителя.

**Расширение (Extension)** - добавление в ЗБ или ПЗ функциональных требований, не содержащихся в ч. 2, и/или требований гарантии, не содержащихся в ч. 3 ОК.

**Ресурс ОО (TOE resource)** - все, что может использоваться или потребляться в ОО.

**Роль (Role)** - заранее определенная совокупность правил, устанавливающих допустимые взаимодействия между пользователем и **ОО.**

**Связность (Connectivity)** - свойство ОО, позволяющее ему взаимодействовать с объектами ИТ, внешними по отношению к ОО. Это взаимодействие включает обмен данными по проводным или беспроводным средствам в любой среде, на любое расстояние и при любой конфигурации.

**Секрет (Secret)** - информация, которая должна быть доступна только уполномоченным пользователям и/или функцией безопасности ОО (ФБО) для реализации определенной политики функции безопасности (ПФБ).

**Семейство (Family)** - совокупность компонентов, объединенных одинаковыми целями безопасности, но отличающихся акцентами или строгостью.

**Система (System)** - автоматизированная система с определенными назначением и условиями эксплуатации.

**Система оценки (Evaluation scheme)** - организационно-правовая структура, в рамках которой осуществляется применение ОК в определенной сфере.

**Средняя СФБ (SOF-medium)** - уровень стойкости функции безопасности ОО, на котором в соответствии с результатами анализа обеспечивается адекватная защита от целенаправленного нарушения безопасности ОО нарушителями с умеренным потенциалом нападения.

**Стойкость функции безопасности (Strength of Function)** - характеристика функции безопасности ОО, выражающая минимально необходимые воздействия непосредственно на ее механизмы безопасности, в результате которых нарушается работа этой функции.

**Субъект (Subject)** - сущность, находящаяся в ОДКСБ, которая инициирует выполнение операций.

**Уполномоченный пользователь (Authorised user)** - пользователь, которому в соответствии с ПБ ОО разрешено выполнять определенные действия.

**Уровень гарантии оценки (Evaluation Assurance Level)** - пакет компонентов гарантии из ч. 3 ОК, соответствующий определенному положению на заданной ОК шкале гарантии.

**Усиление (Augmentation)** - добавление одного или нескольких компонентов гарантии из ч. 3 в УГО или пакет гарантии.

**Уточнение (Refinement)** - добавление деталей в компонент.

**Формальный (Formal)** - выраженный на языке с ограниченным синтаксисом и заданной семантикой, основанной на строго определенных математических концепциях.

**Функция/средство обеспечения безопасности (Security Function)** - часть или части ОО, обеспечивающие выполнение подмножества взаимосвязанных правил ПБ ОО.

**Цель безопасности (Security objective)** - сформулированное намерение противостоять идентифицированным угрозам и/или удовлетворять идентифицированной политике безопасности организации и предположениям.

**Элемент (Element)** - неделимое требование безопасности.

В разделе «Общая модель» представлены общие концепции ОК, включая условия, в которых они должны использоваться, и решения по

их применению. Части 2 и 3 расширяют сферу применения концепций в рамках описанного подхода.

Безопасность рассматривается в ОК с использованием некоторой совокупности понятий и терминологии, приведенных выше. Их понимание является предпосылкой к эффективному использованию ОК. Однако эти понятия имеют общий характер и их использование не ограничивается областью проблем безопасности ИТ, к которой применимы ОК.

Следующая схема иллюстрирует общие понятия безопасности и их взаимосвязь (рис. 2.18).

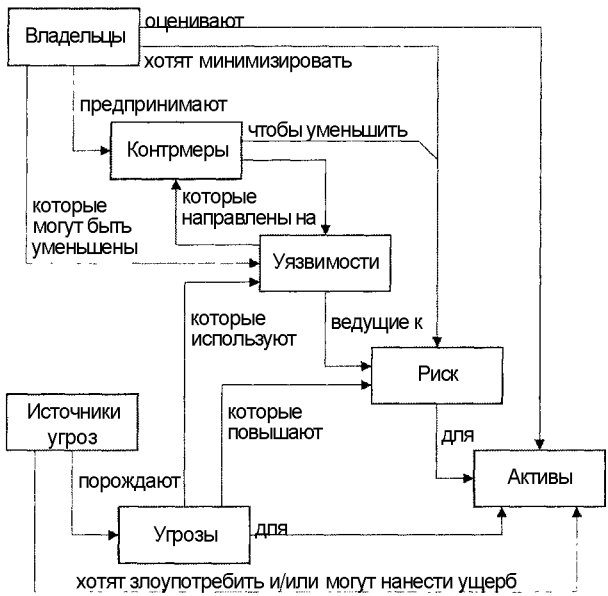



Рис. 2.18. Общие понятия безопасности и их взаимосвязь

Безопасность связана с защитой активов от угроз, классифицируемых в зависимости от возможности злоупотреблений защищаемыми активами. Во внимание должны приниматься все разновидности угроз, но в первую очередь те, которые связаны со случайными или умышленными действиями человека. Сохранность защищаемых активов представляет интерес для их собственников, которые придают большое значение таким активам. Существующие или предполагаемые агенты угроз (нарушители) также могут придавать большое значение этим активам и стремиться их использовать вопреки интересам их собственника. Собственники воспринимают подобные угрозы как возможность воздействия на активы,

ведущего к снижению их ценности для собственника. К нарушениям безопасности обычно относятся (но не обязательно ими ограничиваются): наносящее ущерб раскрытие актива несанкционированным получателем (потеря конфиденциальности), повреждение актива посредством несанкционированной модификации (потеря целостности) или несанкционированное лишение доступа к активу (потеря доступности).

Владельцы активов должны проанализировать возможные угрозы, чтобы определить, какие из них действительно присущи их среде. В результате анализа определяются риски. Анализ должен помочь при выборе мер противодействия угрозам и при уменьшении рисков до приемлемого уровня.

Контрмеры направлены на уменьшение уязвимостей и выполнение политики безопасности владельцев активов (прямо или косвенно распределяясь между этими составляющими). Но и после принятия этих мер уязвимости могут остаться. Такие уязвимости могут использоваться агентами угроз (нарушителями), представляя уровень остаточного риска для активов. Владельцы будут стремиться минимизировать этот риск, задавая дополнительные ограничения.

ОК определяют совокупность конструкций, объединяемых в содержательные наборы требований безопасности известной пригодности, которые затем могут быть использованы при установлении требований безопасности к перспективным продуктам и системам. Взаимосвязь различных конструкций для выражения требований иллюстрируется на следующей схеме (рис. 2.19).

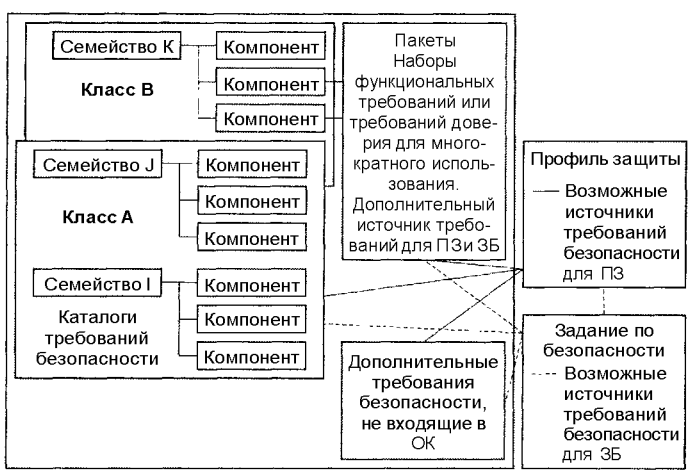



Рис. 2.19. Организация и структура требований

Организация требований безопасности в ОК в виде иерархии «класс - семейство - компонент» призвана помочь потребителям в поиске конкретных требований безопасности.

Функциональные требования и требования доверия представлены в ОК в едином стиле с использованием одной и той же структуры и терминологии.

Термин «класс» применяется для наиболее общего группирования требований безопасности. Все составляющие класса имеют общую направленность, но различаются по охвату целей безопасности.

Составляющие класса называются семействами.

Семейство - это группа наборов требований безопасности, имеющих общие цели безопасности, но различающихся акцентами или строгостью.

Составляющие семейства называются компонентами.

Компонент описывает специфический набор требований безопасности, который является наименьшим выбираемым набором требований безопасности для включения в структуры, определенные в ОК. Совокупность компонентов, входящих в семейство, может быть упорядочена для представления возрастания строгости или возможностей требований безопасности, имеющих общее назначение. Они могут быть также упорядочены частично для представления связанных неиерархических наборов. Упорядочение неприменимо в случае, когда в семействе имеется только один компонент.

Компоненты составлены из отдельных элементов. Элемент - это выражение требований безопасности на самом нижнем уровне. Он является тем неделимым требованием безопасности, которое может быть верифицировано при оценке.

Автор пишет только половину книги:
другую половину пишет читатель.
*Джозеф Конрад*

# 9. Функции и задачи защиты информации

## 9.1. Общие положения

Одно из фундаментальных положений системно-концептуального подхода к защите информации состоит в том, что предполагается разработка такой концепции, в рамках которой имелись бы (по крайней мере потенциально) возможности гарантированной защиты информации для самого общего случая архитектурного построения АСОИ, технологии и условий их функционирования. Для того чтобы множество функций

соответствовало своему назначению, оно должно удовлетворять требованию полноты, причем под полнотой множества функции понимается свойство, состоящее в том, что при надлежащем обеспечении соответствующего уровня (соответствующей степени) осуществления каждой из функций множества гарантированно может быть достигнут требуемый уровень защищенности информации.

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

Обеспечение регулярного осуществления функций защиты достигается тем, что в АСОИ регулярно решаются специальные задачи защиты. При этом задачей защиты информации называются организованные возможности средств, методов и мероприятий, реализуемых в АСОИ с целью осуществления функций защиты. Основное концептуальное требование к задачам защиты состоит в надежном обеспечении заданного уровня осуществления каждой из полного множества функций защиты. Сущность этого требования заключается в следующем.

Множество функций защиты должно быть полным в том смысле, что регулярное их осуществление обеспечивает условия для надежной защиты информации в системном плане. При этом варьируя усилиями и ресурсами, вкладываемыми в осуществление различных функций, можно стремиться к такому положению, когда требуемый уровень защиты информации будет достигаться при минимальных затратах, или к положению, когда при заданных затратах будет достигаться максимальный уровень защиты. Иными словами, полнота множества функций защиты и взаимозависимости различных функций создают предпосылки для оптимального построения системы защиты информации в АСОИ. Практическая реализация этой возможности может быть обеспечена лишь в том случае, если множество задач защиты будет репрезентативным в том смысле, что будет позволять обеспечивать любой заданный уровень осуществления каждой функции защиты, и притом с минимизацией расходов на осуществление как каждой функции отдельно, так и их совокупности. Таким образом, задачи защиты информации являются инструментом практической реализации функций защиты в соответствии с объективными потребностями защиты.

## 9.2. Методы формирования функций защиты

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

- Множество функций обеспечения защиты должно быть таким, чтобы осуществлением их в различных комбинациях и с различными усилиями в любой ситуации при функционировании АСОИ могли быть созданы все условия, необходимые для надежной защиты информации.
- Множество функций управления должно создавать все предпосылки для оптимальной реализации функций обеспечения в любых условиях.

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

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

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

Для того чтобы защищенность информации могла быть нарушена, должны существовать (иметь место) такие условия, при которых могут проявиться дестабилизирующие факторы. Если таких условий не будет, то не будет необходимости в специальной защите информации. Если же потенциальные возможности для проявления дестабилизирующих факторов будут иметь место, то надо оценивать реальную возможность их проявления, обнаруживать факты их проявления, принимать меры к предотвращению воздействия их на информацию, обнаружению, локализации и ликвидации последствий этих воздействий (рис. 2.20).

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

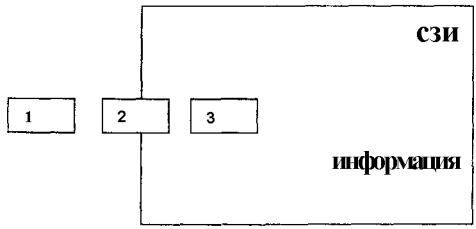



Рис. 2.20. Уровни событий при возникновении дестабилизирующих факторов

**Событие 2** - защита информации нарушена, поскольку не удалось предотвратить воздействие дестабилизирующих факторов на информацию, однако это воздействие локализовано.

**Событие 3** - защита информации разрушена, поскольку воздействие дестабилизирующих факторов на информацию не только не предотвращено, но даже не локализовано.

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

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

### 9.3. Классы задач защиты информации

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

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

**Класс 1.1.** Сокрытие информации о средствах, комплексах, объектах и системах обработки информации. Эти задачи могут подразделяться на технические и организационные.

Организационные задачи по сокрытию информации об объектах направлены на недопущение разглашения этих сведений сотрудниками и утечки их по агентурным каналам.

Технические задачи направлены на устранение или ослабление технических демаскирующих признаков объектов защиты и технических каналов утечки сведений о них. При этом сокрытие осуществляется уменьшением электромагнитной, временной, структурной и признаковой доступности, а также ослаблением адекватности между структурой, топологией и характером функционирования средств, комплексов, объектов, систем обработки информации и управления.

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

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

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

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

**Класс 1.2.** Дезинформация противника.

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

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

Роль дезинформации подчеркивал А. Ф. Вивиани, специалист в области контршпионажа: «На нас обрушивается, валится, извергается огромное количество информации. Она бывает фальшивой, но выглядит правдоподобно; бывает правдивой, а на самом деле хитроумно перекроена, дабы производить впечатление фальшивой; бывает отчасти фальшивой и отчасти правдивой. Все зависит от выбранного способа так называемой дезинформации, цель которой - заставить вас верить, желать, думать, принимать решения в направлении, выгодном для тех, кому зачем-то нужно на нас воздействовать» [43].

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

Частными задачами технической дезинформации являются:

- искажение демаскирующих признаков реальных объектов и систем, соответствующих признакам ложных объектов;
- создание (имитация) ложной обстановки, объектов, систем, комплексов путем воспроизведения демаскирующих признаков реальных объектов, структур систем, ситуаций, действий, функций и т. д.
- передача, обработка, хранение в системах обработки ложной информации.

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

**Класс 1.3.** Легендирование.

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

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

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

**Класс 2.1.** Введение избыточности элементов системы.

Под избыточностью понимается включение в состав элементов системы обработки информации дополнительных компонентов, обеспечи-

вающих реализацию заданного множества целей защиты с учетом воздействий внешних и внутренних дестабилизирующих факторов.

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

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

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

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

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

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

**Класс 2.2.** Резервирование элементов системы.

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

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

Класс 2.3. Регулирование доступа к элементам системы и защищаемой информации.

Регулирование доступа к средствам, комплексам и системам обработки информации (на территорию, в помещение, к техническим средствам, к программам, к базам данных и т. п.) предполагает реализацию идентификации, проверки подлинности и контроля доступа, регистрацию субъекта, учет носителей информации в системе ее обработки.

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

**Класс 2.4.** Регулирование использования элементов системы и защищаемой информации.

Регулирование использования заключается в осуществлении запрашиваемых процедур (операций) при условии предъявления некоторых заранее обусловленных полномочий.

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

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

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

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

**Класс 2.5.** Маскировка информации.

Маскировка информации заключается в преобразовании данных, исключающем доступ посторонних лиц к содержанию информации и обеспечивающем доступ разрешенным пользователям при предъявлении ими специального ключа преобразования. Решение этой задачи осуществляется на основе криптографических, некриптографических и смежных с ними (кодовое зашумление, ортогональные преобразования) преобразований.

**Класс 2.6.** Регистрация сведений.

Регистрация предполагает фиксацию всех сведений о фактах, событиях, возникающих в процессе функционирования средств и систем об-

работки информации, относящихся к защите информации, на основании которых осуществляется решение задач оценки состояния безопасности информации с целью повышения эффективности и управления механизмами защиты.

**Класс 2.7.** Уничтожение информации.

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

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

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

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

**Класс 2.8.** Обеспечение сигнализации.

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

**Класс 2.9.** Обеспечение реагирования.

Получив по каналам обратной связи информацию о состоянии системы защиты, в соответствии с законами управления орган управления должен при необходимости выработать управленческое решение, т. е. отреагировать на полученный сигнал. Реагирование на проявление дестабилизирующих факторов является признаком активности системы защи-

ты информации, реализация которого направлена на предотвращение или снижение степени воздействия факторов на информацию.

**Класс 2.10.** Управление системой защиты информации.

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

**Класс 2.11.** Обеспечение требуемого уровня готовности обслуживающего персонала к решению задач информационной безопасности.

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

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

**Класс** 3.1. Защита от информационного воздействия на технические средства обработки.

Информационное воздействие на технические средства обработки, хранения и передачи информации может быть направлено:

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

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

**Класс 3.2.** Защита от информационного воздействия на общество.

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

**Класс 3.3.** Защита от информационного воздействия на психику человека.

Включает широкий круг задач, направленных как непосредственно на защиту от технических средств воздействия на психику (психотронного оружия), так и на определение и формирование у человека высокой стрессоустойчивости, высоких моральных качеств и т. д., позволяющих противостоять такому воздействия.

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

## 9.4. Функции защиты

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

## 9.5. Состояния и функции системы защиты информации

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

**Состояние 1** - защита информации обеспечена, если при наличии условий, способствующих появлению угроз, их воздействие на защищаемую информацию предотвращено или, ликвидированы последствия такого воздействия.

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

**Состояние 3** - защиты информации разрушена, если результаты воздействий на нее угроз не только не предотвращены, но и не локализованы.

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

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

**Функция 2** - обнаружение проявившихся угроз и предупреждение их воздействия на информацию. Осуществляется комплекс мероприятий, в результате которых проявившиеся угрозы должны быть обнаружены до их воздействия на защищаемую информацию, а также обеспечено недопущение воздействий этих угроз на защищаемую информацию в условиях их проявления и обнаружения. Так, для нейтрализации закладных устройств необходимо регулярно проводить специальные проверки помещений, устанавливать системы их автоматического поиска, а для предупреждения их воздействия на конфиденциальную информацию использовать устройства защиты типа генераторов объемного зашумления, позволяющих создавать вокруг устройств обработки информации шумовое поле.

**Функция 3** - обнаружение воздействия угроз на защищаемую информацию и локализация этого воздействия. Содержание функции на-

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

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

От несоблюдения техники
безопасности человек может не только
умереть, но и родиться.
*NN*

## 10. Стратегии защиты информации

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

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

Потребности в защите обусловливаются прежде всего важностью и объемами защищаемой информации, а также условиями ее хранения, обработки и использования. Эти условия определяются уровнем (качеством) структурно-организационного построения объекта обработки информации, уровнем организации технологических схем обработки, местом и условиями расположения объекта и его компонентов и другими параметрами.

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

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

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

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

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

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

2) ото всех известных угроз;

3) ото всех потенциально возможных угроз.

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

1. Никакое вмешательство в систему обработки информации не допускается. Такое требование может быть предъявлено к уже функционирующим системам обработки информации, и нарушение процесса их функционирования для установки механизмов защиты не разрешается.
2. К архитектурному построению системы обработки информации и технологии ее функционирования допускается предъявлять требования неконцептуального характера. Другими словами, допускается

приостановка процесса функционирования системы обработки информации для установки некоторых механизмов защиты.

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

Практически можно выделить три основные стратегии, представленные в табл. 2.30.

*Таблица 2.30. Стратегии защиты информации*

| *Учитываемые угрозы* | *Влияние на системы обработки информации* | | |
|---|---|---|---|
| | *отсутствует* | *частичное* | *полное* |
| Наиболее опасные | Оборонительная стратегия | | |
| Все известные | | Наступательная стратегия | |
| Все потенциально возможные | | | Упреждающая стратегия |

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

## 11. Способы и средства защиты информации

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

Рассмотрим содержание представленных способов и средств обеспечения безопасности.

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

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

- идентификацию лиц, претендующих на доступ, персонала и ресурсов системы (присвоение каждому объекту персонального идентификатора);
- опознавание (установление подлинности) объекта или субъекта по предъявленному идентификатору;
- проверку полномочий (проверка соответствия дня недели, времени суток, запрашиваемых ресурсов и процедур установленному регламенту);
- регистрацию (протоколирование) обращений к защищаемым ресурсам;
- реагирование (сигнализация, отключение, задержка работ, отказ в процессе) при попытках несанкционированных действий.

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

**Регламентация** как способ защиты информации заключается в разработке и реализации в процессе функционирования объекта комплекса мероприятий, создающих такие условия, при которых существенно затрудняются проявление и воздействие угроз. К регламентации относится разработка таких правил обращения с конфиденциальной информацией

и средствами ее обработки, которые позволили бы максимально затруднить получение этой информации злоумышленником.

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

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

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

Рассмотренные способы обеспечения защиты информации реализуются с применением различных методов и средств. При этом различают формальные и неформальные средства. К формальным относятся такие средства, которые выполняют свои функции по защите информации формально, т. е. преимущественно без участия человека. К неформальным относятся средства, основу которых составляет целенаправленная деятельность людей. Формальные средства делятся на физические, аппаратные и программные.

**Физические средства** - механические, электрические, электромеханические и т. п. устройства и системы, которые функционируют автономно, создавая различного рода препятствия на пути дестабилизирующих факторов.

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

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

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

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

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

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

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

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

Интересный подход к формированию множества способов защиты предлагает член-корреспондент Академии криптографии С. П. Расторгуев. В основу названной им «абсолютной системы защиты», обладающей всеми возможными способами защиты, положены основные принципы защиты, реализуемые в живой природе. Развивая этот подход, можно выделить следующие основные способы защиты животного мира в сравнении с рассмотренными способами защиты информации.

1. Пассивная защита. Перекрывает все возможные каналы воздействия угроз и предполагает «надевание брони» на себя и создание терри-

ториальных препятствий. Налицо полное соответствие такому способу защиты информации, как препятствие.

2. Изменение местоположения. Желание спрятаться можно соотнести с таким способом, как сокрытие.
3. Изменение собственной внешности, мимикрия - слияние с ландшафтом и т. п. Цель - представиться объектом неинтересным или незаметным для нападающей стороны. Аналогичную функцию защиты информации реализуют ее маскировкой.
4. Нападение с целью уничтожения нападающего. Выше был рассмотрен соответствующий способ защиты информации.
5. Воспитание навыков безопасности у потомства, доведение этих навыков до уровня инстинкта. Для систем защиты информации аналогичные навыки у обслуживающего персонала формируются принуждением и побуждением.
6. Выработка определенных правил жизнедеятельности, способствующих выживанию и сохранению рода. К таким правилам, выработанным природой, можно отнести мирное существование особей одного вида, жизнь в стаях (стадах) и т. д. Другими словами, природа регламентирует необходимые для безопасности правила жизни.

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

Продам таблицу умножения без чисел.
*Объявление*

## 12. Криптографические методы защиты информации

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

Разные люди понимают под шифрованием разные вещи. Дети играют в игрушечные шифры и секретные языки. Это, однако, не имеет ничего

общего с настоящей криптографией. Настоящая криптография (strong cryptography) должна обеспечивать такой уровень секретности, чтобы можно было надежно защитить критическую информацию от расшифровки крупными организациями - такими, как мафия, транснациональные корпорации и крупные государства. Настоящая криптография в прошлом использовалась лишь в военных целях. Однако сейчас, со становлением информационного общества, она становится центральным инструментом для обеспечения конфиденциальности.

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

Криптография не является более придумкой военных, с которой не стоит связываться. Настала пора снять с криптографии покровы таинственности и использовать все ее возможности на пользу современному обществу. Широкое распространение криптографии является одним из немногих способов защитить человека от ситуации, когда он вдруг обнаруживает, что живет в тоталитарном государстве, которое может контролировать каждый его шаг.

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

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

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

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

Проблемой защиты информации путем ее преобразования занимается *криптология (kryptos* - тайный, *logos* - наука). Криптология разделяется на два направления - *криптографию* и *криптоанализ*. Цели этих направлений прямо противоположны.

*Криптография* занимается поиском и исследованием математических методов преобразования информации.

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

Современная криптография включает в себя 4 крупных раздела.

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

Основные направления использования криптографических методов - передача конфиденциальной информации по каналам связи (например, электронная почта), установление подлинности передаваемых сообщений, хранение информации (документов, баз данных) на носителях в зашифрованном виде.

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

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

*Алфавит* - конечное множество используемых для кодирования информации знаков.

*Текст* - упорядоченный набор из элементов алфавита.

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

- алфавит Z33 - 32 буквы русского алфавита и пробел;
- алфавит Z256 - символы, входящие в стандартные коды ASCII и КОИ-8;
- бинарный алфавит - Z2 = {0,1};
- восьмеричный алфавит или шестнадцатеричный алфавит.

*Шифрование* - преобразовательный процесс: исходный текст, который носит также название открытого текста, заменяется шифрованным текстом.

*Дешифрование* - обратный шифрованию процесс. На основе ключа шифрованный текст преобразуется в исходный.

*Ключ* - информация, необходимая для беспрепятственного шифрования и дешифрования текстов.

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

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

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

*В системах с открытым ключом* используются два ключа - открытый и закрытый, которые математически связаны друг с другом. Информация шифруется с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения [29].

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

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

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

- количество всех возможных ключей;
- среднее время, необходимое для криптоанализа.

Преобразование Tk определяется соответствующим алгоритмом и значением параметра k. ЭФФЕКТИВНОСТЬ шифрования с целью защиты информации зависит от сохранения тайны ключа и криптостойкости шифра.

## 12.1. Требования к криптосистемам

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

Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:

- зашифрованное сообщение должно поддаваться чтению только при наличии ключа;
- число операций, необходимых для определения использованного ключа шифрования по фрагменту шифрованного сообщения и соответствующего ему открытого текста, должно быть не меньше общего числа возможных ключей;
- число операций, необходимых для расшифровывания информации путем перебора всевозможных ключей, должно иметь строгую нижнюю оценку и выходить за пределы возможностей современных компьютеров (с учетом возможности использования сетевых вычислений);
- знание алгоритма шифрования не должно влиять на надежность защиты;
- незначительное изменение ключа должно приводить к существенному изменению вида зашифрованного сообщения даже при использовании одного и того же ключа;
- структурные элементы алгоритма шифрования должны быть неизменными;
- дополнительные биты, вводимые в сообщение в процессе шифрования, должен быть полностью и надежно скрыты в шифрованном тексте;
- длина шифрованного текста должна быть равной длине исходного текста;
- не должно быть простых и легко устанавливаемых зависимостей между ключами, последовательно используемыми в процессе шифрования;
- любой ключ из множества возможных должен обеспечивать надежную защиту информации;
- алгоритм должен допускать как программную, так и аппаратную реализацию, при этом изменение длины ключа не должно вести к качественному ухудшению алгоритма шифрования.

## 12.2. Основные алгоритмы шифрования

Метод шифровки-дешифровки называют шифром (cipher). Некоторые алгоритмы шифрования основаны на том, что сам метод шифрования (алгоритм) является секретным. Ныне такие методы представляют лишь исторический интерес и не имеют практического значения. Все современные алгоритмы используют ключ для управления шифровкой и де-

шифровкой; сообщение может быть успешно дешифровано, только если известен ключ. Ключ, используемый для дешифровки, может не совпадать с ключом, используемым для шифрования, однако в большинстве алгоритмов ключи совпадают.

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

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

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

Современные алгоритмы шифровки-дешифровки достаточно сложны и их невозможно проводить вручную. Настоящие криптографические алгоритмы разработаны для использования компьютерами или специальными аппаратными устройствами. В большинстве приложений криптография производится программным обеспечением и имеется множество доступных криптографических пакетов.

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

Многие качественные криптографические алгоритмы доступны широко - в книжном магазине, библиотеке, патентном бюро или в Интернете. К широко известным симметричным алгоритмам относятся DES и IDEA, Наверное самым лучшим асимметричным алгоритмом является RSA. В России за стандарт шифрования принят ГОСТ 28147-89.

В табл. 2.31 приведена классификация криптографического закрытия информации.

*Таблица 2.31. Криптографическое закрытие информации*

| *Виды преобразований* | *Способы преобразований* | *Разновидности способа* | *Способ реализации* |
|---|---|---|---|
| Шифрование | Замена (подстановка) | Простая (одноалфавитная) | П |
| | | Многоалфавитная одноконтурная ооыкновенная | П |
| | | Многоалфавитная одноконтурная монофоническая | П |
| | | Многоалфавитная многоконтурная | П |
| | Перестановка | Простая | П |
| | | Усложненная по таблице | П |
| | | Усложненная по маршрутам | П |
| | Аналитическое преобразование | По правилам алгебры матриц | П |
| | | По особым зависимостям | П |
| | Гаммирование | С конечной короткой гаммой | АП |
| | | С конечной длиной гаммой | АП |
| | | С бесконечной гаммой | АП |
| | Комбинированные | Замена+перестановка | АП |
| | | Замена+гаммирование | АП |
| | | Перестановка+ гаммирование | АП |
| | | Гаммирование+гаммирование | АП |
| Кодирование | Смысловое | По специальным таблицам (словарям) | П |
| | Символьное | По кодовому алфавиту | П |
| Другие виды | Рассечение-разнесение | Смысловое | АП |
| | | Механическое | П |
| | Сжатие-расширение | | |

*Примечание.* А - аппаратный; П - программный.

## 12.3. Цифровые подписи

Некоторые из асимметричных алгоритмов могут использоваться для генерирования *цифровой подписи.* Цифровой подписью называют блок данных, сгенерированный с использованием некоторого секретного клю-

ча. При этом с помощью открытого ключа можно проверить, что данные были действительно сгенерированы с помощью этого секретного ключа. Алгоритм генерации цифровой подписи должен обеспечивать, невозможность без секретного ключа создать подпись, которая при проверке окажется правильной.

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

Цифровые подписи также можно использовать для удостоверения *(сертификации - to certify)* того, что документ принадлежит определенному лицу. Это делается так: открытый ключ и информация о том, кому он принадлежит, подписываются стороной, которой доверяем. При этом доверять подписывающей стороне мы можем на основании того, что ее ключ был подписан третьей стороной. Таким образом возникает иерархия доверия. Очевидно, что некоторый ключ должен быть корнем иерархии (т. е. ему мы доверяем не потому, что он кем-то подписан, а потому, что мы верим априори, что ему можно доверять). В *централизованной инфраструктуре ключей* имеется очень небольшое количество корневых ключей сети (например, облеченные полномочиями государственные агентства; их также называют *сертификационными агентствами - certification authorities).* В *распределенной инфраструктуре* нет необходимости иметь универсальные для всех корневые ключи, и каждая из сторон может доверять своему набору корневых ключей (скажем, своему собственному ключу и ключам, им подписанным). Эта концепция носит название *сети доверия (web of trust)* и реализована, например, в PGP.

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

жимое соответствует документу (дайджест и др.), то сообщение считается подтвержденным.

Свободно доступны несколько методов создания и проверки цифровых подписей. Наиболее известным является алгоритм RSA, ГОСТ 34.10-94.

## 12.4. Криптографические хеш-функции

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

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

Много хороших криптографических хеш-функций доступно бесплатно. Широко известные включают MD5 и SHA.

## 12.5. Криптографические генераторы случайных чисел

*Криптографические генераторы случайных чисел* производят случайные числа, которые используются в криптографических приложениях, например для генерации ключей. Обычные генераторы случайных чисел, имеющиеся во многих языках программирования и программных средах, не подходят для нужд криптографии (они создавались с целью получить статистически случайное распределение, криптоаналитики могут предсказать поведение таких случайных генераторов).

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

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

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

Несмотря на то что при аккуратном проектировании криптографически надежный генератор случайных чисел реализовать не так уж и трудно, этот вопрос часто упускают из виду. Таким образом, следует подчеркнуть важность криптографического генератора случайных чисел - если он сделан плохо, он может легко стать самым уязвимым элементом системы.

## 12.6. Обеспечиваемая шифром степень защиты

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

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

Ключ длиной 32 бита требует 232 (около 109) шагов. Такая задача под силу любому дилетанту и решается на домашнем компьютере. Системы с 40-битовым ключом (например, экспортный американский вариант алгоритма RC4) требуют 240 шагов - такие компьютерные мощности имеются в большинстве университетов и даже в небольших компаниях. Системы с 56-битовыми ключами (DES) требуют для вскрытия заметных усилий, однако могут быть легко вскрыты с помощью специальной аппаратуры. Стоимость такой аппаратуры значительна, но доступна для мафии, крупных компаний и правительств. Ключи длиной 64 бита в настоящий момент, возможно, могут быть вскрыты крупными государствами и уже в ближайшие несколько лет будут доступны для вскрытия преступными организациями, крупными компаниями и небольшими государствами. Ключи длиной 80 бит могут в будущем стать уязвимыми. Ключи длиной 128 бит, вероятно, останутся недоступными для вскрытия, методом грубой силы в обозримом будущем. Можно использовать и более длинные ключи. В пределе нетрудно добиться того, чтобы энергия, требуемая для вскрытия (считая, что на один шаг затрачивается минимальный квантовомеханический квант энергии), превзойдет массу Солнца или Вселенной.

Однако длина ключа это еще не все. Многие шифры можно вскрыть и не перебирая всех возможных комбинаций. Вообще говоря, очень трудно придумать шифр, который нельзя было бы вскрыть другим более эффективным способом. Разработка собственных шифров может стать приятным занятием, но для реальных приложений использовать самодельные шифры не рекомендуется, если вы не являетесь экспертом и не уверены на 100 % в том, что делаете.

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

Длины ключей, используемых в криптографии с открытым ключом, обычно значительно больше, чем в симметричных алгоритма. Здесь проблема заключается не в подборе ключа, а в воссоздании секретного ключа по открытому. В случае RSA проблема эквивалентна разложению на множители большого целого числа, которое является произведением

пары неизвестных простых чисел. В случае некоторых других криптосистем проблема эквивалентна вычислению дискретного логарифма по модулю большого целого числа (такая задача считается примерно аналогичной по трудности задаче разложения на множители). Имеются криптосистемы, которые используют другие проблемы.

Чтобы дать представление о степени сложности вскрытия RSA, скажем, что модули длиной 256 бит легко факторизуются обычными программистами. Ключи в 384 бита могут быть вскрыты исследовательской группой университета или компании; 512-битовые ключи находятся в пределах досягаемости крупных государств. Ключи длиной 768 бит, вероятно, не будут надежны продолжительное время. Ключи длиной 1024 бита могут считаться безопасными до тех пор, пока не будет существенного прогресса в алгоритме факторизации; ключи длиной 2048 бит большинство считает надежными на десятилетия. Более подробную информацию о длинах ключей RSA можно почерпнуть из статьи [35].

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

## 12.7. Криптоанализ и атаки на криптосистемы

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

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

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

**Атака с заданным текстом (chosen-plaintext attack).** Атакующий имеет возможнот получить шифрованный документ для любого нужного ему текста, но не знает ключа. Задачей является нахождение ключа. Не-

которые методы шифрования, и в частности RSA, весьма уязвимы для атак этого типа. При использовании таких алгоритмов надо тщательно следить, чтобы атакующий не мог зашифровать заданный им текст.

**Атака с подставкой (Man-in-the-middle attack).** Атака направлена на обмен шифрованными сообщениями и в особенности на протокол обмена ключами. Идея заключается в том, что, когда две стороны обмениваются ключами для секретной коммуникации (например, используя шифр Диффи-Хелмана, Diffie-Hellman), противник внедряется между ними на линии обмена сообщениями. Далее противник выдает каждой стороне свои ключи. В результате, каждая из сторон будет иметь разные ключи, каждый из которых известен противнику. Теперь противник будет расшифровывать каждое сообщение своим ключом и затем зашифровывать его с помощью другого ключа перед отправкой адресату. Стороны будут иметь иллюзию секретной переписки, в то время как на самом деле противник читает все сообщения.

Одним из способов предотвратить такой тип атак заключается в том, что стороны при обмене ключами вычисляют криптографическую хеш-функцию значения протокола обмена (или по меньшей мере значения ключей), подписывают ее алгоритмом цифровой подписи и посылают подпись другой стороне. Получатель проверит подпись и то, что значение хеш-функции совпадает с вычисленным значением. Такой метод используется, в частности, в системе Фотурис (Photuris).

**Атака с помощью таймера (timing attack).** Этот новый тип атак основан на последовательном измерении времен, затрачиваемых на выполнение операции возведения в стенень по модулю целого числа. Ей подвержены по крайней мере следующие шифры: RSA, Диффи-Хеллман и метод эллиптических кривых.

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

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

Наиболее простой критерий такой эффективности - вероятность раскрытия ключа или мощность множества ключей (M). По сути, это то же

самое, что и криптостойкость. Для ее численной оценки можно использовать также и сложность раскрытия шифра путем перебора всех ключей.

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

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

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

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

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

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

Осмельтесь мыслить самостоятельно!
*Вольтер*

# 13. Архитектура систем защиты информации

## 13.1. Требования к архитектуре СЗИ

**Система защиты информации (СЗИ)** в самом общем виде может быть определена как организованная совокупность всех средств, методов и мероприятий, выделяемых (предусматриваемых) на объекте обработки информации (ООИ) для решения в ней выбранных задач защиты.

Введением понятия СЗИ определяется тот факт, что все ресурсы, выделяемые для защиты информации, должны объединяться в единую, це-

лостную систему, которая является функционально самостоятельной подсистемой любого ООИ.

Важнейшим концептуальным требованием к СЗИ является требование адаптируемости, т. е. способности к целенаправленному приспособлению при изменении структуры, технологических схем или условий функционирования ООИ. Важность требования адаптируемости обусловливается, с одной стороны, тем, что перечисленные факторы могут существенно изменяться, а с другой - тем, что процессы защиты информации относятся к слабоструктурированным, т. е. имеющим высокий уровень неопределенности. Управление же слабоструктурированными процессами может быть эффективным лишь при условии адаптируемости системы управления.

Помимо общего концептуального требования, к СЗИ предъявляется еще целый ряд более конкретных, целевых требований, которые могут быть разделены на:

- функциональные;
- эргономические;
- экономические;
- технические;
- организационные.

Сформированная к настоящему времени система включает следующий перечень общеметодологических принципов:

- концептуальное единство;
- адекватность требованиям;
- гибкость (адаптируемость);
- функциональная самостоятельность;
- удобство использования;
- минимизация предоставляемых прав;
- полнота контроля;
- адекватность реагирования;
- экономичность.

*Концептуальное единство* означает, что архитектура, технология, организация и обеспечение функционирования как СЗИ в целом, так и составных компонентов должны рассматриваться и реализовываться

в строгом соответствии с основными положениями единой концепции защиты информации.

*Адекватность требованиям* означает, что СЗИ должна строиться в строгом соответствии с требованиями к защите, которые, в свою очередь, определяются категорией соответствующего объекта и значениями параметров, влияющих на защиту информации.

*Гибкость (адаптируемость)* системы защиты означает такое построение и такую организацию ее функционирования, при которых функции защиты осуществлялись бы достаточно эффективно при изменении в некотором диапазоне структуры объекта обработки информации, технологических схем или условий функционирования каких-либо ее компонентов.

*Функциональная самостоятельность* предполагает, что СЗИ должна быть самостоятельной обеспечивающей подсистемой системы обработки информации и при осуществлении функций защиты не должна зависеть от других подсистем.

*Удобство использования* означает, что СЗИ не должна создавать дополнительных неудобств для пользователей и персонала объекта обработки информации.

*Минимизация предоставляемых прав* означает, что каждому пользователю и каждому лицу из состава персонала объекта обработки информации должны предоставляться лишь те полномочия на доступ к ресурсам объекта обработки информации и находящейся в ней информации, которые ему действительно необходимы для выполнения своих функций в процессе автоматизированной обработки информации. При этом предоставляемые права должны быть определены и установленным порядком утверждены заблаговременно.

*Полнота контроля* предполагает, что все процедуры автоматизированной обработки защищаемой информации должны контролироваться системой защиты в полном объеме, причем основные результаты контроля должны фиксироваться в специальных регистрационных журналах.

*Активность реагирования* означает, что СЗИ должна реагировать на любые попытки несанкционированных действий. Характер реагирования может быть различным и включает: просьбу повторить действие; отключение структурного элемента, с которого осуществлено несанкционированное действие; исключение нарушителя из числа зарегистрированных пользователей; подача специального сигнала и др.

*Экономичность СЗИ* означает, что при условии соблюдения основных требований всех предыдущих принципов расходы на СЗИ должны быть минимальными.

## 13.2. Построение СЗИ

*Функциональным построением* любой системы называется организованная совокупность тех функций, для регулярного осуществления которых она создается.

Под *организационным построением* понимается общая организация системы, адекватно отражающая концептуальные подходы к ее созданию. Организационно СЗИ состоит из трех механизмов:

- обеспечения защиты информации;
- управления механизмами защиты;
- общей организации работы системы.

В механизмах обеспечения защиты выделяются два организационных компонента: постоянные и переменные. При этом под постоянными понимаются такие механизмы, которые встраиваются в компоненты объекта обработки информации в процессе создания СЗИ и находятся в рабочем состоянии в течение всего времени функционирования соответствующих компонентов. Переменные же механизмы являются автономными, использование их для решения задач защиты информации предполагает предварительное осуществление операций ввода в состав используемых механизмов. Встроенные и переменные механизмы могут иметь в своем составе технические, программные и организационные средства обеспечения защиты.

Соответственно составу механизмов обеспечения защиты информации, очевидно, должны быть организованы механизмы управления ими.

Механизмы общей организации работы СЗИ предназначены для системной увязки и координации работы всех компонентов СЗИ.

В понятие «организационное построение» СЗИ входит также распределение элементов этой системы по организационно-структурным элементам ООИ. Исходя из этого, в организационном построении СЗИ должны быть предусмотрены подсистемы защиты на объектах (структурных компонентах) ООИ со своими специфическими механизмами защиты и некоторое управляющее звено, которое имеет название *ядро* СЗИ.

## 13.3. Ядро системы защиты информации

**Ядро системы защиты** предназначено для объединения всех подсистем СЗИ в единую целостную систему, организации обеспечения управления ее функционированием.

Ядро может включать организационные и технические составляющие.

*Организационная составляющая* представляет собой совокупность специально выделенных для обеспечения ЗИ сотрудников, выполняющих свои функции в соответствии с разработанными правилами, а также нормативную базу, регламентирующую выполнение этих функций.

*Техническая составляющая* обеспечивает техническую поддержку организационной составляющей и представляет собой совокупности технических средств отображения состояний элементов СЗИ, контроля доступа к ним, управления их включением и т. д. Чаще всего эти средства объединены в соответствующий пульт управления СЗИ.

Ядро СЗИ обладает следующими функциями.

1. Включение компонентов СЗИ в работу при поступлении запросов на обработку защищаемой информации и блокирование бесконтрольного доступа к ней:

- оборудование объекта средствами охранной сигнализации;
- организация хранения носителей защищаемой информации в отдельных хранилищах (документация, шифры, магнитные носители и т. д.).
- включение блокирующих устройств, регулирующих доступ к элементам СЗИ при предъявлении соответствующих полномочий и средств сигнализации.

2. Организация и обеспечение проверок правильности функционирования СЗИ:

- аппаратных средств - по тестовым программам и организационно;
- физических средств - организационно (плановые проверки средств охранной сигнализации, сигнализации о повышении давления в кабелях и т. д.);
- программных средств - по специальным контрольным суммам (на целостность) и по другим идентифицирующим признакам.

## 13.4. Ресурсы системы защиты информации

**Ресурсы** информационно-вычислительной системы, необходимые для создания и поддержания функционирования СЗИ, как и любой другой автоматизированной системы, объединяются в техническое, математическое, программное, информационное и лингвистическое обеспечение.

1. *Техническое обеспечение* - совокупность технических средств, необходимых для технической поддержки решения всех тех задач защиты информации, решение которых может потребоваться в процессе функционирования СЗИ.

2. *Математическое обеспечение* - совокупность математических методов, моделей и алгоритмов, необходимых для оценки уровня защищенности информации и решения других задач защиты.
3. *Программное обеспечение* - совокупность программ, реализующих программные средства защиты, а также программ, необходимых для решения задач управления механизмами защиты. К ним должны быть отнесены также сервисные и вспомогательные программы СЗИ.
4. *Информационное обеспечение* - совокупность систем классификации и кодирования данных о защите информации, массивы дынных СЗИ, в также входные и выходные документы СЗИ.
5. *Лингвистическое обеспечение* - совокупность языковых средств, необходимых для обеспечения взаимодействия компонентов СЗИ между собой, с компонентами объекта обработки информации и с внешней средой.

## 13.5. Организационное построение

Организационное построение СЗИ в самом общем случае может быть представлено совокупностью следующих рубежей защиты (рис. 2.21):

1) территории, занимаемой ООИ;
2) зданий, расположенных на территории;
3) помещений внутри здания, в которых расположены ресурсы ООИ и защищаемая информация;
4) ресурсов, используемых для обработки и хранения информации и самой защищаемой информации;
5) линий связи, проходящих в пределах одного и того же здания;
6) линий (каналов) связи, проходящих между различными зданиями, расположенными на одной и той же охраняемой территории;
7) линий (каналов) связи, соединяющих с другими объектами вне охраняемой территории.

Таким образом, можно провести организационное построение системы защиты информации с помощью приведенной семирубежной модели. В наиболее общем случае необходимо в зависимости от выбранной стратегии защиты сформулировать требования к ядру СЗИ и ресурсам СЗИ, а также использовать критерии построения СЗИ, изложенные в данной главе.

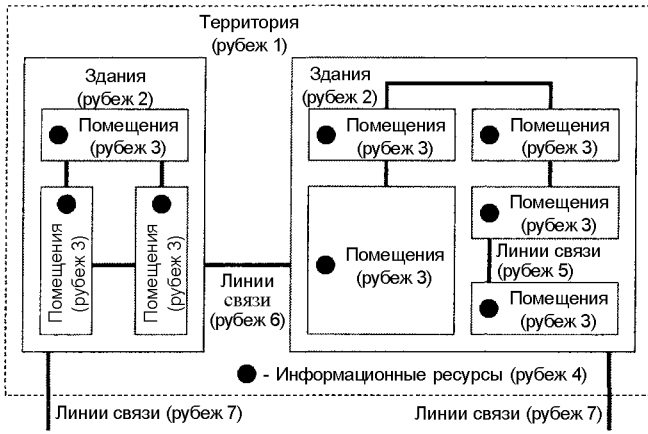



Рис. 2.21. Семирубежная модель защиты информации

Необходимо отметить, что построение СЗИ должно проводиться в соответствии с нормативно-правовой документацией, принятой в РФ. На осуществление большинства видов деятельности в сфере защиты информации необходимы лицензии. Так, для работы с государственной тайной, для работы с криптографическими средствами требуются соответствующие лицензии Федеральной службы безопасности, технические средства должны быть аттестованы Федеральной службой по техническому и экспортному контролю.

## Литература

1. Анин Б. Ю. Защита компьютерной информации. СПб.: БХВ - Санкт-Петербург, 2000. 384 с: ил.
2. Бухвинер В. Е. Телеобслуживание и человекомашинная связь. М.: Радио и связь, 1983
3. Второй московский форум диллеров МЕ // Компьютерра. 1993. № 21. С. 14.
4. Гайкович В. Ю., Першин А. Ю. Безопасность электронных банковских систем. М.: Единая Европа, 1994.
5. Герасименко В. А. Защита информации в автоматизированных системах обработки данных. В 2-х кн. М.: Энергоатомиздат.1994.
6. Герасименко В. А., Малюк А. А. Основы защиты информации. М.: Инкомбук, 1997. 540 с.

7. Грушко А. А., Тимонина Е. Е. Теоретические основы защиты информации. Яхтсмен, 1996.
8. Дружинин Т. В., Сергеева И. В. Качество информации. М.: Радио и связь, 1990. С. 170.
9. Закон РФ об информации, информатизации и защите информации.
10. Касперский Е. Компьютерные вирусы: что это такое и как с ними бороться. М.: СК Пресс, 1998.
11. Корюкова А. А., Дера В. Т. Основы научно-технической информации. М.: Высш. шк., 1985.
12. Лопатников Л. И. Популярный экономико-математический словарь. М.: Знание, 1990. С. 49.
13. Мафик С. Механизмы защиты в сетях ЭВМ. М.: Мир, 1993.
14. Мельников В. В. Защита информации в компьютерных системах. М.: Финансы и статистика: Электроинформ, 1997.
15. Новик И. Б., Абдуллаев А. Ш. Введение в информационный мир. М.: Наука, 1991. С.7.
16. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных: Учеб. пособие для вузов / П. Ю. Белкин, О. О. Михальский, А. С. Першаков и др. М.: Радио и связь, 2000. 168 с.: ил.
17. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах: Учеб. пособие для вузов /Проскурин В.Г., Кругов СВ., Мацкевич И.В. М.: Радио и связь, 2000. 168 с.
18. Расторгуев С. П. Программные методы защиты информации в компьютерах и сетях. М.: Яхтсмен, 1993.
19. Руководящий документ ГТК РФ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требований по защите информации. М.: Воениздат, 1992.
20. Руководящий документ ГТК РФ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. М.: Воениздат, 1992.
21. Самосук М. Компьютерное пиратство. // Защита программного обеспечения: Сб./ Под ред. Гроубера. М.: Мир, 1992

22. Семкин С. Н., Семкин А. Н. Основы информационной безопасности объектов обработки информации: Науч.-практ. пособие. Орел: 2000. 300 с.
23. Слепов Б. С., Чистяков В. М. Управление процессами использования информационных ресурсов. Новосибирск: Наука, 1984, с. 235.
24. Спесивцев А. П. Защита информации в персональных ЭВМ. М.: Радио и связь, 1992.
25. Теоретические основы компьютерной безопасности: Учебное пособие для вузов / П. Н. Девянин, О. О. Михальский, Д. И. Правиков и др. М.: Радио и связь, 2000. 192 с: ил.
26. Терминологические основы проблематики информационной безопасности // Мат. к заседанию межвед. междисциплинарного сем. по науч. проблемам информ. безопасности 1 марта 2001 г. М.: МГУ, 2001.
27. Хоффман Л. Дж. Современные методы защиты информации: Пер. с англ. М.: Сов. радио, 1980.
28. Цыкин Г. С. Усилители электрических сигналов. М.: Энергия, 1969.
29. Шеннон К. Работы по теории информации и кибернетике. М.: Изд-во иностранной литературы, 1963. 489 с.
30. Ярочкин В. И. Безопасность информационных систем. М.: Ось-89, 1996. 320 с. (безопасность предпринимательства).
31. Ярочкин В. И. Система безопасности фирмы. 2-е изд. М.: Ось-89, 1999. 192 с.
32. Ярочкин В. И. Технические каналы утечки информации. М.: ИПКОР, 1994.
33. Bovteiller R. Das Hacker HACKBUCH, Tdition Aragon, Moers, 1985.
34. Lemere H.M. SECURITE DES SYSTEMES D'INFORMATION. Informatique E Stratigue Paris, DUNOD, 1991.
35. Шнайдер Б. Прикладная криптография. М.: Мир 1999.
36. Интеллектуальные системы в управлении, конструировании и образовании / Под ред. проф. А. А. Шелупанова. Томск: STT, 2001. 224 с.
37. www.kara-murza.ru.
38. Труд. 2000. № 19. С. 5.
39. www.dni.ru/news/society/2002/2/16/6047.html.
40. www.fr.ru/arhiv/2001/37/57.html.
41. Эксперт. № 1-12.2000.
42. Эксперт. № 1-12.2001.
43. http://bit.tsure.ru/books/ezi/uchebnik/3.htm.

## Приложение 1

# РАБОЧАЯ ПРОГРАММА ПО ДИСЦИПЛИНЕ «ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

## I. Цели и задачи дисциплины, ее место в учебном процессе. Цели преподавания дисциплины

Цель дисциплины «Основы информационной безопасности» - заложить терминологический фундамент, научить правильно проводить анализ угроз информационной безопасности, выполнять основные этапы решения задач информационной безопасности, приобрести навыки анализа угроз информационной безопасности, рассмотреть основные общеметодологические принципы теории информационной безопасности; изучение методов и средств обеспечения информационной безопасности, методов нарушения конфиденциальности, целостности и доступности информации.

### Задачи изучения дисциплины

1. Ознакомление студентов с терминологией информационной безопасности.
2. Развитие мышления студентов.
3. Изучение методов и средств обеспечения информационной безопасности.
4. Обучение определению причин, видов, источников и каналов утечки, искажения информации.

### Общие указания к выполнению практических занятий

В целях лучшего понимания сути представления и обработки информации при защите рекомендуется использовать гипотетическую модель информации, что позволит использовать архитектурные особенности, свойственные конкретным моделям анализа. Примеры следует выбирать так, чтобы вычисления были не слишком громоздкими. Следует рассматривать задачи, возникающие в самых различных отраслях, и показать динамику решения задач: как подойти к решению конкретной проблемы, какие ограничения возникают в рамках данного решения и какие результаты получаются в конечном счете. В идеальном случае процесс обучения должен происходить следующим образом: студент слушает лекции,

читает учебную литературу, работает дома и на практических занятиях. Студенту рекомендуется иметь доступ к компьютеру во время самостоятельной работы для выполнения индивидуальных заданий.

Подготовка к каждой работе производится во внеаудиторное время. В самостоятельную работу входит выполнение индивидуальных заданий. Преподаватель принимает решение о допуске студента к практической работе по результатам собеседования. Студенты знакомятся с общими сведениями, порядком выполнения работы, пишут необходимые пояснения в соответствии с полученным вариантом задания. При защите работы студент отвечает преподавателю на контрольные вопросы, представляет теоретическую часть решения задачи, практический расчет.

### Перечень дисциплин, усвоение которых необходимо для изучения данного курса

Для выполнения большинства задач достаточно «здравого смысла», знания элементарной математики и начальных сведений из математического анализа, линейной алгебры, дискретной математики.

## II. Содержание дисциплины

### 1. Теоретические занятия (18 ч)

| *№ п/п* | *Тема и ее содержание* | *Колич. часов* |
|---|---|---|
| 1 | **Понятие национальной безопасности, виды безопасности. Информационная безопасность РФ.** Органы, обеспечивающие национальную безопасность РФ, цели, задачи. Национальные интересы РФ в информационной сфере. Приоритетные направления в области защиты информации в РФ. Тенденции развития информационной политики государств и ведомств. Государственная тайна. Правовое обеспечение защиты информации | 2 |
| 2 | **Терминологические основы информационной безопасности. Основные понятия и определения.** Понятие информации, информатизации, информационных систем и смежных с ними: информационная безопасность, информационная война, информационная агрессия, информационное оружие, информационные процессы, информационная система, информационная сфера. Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене. Защита информации, тайна, средства защиты информации, угрозы - определения, сопоставление | 2 |

| *№ п/п* | *Тема и ее содержание* | *Колич. часов* |
|---|---|---|
| 3 | **Общеметодологические принципы теории информационной безопасности. Комплексность.**<br>Этапы развития информационной безопасности: 1. Системы безопасности ресурса. 2. Этап развитой защиты (постепенное осознание необходимости комплексирования целей защиты, расширение арсенала используемых средств защиты, стали объединяться в функциональные самостоятельные системы защиты). 3. Этап комплексной защиты.<br>Требования к системе защиты информации.<br>Показатели информации: важность, полнота, адекватность, релевантность, толерантность.<br>Комплексность: целевая, инструментальная, структурная, функциональная, временная | 2 |
| 4 | **Угрозы. Классификация и анализ угроз информационной безопасности.**<br>Понятие угрозы. Виды угроз. Три наиболее выраженные угрозы: 1) подверженность физическому искажению или уничтожению; 2) возможность несанкционированной (случайной или злоумышленной) модификации; 3) опасность несанкционированного (случайного и преднамеренного) получения информации лицами, для которых она не предназначена.<br>Характер происхождения угроз: умышленные факторы, естественные факторы. Источники угроз. Предпосылки появления угроз: объективные, субъективные | 4 |
| 5 | **Методы нарушения конфиденциальности, целостности и доступности информации.**<br>Классы каналов несанкционированного получения информации: 1) непосредственно с объекта; 2) с каналов отображения информации; 3) получение по внешним каналам; 4) подключение к каналам получения информации.<br>Причины нарушения целостности информации: субъективные преднамеренные, субъективные непреднамеренные, объективные непреднамеренные.<br>Потенциально возможные злоумышленные действий в автоматизированных системах обработки данных.<br>Функции защиты информации: 4 функции.<br>Стратегии защиты информации: оборонительная стратегия, наступательная стратегия, упреждающая стратегия.<br>Архитектура систем защиты информации.<br>Семирубежная модель защиты информации | 2 |

| *№ п/п* | *Тема и ее содержание* | *Колич. часов* |
|---|---|---|
| 6 | **Причины, виды, каналы утечки и искажения информации.** Три методологических подхода к оценке уязвимости информации: эмпирический, теоретический и теоретико-эмпирический. Модель затрат, разработанная специалистами американской фирмы IBM. Модель защиты - модель системы с полным перекрытием. Последовательность решения задачи защиты информации. Фундаментальных требования, которым должны удовлетворять те вычислительные системы, которые используются для обработки конфиденциальной информации. Требования разделены на три группы: стратегия, подотчетность, гарантии. Классификация автоматизированных систем и требований по защите информации. Факторы, влияющие на требуемый уровень защиты информации | 4 |
| 7 | **Функции и задачи защиты информации. Проблемы региональной информационной безопасности.** Методы формирования функций защиты. Сокрытие информации о средствах, комплексах, объектах и системах обработки информации. Дезинформация противника. Легендирование. Введение избыточности элементов системы. Резервирование элементов системы. Регулирование доступа к элементам системы и защищаемой информации. Регулирование использования элементов системы и защищаемой информации. Маскировка информации. Регистрация сведений. Уничтожение информации. Обеспечение сигнализации. Обеспечение реагирования. Управление системой защиты информации. Обеспечение требуемого уровня готовности обслуживающего персонала к решению задач информационной безопасности. Защита от информационного воздействия на технические средства обработки. Защита от информационного воздействия на общество. Защита от информационного воздействия на психику человека.<br>Применение криптографии.<br>Региональные компоненты защиты информации. Защита информации предприятия. Проведение анализа защищенности локального объекта | 2 |
| | *Итого* | 18 |

### 2. Практические занятия (18 ч)

| *№ п/п* | *Тема и ее содержание* | *Колич. часов* |
|---|---|---|
| 1 | Анализ терминов и определений информационной безопасности. ГОСТы и руководящие документы | 2 |
| 2 | Угрозы информации. Проведение анализа информации на предмет целостности | 2 |
| 3 | Определение коэффициентов важности, полноты, адекватности, релевантности, толерантности информации | 4 |
| 4 | Классификация автоматизированных систем обработки информации по классу защиты информации | 4 |
| 5 | Оценка безопасности информации на объектах ее обработки | 6 |
| | *Итого* | 18 |

### 3. Самостоятельная работа (28 ч)

Самостоятельная работа включает следующие задания:

| *№ п/п* | *Тема и ее содержание* | *Колич. часов* |
|---|---|---|
| 1 | Подготовка к практическим занятиям, повторение изучения лекционного материала (проверка - на практических занятиях) | 10 |
| 2 | Подготовка к лекциям, повторение учебного материала предыдущих лекций (проверка - на экзамене) | 8 |
| 3 | Изучение материалов лекционного курса по заданиям на самостоятельную проработку, выдаваемых преподавателем на занятиях (проверка - на экзамене) | 10 |
| | *Итого* | 28 |

## III. Учебно-методические материалы по дисциплине

### Основная литература

1. Семкин С. Н., Семкин А. Н. Основы информационной безопасности объектов обработки информации: Науч.-практ. пособие. Орел: 2000. 300 с.
2. Герасименко В. А., Малюк А. А. Основы защиты информации. М.: Инкомбук, 1997.540 с.

3. Герасименко В. А. Защита информации в автоматизированных системах обработки данных: В 2 кн. М.: Энергоатомиздат, 1994.
4. Хоффман Л. Дж. Современные методы защиты информации: Пер. с англ. М.: Сов. радио, 1980.
5. Грушко А. А., Тимонина Е. Е. Теоретические основы защиты информации. М: Яхтсмен, 1996.
6. Теоретические основы компьютерной безопасности: Учеб. пособие для вузов / П. Н. Девянин, О. О. Михальский, Д. И. Правиков и др. М.: Радио и связь, 2000. 192 с: ил.
7. Ярочкин В. И. Безопасность информационных систем. М: Ось-89, 1996. 320 с. (Безопасность предпринимательства).

## Дополнительная литература

1. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных: Учеб. пособие для вузов / П. Ю. Белкин, О. О. Михальский, А. С. Першаков и др. М: Радио и связь, 2000. 168 с.: ил.
2. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах: Учеб. пособие для вузов / В. Г. Проскурин, С. В. Кругов, И. В. Мацкевич. М.: радио и связь, 2000. 168 с.
3. Анин Б. Ю. Защита компьютерной информации. СПб.: БХВ - Санкт-Петербург, 2000. 384 с: ил.
4. Мельников В. В. Защита информации в компьютерных системах. М.: Финансы и статистика: Электроинформ, 1997.
5. Гайкович В. Ю., Першин А. Ю. Безопасность электронных банковских систем. М.: Единая Европа, 1994.
6. Ярочкин В. И. Система безопасности фирмы, 2-е изд. М.: Ось-89, 1999. 192 с.
7. Терминологические основы проблематики информационной безопасности // Мат. к заседанию межвед. междисциплинарного сем. по науч. проблемам информ. безопасности 1 марта 2001 г. М.: МГУ, 2001.
8. Расторгуев С. П. Программные методы защиты информации в компьютерах и сетях. М.: Яхтсмен, 1993.

**Законодательство**

1. Конституция РФ.
2. Доктрина информационной безопасности РФ.
3. ФЗ «Об информации, информатизации и защите информации».
4. ФЗ «О безопасности».
5. ФЗ «О государственной тайне».
6. ФЗ «О связи».
7. ФЗ «О лицензировании отдельных видов деятельности».
8. ФЗ «Об электронной цифровой подписи».

# Приложение 2

# ИНДИВИДУАЛЬНЫЕ ЗАДАНИЯ

Индивидуальные задания состоят из двух частей, взаимосвязанных друг с другом по объекту защиты информации. Объект необходимо исследовать таким образом, чтобы можно было применить все основные элементы защиты информации, т. е. определяя местоположение, внешние и внутренние характеристики с учетом естественных событий. Однако уточнение характеристик не должно приводить к абсолютной конкретизации объекта, так как в этом случае будет затруднен анализ объекта.

## Первое задание

Для выполнения первой части необходимо для выбранного определенного объекта защиты информации описать объект защиты, провести анализ защищенности объекта защиты информации по следующим пунктам.

1. Виды угроз.
2. Характер происхождения угроз.
3. Классы каналов несанкционированного получения информации;
4. Источники появления угроз.
5. Причины нарушения целостности информации.
6. Потенциально возможные злоумышленные действия.
7. Определить класс защиты информации.

## Второе задание

Для выполнения второго задания предложить анализ увеличения защищенности объекта защиты информации по следующим пунктам.

1. Определить требования к защите информации.
2. Классифицировать автоматизированную систему.
3. Определить факторы, влияющие на требуемый уровень защиты информации.
4. Выбрать или разработать способы и средства защиты информации;

5. Построить архитектуру систем защиты информации.
6. Сформулировать рекомендации по увеличению уровня защищенности.

Наименование объекта защиты информации:

1. Одиночно стоящий компьютер в бухгалтерии.
2. Сервер в бухгалтерии.
3. Почтовый сервер.
4. Веб-сервер.
5. Компьютерная сеть материальной группы.
6. Одноранговая локальная сеть без выхода в Интернет.
7. Одноранговая локальная сеть с выходом в Интернет.
8. Сеть с выделенным сервером без выхода в Интернет.
9. Сеть с выделенным сервером с выходом в Интернет.
10. Телефонная база данных (содержащая и информацию ограниченного пользования) в твердой копии и на электронных носителях.
11. Телефонная сеть.
12. Средства телекоммуникации (радиотелефон, мобильный телефон, пейджер).
13. Банковские операции (внесение денег на счет и снятие со счета).
14. Операции с банковскими пластиковыми карточками.
15. Компьютер, хранящий конфиденциальную информацию о сотрудниках предприятия.
16. Компьютер, хранящий конфиденциальную информацию о разработках предприятия.
17. Материалы для служебного пользования на твердых носителях в производстве.
18. Материалы для служебного пользования на твердых носителях на закрытом предприятии.
19. Материалы для служебного пользования на твердых носителях в архиве.
20. Материалы для служебного пользования на твердых носителях в налоговой инспекции.
21. Комната для переговоров по сделкам на охраняемой территории.
22. Комната для переговоров по сделкам на неохраняемой территории.

23. Сведения для СМИ, цензура на различных носителях информации (твердая копия, фотография, электронный носитель и др.).
24. Судебные материалы (твердая копия).
25. Паспортный стол РОВД.
26. Материалы по владельцам автомобилей (твердая копия, фотография, электронный носитель и др.).
27. Материалы по недвижимости (твердая копия, фотография, электронный носитель и др.).
28. Сведения по тоталитарным сектам и другим общественно вредным организациям.
29. Сведения по общественно полезным организациям (Красный Крест и др.).
30. Партийные списки и руководящие документы.

# Приложение 3

# ВОПРОСЫ К ЭКЗАМЕНУ

1. Теория защиты информации. Основные направления.
2. Обеспечение информационной безопасности и направления защиты.
3. Комплексность (целевая, инструментальная, структурная, функциональная, временная).
4. Требования к системе защиты информации.
5. Угрозы информации.
6. Виды угроз. Основные нарушения.
7. Характер происхождения угроз.
8. Источники угроз. Предпосылки появления угроз.
9. Система защиты информации.
10. Классы каналов несанкционированного получения информации.
11. Причины нарушения целостности информации.
12. Методы и модели оценки уязвимости информации.
13. Общая модель воздействия на информацию.
14. Общая модель процесса нарушения физической целостности информации.
15. Структурированная схема потенциально возможных злоумышленных действий в автоматизированных системах обработки данных.
16. Методологические подходы к оценке уязвимости информации.
17. Модель защиты системы с полным перекрытием.
18. Рекомендации по использованию моделей оценки уязвимости информации.
19. Допущения в моделях оценки уязвимости информации.
20. Методы определения требований к защите информации.
21. Факторы, обусловливающие конкретные требования к защите, обусловленные спецификой автоматизированной обработки информации.
22. Классификация требований к средствам защиты информации.
23. Требования к защите, определяемые структурой автоматизированной системы обработки данных.

24. Требования к защите, обусловливаемые видом защищаемой информации.
25. Требования, обусловливаемые взаимодействием пользователя с комплексом средств автоматизации.
26. Анализ существующих методик определения требований к защите информации.
27. Стандарт США «Критерии оценки гарантировано защищенных вычислительных систем в интересах Министерства обороны США». Основные положения.
28. О Руководящем документе Гостехкомиссии России «Классификация автоматизированных систем и требований по защите информации», выпущенном в 1992 г. Ч. 1.
29. Классы защищенности средств вычислительной техники от несанкционированного доступа.
30. Факторы, влияющие на требуемый уровень защиты информации.
31. Функции и задачи защиты информации. Основные положения механизмов непосредственной защиты и механизмы управления механизмами непосредственной защиты.
32. Методы формирования функций защиты.
33. События, возникающие при формировании функций защиты.
34. Классы задач функций защиты.
35. Класс задач функций защиты 1 - уменьшение степени распознавания объектов.
36. Класс задач функций защиты 2 - защита содержания обрабатываемой, хранимой и передаваемой информации.
37. Класс задач функций защиты 3 - защита информации от информационного воздействия.
38. Функции защиты информации.
39. Стратегии защиты информации.
40. Способы и средства защиты информации.
41. Способы «абсолютной системы защиты».
42. Архитектура систем защиты информации. Требования.
43. Общеметодологических принципов архитектуры системы защиты информации.
44. Построение средств защиты информации.
45. Ядро системы защиты информации.
46. Семирубежная модель защиты.

## Приложение 4

# ДОКТРИНА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

*УТВЕРЖДАЮ:*
*Президент РФ*
*9 сентября 2000 г. № Пр-1895*

**Доктрина информационной безопасности Российской Федерации представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации.**

Настоящая Доктрина служит основой для:

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

Настоящая Доктрина развивает Концепцию национальной безопасности РФ применительно к информационной сфере.

## I. Информационная безопасность Российской Федерации

### 1. Национальные интересы Российской Федерации в информационной сфере и их обеспечение

Современный этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование инфор-

мации, а также системы регулирования возникающих при этом общественных отношений. Информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности РФ. Национальная безопасность РФ существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать.

Под информационной безопасностью РФ понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.

Интересы общества в информационной сфере заключаются в обеспечении интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении России.

Интересы государства в информационной сфере заключаются в создании условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества.

На основе национальных интересов РФ в информационной сфере формируются стратегические и текущие задачи внутренней и внешней политики государства по обеспечению информационной безопасности.

Выделяются четыре основные составляющие национальных интересов РФ в информационной сфере.

Первая составляющая национальных интересов РФ в информационной сфере включает в себя соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.

Для достижения этого требуется:

- повысить эффективность использования информационной инфраструктуры в интересах общественного развития, консолидации российского общества, духовного возрождения многонационального народа РФ;
- усовершенствовать систему формирования, сохранения и рационального использования информационных ресурсов, составляющих основу научно-технического и духовного потенциала РФ;
- обеспечить конституционные права и свободы человека и гражданина свободно искать, получать, передавать, производить и распространять информацию любым законным способом, получать достоверную информацию о состоянии окружающей среды;
- обеспечить конституционные права и свободы человека и гражданина на личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, на защиту своей чести и своего доброго имени;
- укрепить механизмы правового регулирования отношений в области охраны интеллектуальной собственности, создать условия для соблюдения установленных федеральным законодательством ограничений на доступ к конфиденциальной информации;
- гарантировать свободу массовой информации и запрет цензуры;
- не допускать пропаганду и агитацию, которые способствуют разжиганию социальной, расовой, национальной или религиозной ненависти и вражды;
- обеспечить запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия и другой информации, доступ к которой ограничен федеральным законодательством.

Вторая составляющая национальных интересов РФ в информационной сфере включает в себя информационное обеспечение государственной политики РФ, связанное с доведением до российской и международной общественности достоверной информации о государственной политике РФ, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам.

Для достижения этого требуется:

- укреплять государственные средства массовой информации, расширять их возможности по своевременному доведению достоверной информации до российских и иностранных граждан;

- интенсифицировать формирование открытых государственных информационных ресурсов, повысить эффективность их хозяйственного использования.

Третья составляющая национальных интересов РФ в информационной сфере включает в себя развитие современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов. В современных условиях только на этой основе можно решать проблемы создания наукоемких технологий, технологического перевооружения промышленности, приумножения достижений отечественной науки и техники. Россия должна занять достойное место среди мировых лидеров микроэлектронной и компьютерной промышленности.

Для достижения этого требуется:

- развивать и совершенствовать инфраструктуру единого информационного пространства РФ;
- развивать отечественную индустрию информационных услуг и повышать эффективность использования государственных информационных ресурсов;
- развивать производство в РФ конкурентоспособных средств и систем информатизации, телекоммуникации и связи, расширять участие России в международной кооперации производителей этих средств и систем;
- обеспечить государственную поддержку отечественных фундаментальных и прикладных исследований, разработок в сферах информатизации, телекоммуникации и связи.

Четвертая составляющая национальных интересов РФ в информационной сфере включает в себя защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России.

В этих целях необходимо:

- повысить безопасность информационных систем, включая сети связи, прежде всего безопасность первичных сетей связи и информационных систем федеральных органов государственной власти, органов государственной власти субъектов РФ, финансово-кредитной и бан-

ковской сфер, сферы хозяйственной деятельности, а также систем и средств информатизации вооружения и военной техники, систем управления войсками и оружием, экологически опасными и экономически важными производствами;

- интенсифицировать развитие отечественного производства аппаратных и программных средств защиты информации и методов контроля за их эффективностью;
- обеспечить защиту сведений, составляющих государственную тайну;
- расширять международное сотрудничество РФ в области развития и безопасного использования информационных ресурсов, противодействия угрозе развязывания противоборства в информационной сфере.

## 2. Виды угроз информационной безопасности Российской Федерации

По своей общей направленности угрозы информационной безопасности РФ подразделяются на следующие виды:

- угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;
- угрозы информационному обеспечению государственной политики РФ;
- угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;
- угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.

Угрозами конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России могут являться:

- принятие федеральными органами государственной власти, органами государственной власти субъектов РФ нормативных правовых актов,

ущемляющих конституционные права и свободы граждан в области духовной жизни и информационной деятельности;

- создание монополий на формирование, получение и распространение информации в РФ, в том числе с использованием телекоммуникационных систем;
- противодействие, в том числе со стороны криминальных структур, реализации гражданами своих конституционных прав на личную и семейную тайну, тайну переписки, телефонных переговоров и иных сообщений;
- нерациональное, чрезмерное ограничение доступа к общественно необходимой информации;
- противоправное применение специальных средств воздействия на индивидуальное, групповое и общественное сознание;
- неисполнение федеральными органами государственной власти, органами государственной власти субъектов РФ, органами местного самоуправления, организациями и гражданами требований федерального законодательства, регулирующего отношения в информационной сфере;
- неправомерное ограничение доступа граждан к открытым информационным ресурсам федеральных органов государственной власти, органов государственной власти субъектов РФ, органов местного самоуправления, к открытым архивным материалам, к другой открытой социально значимой информации;
- дезорганизация и разрушение системы накопления и сохранения культурных ценностей, включая архивы;
- нарушение конституционных прав и свобод человека и гражданина в области массовой информации;
- вытеснение российских информационных агентств, средств массовой информации с внутреннего информационного рынка и усиление зависимости духовной, экономической и политической сфер общественной жизни России от зарубежных информационных структур;
- девальвация духовных ценностей, пропаганда образцов массовой культуры, основанных на культе насилия, на духовных и нравственных ценностях, противоречащих ценностям, принятым в российском обществе;
- снижение духовного, нравственного и творческого потенциала населения России, что существенно осложнит подготовку трудовых ре-

сурсов для внедрения и использования новейших технологий, в том числе информационных;

- манипулирование информацией (дезинформация, сокрытие или искажение информации).

Угрозами информационному обеспечению государственной политики РФ могут являться:

- монополизация информационного рынка России, его отдельных секторов отечественными и зарубежными информационными структурами;
- блокирование деятельности государственных средств массовой информации по информированию российской и зарубежной аудитории;
- низкая эффективность информационного обеспечения государственной политики РФ вследствие дефицита квалифицированных кадров, отсутствия системы формирования и реализации государственной информационной политики.

Угрозами развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов могут являться:

- противодействие доступу РФ к новейшим информационным технологиям, взаимовыгодному и равноправному участию российских производителей в мировом разделении труда в индустрии информационных услуг, средств информатизации, телекоммуникации и связи, информационных продуктов, а также создание условий для усиления технологической зависимости России в области современных информационных технологий;
- закупка органами государственной власти импортных средств информатизации, телекоммуникации и связи при наличии отечественных аналогов, не уступающих по своим характеристикам зарубежным образцам;
- вытеснение с отечественного рынка российских производителей средств информатизации, телекоммуникации и связи;
- увеличение оттока за рубеж специалистов и правообладателей интеллектуальной собственности.

Угрозами безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России, могут являться:

- противоправные сбор и использование информации;
- нарушения технологии обработки информации;
- внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;
- разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;
- уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;
- воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации;
- компрометация ключей и средств криптографической защиты информации;
- утечка информации по техническим каналам;
- внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти, предприятий, учреждений и организаций независимо от формы собственности;
- уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;
- перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации;
- использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии российской информационной инфраструктуры;
- несанкционированный доступ к информации, находящейся в банках и базах данных;
- нарушение законных ограничений на распространение информации.

## 3. Источники угроз информационной безопасности Российской Федерации

Источники угроз информационной безопасности РФ подразделяются на внешние и внутренние. К внешним источникам относятся:

- деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов РФ в информационной сфере;
- стремление ряда стран к доминированию и ущемлению интересов России в мировом информационном пространстве, вытеснению ее с внешнего и внутреннего информационных рынков;
- обострение международной конкуренции за обладание информационными технологиями и ресурсами;
- деятельность международных террористических организаций;
- увеличение технологического отрыва ведущих держав мира и наращивание их возможностей по противодействию созданию конкурентоспособных российских информационных технологий;
- деятельность космических, воздушных, морских и наземных технических и иных средств (видов) разведки иностранных государств;
- разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним.

К внутренним источникам относятся:

- критическое состояние отечественных отраслей промышленности;
- неблагоприятная криминогенная обстановка, сопровождающаяся тенденциями сращивания государственных и криминальных структур в информационной сфере, получения криминальными структурами доступа к конфиденциальной информации, усиления влияния организованной преступности на жизнь общества, снижения степени защищенности законных интересов граждан, общества и государства в информационной сфере;
- недостаточная координация деятельности федеральных органов государственной власти, органов государственной власти субъектов РФ

по формированию и реализации единой государственной политики в области обеспечения информационной безопасности РФ;

- недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика;
- неразвитость институтов гражданского общества и недостаточный государственный контроль за развитием информационного рынка России;
- недостаточное финансирование мероприятий по обеспечению информационной безопасности РФ;
- недостаточная экономическая мощь государства;
- снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности;
- недостаточная активность федеральных органов государственной власти, органов государственной власти субъектов РФ в информировании общества о своей деятельности, в разъяснении принимаемых решений, в формировании открытых государственных ресурсов и развитии системы доступа к ним граждан;
- отставание России от ведущих стран мира по уровню информатизации федеральных органов государственной власти, органов государственной власти субъектов РФ и органов местного самоуправления, кредитно-финансовой сферы, промышленности, сельского хозяйства, образования, здравоохранения, сферы услуг и быта граждан.

## 4. Состояние информационной безопасности Российской Федерации и основные задачи по ее обеспечению

За последние годы в РФ реализован комплекс мер по совершенствованию обеспечения ее информационной безопасности.

Начато формирование базы правового обеспечения информационной безопасности. Приняты Закон РФ «О государственной тайне», Основы законодательства РФ об Архивном фонде РФ и архивах, Федеральные законы «Об информации, информатизации и защите информации», «Об участии в международном информационном обмене», ряд других законов, развернута работа по созданию механизмов их реализации, подготовке законопроектов, регламентирующих общественные отношения в информационной сфере.

Осуществлены мероприятия по обеспечению информационной безопасности в федеральных органах государственной власти, органах государственной власти субъектов РФ, на предприятиях, в учреждениях и организациях независимо от формы собственности. Развернуты работы по созданию защищенной информационно-телекоммуникационной системы специального назначения в интересах органов государственной власти.

Успешному решению вопросов обеспечения информационной безопасности РФ способствуют государственная система защиты информации, система защиты государственной тайны, системы лицензирования деятельности в области защиты государственной тайны и системы сертификации средств защиты информации.

Вместе с тем анализ состояния информационной безопасности РФ показывает, что ее уровень не в полной мере соответствует потребностям общества и государства.

Современные условия политического и социально-экономического развития страны вызывают обострение противоречий между потребностями общества в расширении свободного обмена информацией и необходимостью сохранения отдельных регламентированных ограничений на ее распространение.

Противоречивость и неразвитость правового регулирования общественных отношений в информационной сфере приводят к серьезным негативным последствиям. Так, недостаточность нормативного правового регулирования отношений в области реализации возможностей конституционных ограничений свободы массовой информации в интересах защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороноспособности страны и безопасности государства существенно затрудняет поддержание необходимого баланса интересов личности, общества и государства в информационной сфере. Несовершенное нормативное правовое регулирование отношений в области массовой информации затрудняет формирование на территории РФ конкурентоспособных российских информационных агентств и средств массовой информации.

Необеспеченность прав граждан на доступ к информации, манипулирование информацией вызывают негативную реакцию населения, что в ряде случаев ведет к дестабилизации социально-политической обстановки в обществе.

Закрепленные в Конституции РФ права граждан на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки практически не имеют достаточного правового, организационного и технического обеспечения. Неудовлетворительно организована защита собираемых федеральными органами государственной власти, органами

государственной власти субъектов РФ, органами местного самоуправления данных о физических лицах (персональных данных).

Нет четкости при проведении государственной политики в области формирования российского информационного пространства, развития системы массовой информации, организации международного информационного обмена и интеграции информационного пространства России в мировое информационное пространство, что создает условия для вытеснения российских информационных агентств, средств массовой информации с внутреннего информационного рынка и деформации структуры международного информационного обмена.

Недостаточна государственная поддержка деятельности российских информационных агентств по продвижению их продукции на зарубежный информационный рынок.

Ухудшается ситуация с обеспечением сохранности сведений, составляющих государственную тайну.

Серьезный урон нанесен кадровому потенциалу научных и производственных коллективов, действующих в области создания средств информатизации, телекоммуникации и связи, в результате массового ухода из этих коллективов наиболее квалифицированных специалистов.

Отставание отечественных информационных технологий вынуждает федеральные органы государственной власти, органы государственной власти субъектов РФ и органы местного самоуправления при создании информационных систем идти по пути закупок импортной техники и привлечения иностранных фирм, из-за чего повышается вероятность несанкционированного доступа к обрабатываемой информации и возрастает зависимость России от иностранных производителей компьютерной и телекоммуникационной техники, а также программного обеспечения.

В связи с интенсивным внедрением зарубежных информационных технологий в сферы деятельности личности, общества и государства, а также с широким применением открытых информационно-телекоммуникационных систем, интеграцией отечественных информационных систем и международных информационных систем возросли угрозы применения «информационного оружия» против информационной инфраструктуры России. Работы по адекватному комплексному противодействию этим угрозам ведутся при недостаточной координации и слабом бюджетном финансировании. Недостаточное внимание уделяется развитию средств космической разведки и радиоэлектронной борьбы.

Сложившееся положение дел в области обеспечения информационной безопасности РФ требует безотлагательного решения таких задач, как:

- разработка основных направлений государственной политики в области обеспечения информационной безопасности РФ, а также мероприятий и механизмов, связанных с реализацией этой политики;
- развитие и совершенствование системы обеспечения информационной безопасности РФ, реализующей единую государственную политику в этой области, включая совершенствование форм, методов и средств выявления, оценки и прогнозирования угроз информационной безопасности РФ, а также системы противодействия этим угрозам;
- разработка федеральных целевых программ обеспечения информационной безопасности РФ;
- разработка критериев и методов оценки эффективности систем и средств обеспечения информационной безопасности РФ, а также сертификации этих систем и средств;
- совершенствование нормативной правовой базы обеспечения информационной безопасности РФ, включая механизмы реализации прав граждан на получение информации и доступ к ней, формы и способы реализации правовых норм, касающихся взаимодействия государства со средствами массовой информации;
- установление ответственности должностных лиц федеральных органов государственной власти, органов государственной власти субъектов РФ, органов местного самоуправления, юридических лиц и граждан за соблюдение требований информационной безопасности;
- координация деятельности федеральных органов государственной власти, органов государственной власти субъектов РФ, предприятий, учреждений и организаций независимо от формы собственности в области обеспечения информационной безопасности РФ;
- развитие научно-практических основ обеспечения информационной безопасности РФ с учетом современной геополитической ситуации, условий политического и социально-экономического развития России и реальности угроз применения «информационного оружия»;
- разработка и создание механизмов формирования и реализации государственной информационной политики России;
- разработка методов повышения эффективности участия государства в формировании информационной политики государственных телерадиовещательных организаций, других государственных средств массовой информации;

- обеспечение технологической независимости РФ в важнейших областях информатизации, телекоммуникации и связи, определяющих ее безопасность, и в первую очередь в области создания специализированной вычислительной техники для образцов вооружения и военной техники;
- разработка современных методов и средств защиты информации, обеспечения безопасности информационных технологий, и прежде всего используемых в системах управления войсками и оружием, экологически опасными и экономически важными производствами;
- развитие и совершенствование государственной системы защиты информации и системы защиты государственной тайны;
- создание и развитие современной защищенной технологической основы управления государством в мирное время, в чрезвычайных ситуациях и в военное время;
- расширение взаимодействия с международными и зарубежными органами и организациями при решении научно-технических и правовых вопросов обеспечения безопасности информации, передаваемой с помощью международных телекоммуникационных систем и систем связи;
- обеспечение условий для активного развития российской информационной инфраструктуры, участия России в процессах создания и использования глобальных информационных сетей и систем;
- создание единой системы подготовки кадров в области информационной безопасности и информационных технологий.

# II. Методы обеспечения информационной безопасности Российской Федерации

## 5. Общие методы обеспечения информационной безопасности Российской Федерации

Общие методы обеспечения информационной безопасности РФ разделяются на правовые, организационно-технические и экономические.

К правовым методам обеспечения информационной безопасности РФ относится разработка нормативных правовых актов, регламентирующих отношения в информационной сфере, и нормативных методических документов по вопросам обеспечения информационной безопасности РФ. Наиболее важными направлениями этой деятельности являются:

- внесение изменений и дополнений в законодательство РФ, регулирующее отношения в области обеспечения информационной безопасности, в целях создания и совершенствования системы обеспечения информационной безопасности РФ, устранения внутренних противоречий в федеральном законодательстве, противоречий, связанных с международными соглашениями, к которым присоединилась РФ, и противоречий между федеральными законодательными актами и законодательными актами субъектов РФ, а также в целях конкретизации правовых норм, устанавливающих ответственность за правонарушения в области обеспечения информационной безопасности РФ;
- законодательное разграничение полномочий в области обеспечения информационной безопасности РФ между федеральными органами государственной власти и органами государственной власти субъектов РФ, определение целей, задач и механизмов участия в этой деятельности общественных объединений, организаций и граждан;
- разработка и принятие нормативных правовых актов РФ, 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;
- уточнение статуса иностранных информационных агентств, средств массовой информации и журналистов, а также инвесторов при привлечении иностранных инвестиций для развития информационной инфраструктуры России;
- 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;
- создание правовой базы для формирования в РФ региональных структур обеспечения информационной безопасности.

Организационно-техническими методами обеспечения информационной безопасности РФ являются:

- создание и совершенствование системы обеспечения информационной безопасности РФ;
- усиление правоприменительной деятельности федеральных органов исполнительной власти, органов исполнительной власти субъектов РФ, включая предупреждение и пресечение правонарушений в информационной сфере, а также выявление, изобличение и привлечение к ответственности лиц, совершивших преступления и другие правонарушения в этой сфере;
- разработка, использование и совершенствование средств защиты информации и методов контроля эффективности этих средств, развитие защищенных телекоммуникационных систем, повышение надежности специального программного обеспечения;
- создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи;
- выявление технических устройств и программ, представляющих опасность для нормального функционирования информационно-телекоммуникационных систем, предотвращение перехвата информации по техническим каналам, применение криптографических средств защиты информации при ее хранении, обработке и передаче по каналам связи, контроль за выполнением специальных требований по защите информации;
- сертификация средств защиты информации, лицензирование деятельности в области защиты государственной тайны, стандартизация способов и средств защиты информации;
- совершенствование системы сертификации телекоммуникационного оборудования и программного обеспечения автоматизированных систем обработки информации по требованиям информационной безопасности;
- контроль за действиями персонала в защищенных информационных системах, подготовка кадров в области обеспечения информационной безопасности РФ;
- формирование системы мониторинга показателей и характеристик информационной безопасности РФ в наиболее важных сферах жизни и деятельности общества и государства.

Экономические методы обеспечения информационной безопасности РФ включают в себя:

- разработку программ обеспечения информационной безопасности РФ и определение порядка их финансирования;
- совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-технических методов защиты информации, создание системы страхования информационных рисков физических и юридических лиц.

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

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

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

В сфере экономики. Обеспечение информационной безопасности РФ в сфере экономики играет ключевую роль в обеспечении национальной безопасности РФ.

Воздействию угроз информационной безопасности РФ в сфере экономики наиболее подвержены:

- система государственной статистики;
- кредитно-финансовая система;
- информационные и учетные автоматизированные системы подразделений федеральных органов исполнительной власти, обеспечивающих деятельность общества и государства в сфере экономики;
- системы бухгалтерского учета предприятий, учреждений и организаций независимо от формы собственности;

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

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

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

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

Недостаточность нормативной правовой базы, определяющей ответственность хозяйствующих субъектов за недостоверность или сокрытие сведений об их коммерческой деятельности, о потребительских свойствах производимых ими товаров и услуг, о результатах их хозяйственной деятельности, об инвестициях и тому подобном, препятствует нормальному функционированию хозяйствующих субъектов. В то же время существенный экономический ущерб хозяйствующим субъектам может быть нанесен вследствие разглашения информации, содержащей коммерческую тайну. В системах сбора, обработки, хранения и передачи финансовой, биржевой, налоговой, таможенной информации наиболее опасны противоправное копирование информации и ее искажение вследствие преднамеренных или случайных нарушений технологии работы с информацией, несанкционированного доступа к ней. Это касается и федераль-

ных органов исполнительной власти, занятых формированием и распространением информации о внешнеэкономической деятельности РФ.

Основными мерами по обеспечению информационной безопасности РФ в сфере экономики являются:

- организация и осуществление государственного контроля за созданием, развитием и защитой систем и средств сбора, обработки, хранения и передачи статистической, финансовой, биржевой, налоговой, таможенной информации;
- коренная перестройка системы государственной статистической отчетности в целях обеспечения достоверности, полноты и защищенности информации, осуществляемая путем введения строгой юридической ответственности должностных лиц за подготовку первичной информации, организацию контроля за деятельностью этих лиц и служб обработки и анализа статистической информации, а также путем ограничения коммерциализации такой информации;
- разработка национальных сертифицированных средств защиты информации и внедрение их в системы и средства сбора, обработки, хранения и передачи статистической, финансовой, биржевой, налоговой, таможенной информации;
- разработка и внедрение национальных защищенных систем электронных платежей на базе интеллектуальных карт, систем электронных денег и электронной торговли, стандартизация этих систем, а также разработка нормативной правовой базы, регламентирующей их использование;
- совершенствование нормативной правовой базы, регулирующей информационные отношения в сфере экономики;
- совершенствование методов отбора и подготовки персонала для работы в системах сбора, обработки, хранения и передачи экономической информации.

В сфере внутренней политики. Наиболее важными объектами обеспечения информационной безопасности РФ в сфере внутренней политики являются:

- конституционные права и свободы человека и гражданина;
- конституционный строй, национальное согласие, стабильность государственной власти, суверенитет и территориальная целостность РФ;
- открытые информационные ресурсы федеральных органов исполнительной власти и средств массовой информации.

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

- нарушение конституционных прав и свобод граждан, реализуемых в информационной сфере;
- недостаточное правовое регулирование отношений в области прав различных политических сил на использование средств массовой информации для пропаганды своих идей;
- распространение дезинформации о политике РФ, деятельности федеральных органов государственной власти, событиях, происходящих в стране и за рубежом;
- деятельность общественных объединений, направленная на насильственное изменение основ конституционного строя и нарушение целостности РФ, разжигание социальной, расовой, национальной и религиозной вражды, на распространение этих идей в средствах массовой информации.

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

- создание системы противодействия монополизации отечественными и зарубежными структурами составляющих информационной инфраструктуры, включая рынок информационных услуг и средства массовой информации;
- активизация контрпропагандистской деятельности, направленной на предотвращение негативных последствий распространения дезинформации о внутренней политике России.

В сфере внешней политики. К наиболее важным объектам обеспечения информационной безопасности РФ в сфере внешней политики относятся:

- информационные ресурсы федеральных органов исполнительной власти, реализующих внешнюю политику РФ, российских представительств и организаций за рубежом, представительств РФ при международных организациях;
- информационные ресурсы представительств федеральных органов исполнительной власти, реализующих внешнюю политику РФ, на территориях субъектов РФ;
- информационные ресурсы российских предприятий, учреждений и организаций, подведомственных федеральным органам исполнительной власти, реализующим внешнюю политику РФ;

- блокирование деятельности российских средств массовой информации по разъяснению зарубежной аудитории целей и основных направлений государственной политики РФ, ее мнения по социально значимым событиям российской и международной жизни.

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

- информационное воздействие иностранных политических, экономических, военных и информационных структур на разработку и реализацию стратегии внешней политики РФ;
- распространение за рубежом дезинформации о внешней политике РФ;
- нарушение прав российских граждан и юридических лиц в информационной сфере за рубежом;
- попытки несанкционированного доступа к информации и воздействия на информационные ресурсы, информационную инфраструктуру федеральных органов исполнительной власти, реализующих внешнюю политику РФ, российских представительств и организаций за рубежом, представительств РФ при международных организациях.

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

- нарушение установленного порядка сбора, обработки, хранения и передачи информации в федеральных органах исполнительной власти, реализующих внешнюю политику РФ, и на подведомственных им предприятиях, в учреждениях и организациях;
- информационно-пропагандистская деятельность политических сил, общественных объединений, средств массовой информации и отдельных лиц, искажающая стратегию и тактику внешнеполитической деятельности РФ;
- недостаточная информированность населения о внешнеполитической деятельности РФ.

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

- разработка основных направлений государственной политики в области совершенствования информационного обеспечения внешнеполитического курса РФ;
- разработка и реализация комплекса мер по усилению информационной безопасности информационной инфраструктуры федеральных

органов исполнительной власти, реализующих внешнюю политику РФ, российских представительств и организаций за рубежом, представительств РФ при международных организациях;

- создание российским представительствам и организациям за рубежом условий для работы по нейтрализации распространяемой там дезинформации о внешней политике РФ;
- совершенствование информационного обеспечения работы по противодействию нарушениям прав и свобод российских граждан и юридических лиц за рубежом;
- совершенствование информационного обеспечения субъектов РФ по вопросам внешнеполитической деятельности, которые входят в их компетенцию.

В области науки и техники. Наиболее важными объектами обеспечения информационной безопасности РФ в области науки и техники являются:

- результаты фундаментальных, поисковых и прикладных научных исследований, потенциально важные для научно-технического, технологического и социально-экономического развития страны, включая сведения, утрата которых может нанести ущерб национальным интересам и престижу РФ;
- открытия, незапатентованные технологии, промышленные образцы, полезные модели и экспериментальное оборудование;
- научно - технические кадры и система их подготовки;
- системы управления сложными исследовательскими комплексами (ядерными реакторами, ускорителями элементарных частиц, плазменными генераторами и другими).

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

- стремление развитых иностранных государств получить противоправный доступ к научно-техническим ресурсам России для использования полученных российскими учеными результатов в собственных интересах;
- создание льготных условий на российском рынке для иностранной научно-технической продукции и стремление развитых стран в то же время ограничить развитие научно-технического потенциала России (скупка акций передовых предприятий с их последующим пере-

профилированием, сохранение экспортно-импортных ограничений и тому подобное);

- политику западных стран, направленную на дальнейшее разрушение унаследованного от СССР единого научно - технического пространства государств - участников Содружества Независимых Государств за счет переориентации на западные страны их научно-технических связей, а также отдельных, наиболее перспективных научных коллективов;
- активизацию деятельности иностранных государственных и коммерческих предприятий, учреждений и организаций в области промышленного шпионажа с привлечением к ней разведывательных и специальных служб.

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

- сохраняющуюся сложную экономическую ситуацию в России, ведущую к резкому снижению финансирования научно-технической деятельности, временному падению престижа научно-технической сферы, утечке за рубеж идей и передовых разработок;
- неспособность предприятий национальных отраслей электронной промышленности производить на базе новейших достижений микроэлектроники, передовых информационных технологий конкурентоспособную наукоемкую продукцию, позволяющую обеспечить достаточный уровень технологической независимости России от зарубежных стран, что приводит к вынужденному широкому использованию импортных программно-аппаратных средств при создании и развитии в России информационной инфраструктуры;
- серьезные проблемы в области патентной защиты результатов научно-технической деятельности российских ученых;
- сложности реализации мероприятий по защите информации, особенно на акционированных предприятиях, в научно-технических учреждениях и организациях.

Реальный путь противодействия угрозам информационной безопасности РФ в области науки и техники - это совершенствование законодательства РФ, регулирующего отношения в данной области, и механизмов его реализации. В этих целях государство должно способствовать созданию системы оценки возможного ущерба от реализации угроз наиболее важным объектам обеспечения информационной безопасности РФ в области науки и техники, включая общественные научные советы и органи-

зации независимой экспертизы, вырабатывающие рекомендации для федеральных органов государственной власти и органов государственной власти субъектов РФ по предотвращению противоправного или неэффективного использования интеллектуального потенциала России.

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

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

- достоинство личности, свобода совести, включая право свободно выбирать, иметь и распространять религиозные и иные убеждения и действовать в соответствии с ними, свобода мысли и слова (за исключением пропаганды или агитации, возбуждающих социальную, расовую, национальную или религиозную ненависть и вражду), а также свобода литературного, художественного, научного, технического и других видов творчества, преподавания;
- свобода массовой информации;
- неприкосновенность частной жизни, личная и семейная тайна;
- русский язык как фактор духовного единения народов многонациональной России, язык межгосударственного общения народов государств - участников Содружества Независимых Государств;
- языки, нравственные ценности и культурное наследие народов и народностей РФ;
- объекты интеллектуальной собственности.

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

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

- ухудшение состояния и постепенный упадок объектов российского культурного наследия, включая архивы, музейные фонды, библиотеки, памятники архитектуры, ввиду недостаточного финансирования соответствующих программ и мероприятий;
- возможность нарушения общественной стабильности, нанесение вреда здоровью и жизни граждан вследствие деятельности религиозных объединений, проповедующих религиозный фундаментализм, а также тоталитарных религиозных сект;
- использование зарубежными специальными службами средств массовой информации, действующих на территории РФ, для нанесения ущерба обороноспособности страны и безопасности государства, распространения дезинформации;
- неспособность современного гражданского общества России обеспечить формирование у подрастающего поколения и поддержание в обществе общественно необходимых нравственных ценностей, патриотизма и гражданской ответственности за судьбу страны.

Основными направлениями обеспечения информационной безопасности РФ в сфере духовной жизни являются:

- развитие в России основ гражданского общества;
- создание социально-экономических условий для осуществления творческой деятельности и функционирования учреждений культуры;
- выработка цивилизованных форм и способов общественного контроля за формированием в обществе духовных ценностей, отвечающих национальным интересам страны, воспитанием патриотизма и гражданской ответственности за ее судьбу;
- совершенствование законодательства РФ, регулирующего отношения в области конституционных ограничений прав и свобод человека и гражданина;
- государственная поддержка мероприятий по сохранению и возрождению культурного наследия народов и народностей РФ;
- формирование правовых и организационных механизмов обеспечения конституционных прав и свобод граждан, повышения их правовой культуры в интересах противодействия сознательному или непреднамеренному нарушению этих конституционных прав и свобод в сфере духовной жизни;
- разработка действенных организационно-правовых механизмов доступа средств массовой информации и граждан к открытой информа-

ции о деятельности федеральных органов государственной власти и общественных объединений, обеспечение достоверности сведений о социально значимых событиях общественной жизни, распространяемых через средства массовой информации;

- разработка специальных правовых и организационных механизмов недопущения противоправных информационно-психологических воздействий на массовое сознание общества, неконтролируемой коммерциализации культуры и науки, а также обеспечивающих сохранение культурных и исторических ценностей народов и народностей РФ, рациональное использование накопленных обществом информационных ресурсов, составляющих национальное достояние;
- введение запрета на использование эфирного времени в электронных средствах массовой информации для проката программ, пропагандирующих насилие и жестокость, антиобщественное поведение;
- противодействие негативному влиянию иностранных религиозных организаций и миссионеров.

В общегосударственных информационных и телекоммуникационных системах. Основными объектами обеспечения информационной безопасности РФ в общегосударственных информационных и телекоммуникационных системах являются:

- информационные ресурсы, содержащие сведения, отнесенные к государственной тайне, и конфиденциальную информацию;
- средства и системы информатизации (средства вычислительной техники, информационно-вычислительные комплексы, сети и системы), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), автоматизированные системы управления, системы связи и передачи данных, осуществляющие прием, обработку, хранение и передачу информации ограниченного доступа, их информативные физические поля;
- технические средства и системы, обрабатывающие открытую информацию, но размещенные в помещениях, в которых обрабатывается информация ограниченного доступа, а также сами помещения, предназначенные для обработки такой информации;
- помещения, предназначенные для ведения закрытых переговоров, а также переговоров, в ходе которых оглашаются сведения ограниченного доступа.

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

- деятельность специальных служб иностранных государств, преступных сообществ, организаций и групп, противозаконная деятельность отдельных лиц, направленная на получение несанкционированного доступа к информации и осуществление контроля за функционированием информационных и телекоммуникационных систем;
- вынужденное в силу объективного отставания отечественной промышленности использование при создании и развитии информационных и телекоммуникационных систем импортных программно-аппаратных средств;
- нарушение установленного регламента сбора, обработки и передачи информации, преднамеренные действия и ошибки персонала информационных и телекоммуникационных систем, отказ технических средств и сбои программного обеспечения в информационных и телекоммуникационных системах;
- использование несертифицированных в соответствии с требованиями безопасности средств и систем информатизации и связи, а также средств защиты информации и контроля их эффективности;
- привлечение к работам по созданию, развитию и защите информационных и телекоммуникационных систем организаций и фирм, не имеющих государственных лицензий на осуществление этих видов деятельности.

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

- предотвращение перехвата информации из помещений и с объектов, а также информации, передаваемой по каналам связи с помощью технических средств;
- исключение несанкционированного доступа к обрабатываемой или хранящейся в технических средствах информации;
- предотвращение утечки информации по техническим каналам, возникающей при эксплуатации технических средств ее обработки, хранения и передачи;
- предотвращение специальных программно-технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств информатизации;

- обеспечение информационной безопасности при подключении общегосударственных информационных и телекоммуникационных систем к внешним информационным сетям, включая международные;
- обеспечение безопасности конфиденциальной информации при взаимодействии информационных и телекоммуникационных систем различных классов защищенности;
- выявление внедренных на объекты и в технические средства электронных устройств перехвата информации.

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

- лицензирование деятельности организаций в области защиты информации;
- аттестация объектов информатизации по выполнению требований обеспечения защиты информации при проведении работ, связанных с использованием сведений, составляющих государственную тайну;
- сертификация средств защиты информации и контроля эффективности их использования, а также защищенности информации от утечки по техническим каналам систем и средств информатизации и связи;
- введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите;
- создание и применение информационных и автоматизированных систем управления в защищенном исполнении.

В сфере обороны. К объектам обеспечения информационной безопасности РФ в сфере обороны относятся:

- информационная инфраструктура центральных органов военного управления и органов военного управления видов Вооруженных Сил РФ и родов войск, объединений, соединений, воинских частей и организаций, входящих в Вооруженные Силы РФ, научно-исследовательских учреждений Министерства обороны РФ;
- информационные ресурсы предприятий оборонного комплекса и научно-исследовательских учреждений, выполняющих государственные оборонные заказы либо занимающихся оборонной проблематикой;
- программно-технические средства автоматизированных и автоматических систем управления войсками и оружием, вооружения и военной техники, оснащенных средствами информатизации;

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

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

- все виды разведывательной деятельности зарубежных государств;
- информационно-технические воздействия (в том числе радиоэлектронная борьба, проникновение в компьютерные сети) со стороны вероятных противников;
- диверсионно-подрывная деятельность специальных служб иностранных государств, осуществляемая методами информационно-психологического воздействия;
- деятельность иностранных политических, экономических и военных структур, направленная против интересов РФ в сфере обороны.

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

- нарушение установленного регламента сбора, обработки, хранения и передачи информации, находящейся в штабах и учреждениях Министерства обороны РФ, на предприятиях оборонного комплекса;
- преднамеренные действия, а также ошибки персонала информационных и телекоммуникационных систем специального назначения;,
- ненадежное функционирование информационных и телекоммуникационных систем специального назначения;
- возможная информационно-пропагандистская деятельность, подрывающая престиж Вооруженных Сил РФ и их боеготовность;
- нерешенность вопросов защиты интеллектуальной собственности предприятий оборонного комплекса, приводящая к утечке за рубеж ценнейших государственных информационных ресурсов;
- нерешенность вопросов социальной защиты военнослужащих и членов их семей.

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

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

- систематическое выявление угроз и их источников, структуризация целей обеспечения информационной безопасности в сфере обороны и определение соответствующих практических задач;
- проведение сертификации общего и специального программного обеспечения, пакетов прикладных программ и средств защиты информации в существующих и создаваемых автоматизированных системах управления военного назначения и системах связи, имеющих в своем составе элементы вычислительной техники;
- постоянное совершенствование средств защиты информации от несанкционированного доступа, развитие защищенных систем связи и управления войсками и оружием, повышение надежности специального программного обеспечения;
- совершенствование структуры функциональных органов системы обеспечения информационной безопасности в сфере обороны и координация их взаимодействия;
- совершенствование приемов и способов стратегической и оперативной маскировки, разведки и радиоэлектронной борьбы, методов и средств активного противодействия информационно-пропагандистским и психологическим операциям вероятного противника;
- подготовка специалистов в области обеспечения информационной безопасности в сфере обороны.

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

- информационные ресурсы федеральных органов исполнительной власти, реализующих правоохранительные функции, судебных органов, их информационно-вычислительных центров, научно-исследовательских учреждений и учебных заведений, содержащие специальные сведения и оперативные данные служебного характера;
- информационно-вычислительные центры, их информационное, техническое, программное и нормативное обеспечение;
- информационная инфраструктура (информационно-вычислительные сети, пункты управления, узлы и линии связи).

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

- разведывательная деятельность специальных служб иностранных государств, международных преступных сообществ, организаций и групп, связанная со сбором сведений, раскрывающих задачи, планы деятельности, техническое оснащение, методы работы и места дислокации специальных подразделений и органов внутренних дел РФ;
- деятельность иностранных государственных и частных коммерческих структур, стремящихся получить несанкционированный доступ к информационным ресурсам правоохранительных и судебных органов.

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

- нарушение установленного регламента сбора, обработки, хранения и передачи информации, содержащейся в картотеках и автоматизированных банках данных и использующейся для расследования преступлений;
- недостаточность законодательного и нормативного регулирования информационного обмена в правоохранительной и судебной сферах;
- отсутствие единой методологии сбора, обработки и хранения информации оперативно-разыскного, справочного, криминалистического и статистического характера;
- отказ технических средств и сбои программного обеспечения в информационных и телекоммуникационных системах;
- преднамеренные действия, а также ошибки персонала, непосредственно занятого формированием и ведением картотек и автоматизированных банков данных.

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

Главными из них являются:

- создание защищенной многоуровневой системы интегрированных банков данных оперативно-разыскного, справочного, криминалистического и статистического характера на базе специализированных информационно-телекоммуникационных систем;
- повышение уровня профессиональной и специальной подготовки пользователей информационных систем.

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

Особое значение для нормального функционирования указанных объектов имеет обеспечение безопасности информационной инфраструктуры страны при авариях, катастрофах и стихийных бедствиях. Сокрытие, задержка поступления, искажение и разрушение оперативной информации, несанкционированный доступ к ней отдельных лиц или групп лиц могут привести как к человеческим жертвам, так и к возникновению разного рода сложностей при ликвидации последствий чрезвычайной ситуации, связанных с особенностями информационного воздействия в экстремальных условиях: к приведению в движение больших масс людей, испытывающих психический стресс; к быстрому возникновению и распространению среди них паники и беспорядков на основе слухов, ложной или недостоверной информации.

К специфическим для данных условий направлениям обеспечения информационной безопасности относятся:

- разработка эффективной системы мониторинга объектов повышенной опасности, нарушение функционирования которых может привести к возникновению чрезвычайных ситуаций, и прогнозирования чрезвычайных ситуаций;
- совершенствование системы информирования населения об угрозах возникновения чрезвычайных ситуаций, об условиях их возникновения и развития;
- повышение надежности систем обработки и передачи информации, обеспечивающих деятельность федеральных органов исполнительной власти;
- прогнозирование поведения населения под воздействием ложной или недостоверной информации о возможных чрезвычайных ситуациях и выработка мер по оказанию помощи большим массам людей в условиях этих ситуаций;
- разработка специальных мер по защите информационных систем, обеспечивающих управление экологически опасными и экономически важными производствами.

## 7. Международное сотрудничество Российской Федерации в области обеспечения информационной безопасности

Международное сотрудничество РФ в области обеспечения информационной безопасности - неотъемлемая составляющая политического, военного, экономического, культурного и других видов взаимодействия стран, входящих в мировое сообщество. Такое сотрудничество должно способствовать повышению информационной безопасности всех членов мирового сообщества, включая РФ.

Особенность международного сотрудничества РФ в области обеспечения информационной безопасности состоит в том, что оно осуществляется в условиях обострения международной конкуренции за обладание технологическими и информационными ресурсами, за доминирование на рынках сбыта, в условиях продолжения попыток создания структуры международных отношений, основанной на односторонних решениях ключевых проблем мировой политики, противодействия укреплению роли России как одного из влиятельных центров формирующегося многополярного мира, усиления технологического отрыва ведущих держав мира и наращивания их возможностей для создания «информационного оружия». Все это может привести к новому этапу развертывания гонки вооружений в информационной сфере, нарастанию угрозы агентурного и оперативно-технического проникновения в Россию иностранных разведок, в том числе с использованием глобальной информационной инфраструктуры.

Основными направлениями международного сотрудничества РФ в области обеспечения информационной безопасности являются:

- запрещение разработки, распространения и применения «информационного оружия»;
- обеспечение безопасности международного информационного обмена, в том числе сохранности информации при ее передаче по национальным телекоммуникационным каналам и каналам связи;
- координация деятельности правоохранительных органов стран, входящих в мировое сообщество, по предотвращению компьютерных преступлений;
- предотвращение несанкционированного доступа к конфиденциальной информации в международных банковских телекоммуникационных сетях и системах информационного обеспечения мировой торговли, к информации международных правоохранительных организаций, ведущих борьбу с транснациональной организованной преступностью, международным терроризмом, распространением нар-

котиков и психотропных веществ, незаконной торговлей оружием и расщепляющимися материалами, а также торговлей людьми.

При осуществлении международного сотрудничества РФ в области обеспечения информационной безопасности особое внимание должно уделяться проблемам взаимодействия с государствами - участниками Содружества Независимых Государств.

Для осуществления этого сотрудничества по указанным основным направлениям необходимо обеспечить активное участие России во всех международных организациях, осуществляющих деятельность в области информационной безопасности, в том числе в сфере стандартизации и сертификации средств информатизации и защиты информации.

# III. Основные положения государственной политики обеспечения информационной безопасности Российской Федерации и первоочередные мероприятия по ее реализации

## 8. Основные положения государственной политики обеспечения информационной безопасности Российской Федерации

Государственная политика обеспечения информационной безопасности РФ определяет основные направления деятельности федеральных органов государственной власти и органов государственной власти субъектов РФ в этой области, порядок закрепления их обязанностей по защите интересов РФ в информационной сфере в рамках направлений их деятельности и базируется на соблюдении баланса интересов личности, общества и государства в информационной сфере.

Государственная политика обеспечения информационной безопасности РФ основывается на следующих основных принципах:

- соблюдение Конституции РФ, законодательства РФ, общепризнанных принципов и норм международного права при осуществлении деятельности по обеспечению информационной безопасности РФ;
- открытость в реализации функций федеральных органов государственной власти, органов государственной власти субъектов РФ и общественных объединений, предусматривающая информирование общества об их деятельности с учетом ограничений, установленных законодательством РФ;

- правовое равенство всех участников процесса информационного взаимодействия вне зависимости от их политического, социального и экономического статуса, основывающееся на конституционном праве граждан на свободный поиск, получение, передачу, производство и распространение информации любым законным способом;
- приоритетное развитие отечественных современных информационных и телекоммуникационных технологий, производство технических и программных средств, способных обеспечить совершенствование национальных телекоммуникационных сетей, их подключение к глобальным информационным сетям в целях соблюдения жизненно важных интересов РФ.

Государство в процессе реализации своих функций по обеспечению информационной безопасности РФ:

- проводит объективный и всесторонний анализ и прогнозирование угроз информационной безопасности РФ, разрабатывает меры по ее обеспечению;
- организует работу законодательных (представительных) и исполнительных органов государственной власти РФ по реализации комплекса мер, направленных на предотвращение, отражение и нейтрализацию угроз информационной безопасности РФ;
- поддерживает деятельность общественных объединений, направленную на объективное информирование населения о социально значимых явлениях общественной жизни, защиту общества от искаженной и недостоверной информации;
- осуществляет контроль за разработкой, созданием, развитием, использованием, экспортом и импортом средств защиты информации посредством их сертификации и лицензирования деятельности в области защиты информации;
- проводит необходимую протекционистскую политику в отношении производителей средств информатизации и защиты информации на территории РФ и принимает меры по защите внутреннего рынка от проникновения на него некачественных средств информатизации и информационных продуктов;
- способствует предоставлению физическим и юридическим лицам доступа к мировым информационным ресурсам, глобальным информационным сетям;
- формулирует и реализует государственную информационную политику России;

- организует разработку федеральной программы обеспечения информационной безопасности РФ, объединяющей усилия государственных и негосударственных организаций в данной области;
- способствует интернационализации глобальных информационных сетей и систем, а также вхождению России в мировое информационное сообщество на условиях равноправного партнерства.

Совершенствование правовых механизмов регулирования общественных отношений, возникающих в информационной сфере, является приоритетным направлением государственной политики в области обеспечения информационной безопасности РФ.

Это предполагает:

- оценку эффективности применения действующих законодательных и иных нормативных правовых актов в информационной сфере и выработку программы их совершенствования;
- создание организационно-правовых механизмов обеспечения информационной безопасности;
- определение правового статуса всех субъектов отношений в информационной сфере, включая пользователей информационных и телекоммуникационных систем, и установление их ответственности за соблюдение законодательства РФ в данной сфере;
- создание системы сбора и анализа данных об источниках угроз информационной безопасности РФ, а также о последствиях их осуществления;
- разработку нормативных правовых актов, определяющих организацию следствия и процедуру судебного разбирательства по фактам противоправных действий в информационной сфере, а также порядок ликвидации последствий этих противоправных действий;
- разработку составов правонарушений с учетом специфики уголовной, гражданской, административной, дисциплинарной ответственности и включение соответствующих правовых норм в уголовный, гражданский, административный и трудовой кодексы, в законодательство РФ о государственной службе;
- совершенствование системы подготовки кадров, используемых в области обеспечения информационной безопасности РФ.

Правовое обеспечение информационной безопасности РФ должно базироваться, прежде всего, на соблюдении принципов законности, баланса интересов граждан, общества и государства в информационной сфере.

Соблюдение принципа законности требует от федеральных органов государственной власти и органов государственной власти субъектов РФ при решении возникающих в информационной сфере конфликтов неукоснительно руководствоваться законодательными и иными нормативными правовыми актами, регулирующими отношения в этой сфере.

Соблюдение принципа баланса интересов граждан, общества и государства в информационной сфере предполагает законодательное закрепление приоритета этих интересов в различных областях жизнедеятельности общества, а также использование форм общественного контроля деятельности федеральных органов государственной власти и органов государственной власти субъектов РФ. Реализация гарантий конституционных прав и свобод человека и гражданина, касающихся деятельности в информационной сфере, является важнейшей задачей государства в области информационной безопасности.

Разработка механизмов правового обеспечения информационной безопасности РФ включает в себя мероприятия по информатизации правовой сферы в целом.

В целях выявления и согласования интересов федеральных органов государственной власти, органов государственной власти субъектов РФ и других субъектов отношений в информационной сфере, выработки необходимых решений государство поддерживает формирование общественных советов, комитетов и комиссий с широким представительством общественных объединений и содействует организации их эффективной работы.

## 9. Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности Российской Федерации

Первоочередными мероприятиями по реализации государственной политики обеспечения информационной безопасности РФ являются:

- разработка и внедрение механизмов реализации правовых норм, регулирующих отношения в информационной сфере, а также подготовка концепции правового обеспечения информационной безопасности РФ;
- разработка и реализация механизмов повышения эффективности государственного руководства деятельностью государственных средств массовой информации, осуществления государственной информационной политики;

- принятие и реализация федеральных программ, предусматривающих формирование общедоступных архивов информационных ресурсов федеральных органов государственной власти и органов государственной власти субъектов РФ, повышение правовой культуры и компьютерной грамотности граждан, развитие инфраструктуры единого информационного пространства России, комплексное противодействие угрозам информационной войны, создание безопасных информационных технологий для систем, используемых в процессе реализации жизненно важных функций общества и государства, пресечение компьютерной преступности, создание информационно-телекоммуникационной системы специального назначения в интересах федеральных органов государственной власти и органов государственной власти субъектов РФ, обеспечение технологической независимости страны в области создания и эксплуатации информационно-телекоммуникационных систем оборонного назначения;
- развитие системы подготовки кадров, используемых в области обеспечения информационной безопасности РФ;
- гармонизация отечественных стандартов в области информатизации и обеспечения информационной безопасности автоматизированных систем управления, информационных и телекоммуникационных систем общего и специального назначения.

# IV. Организационная основа системы обеспечения информационной безопасности Российской Федерации

## 10. Основные функции системы обеспечения информационной безопасности Российской Федерации

Система обеспечения информационной безопасности РФ предназначена для реализации государственной политики в данной сфере.

Основными функциями системы обеспечения информационной безопасности РФ являются:

- разработка нормативной правовой базы в области обеспечения информационной безопасности РФ;
- создание условий для реализации прав граждан и общественных объединений на разрешенную законом деятельность в информационной сфере;

- определение и поддержание баланса между потребностью граждан, общества и государства в свободном обмене информацией и необходимыми ограничениями на распространение информации;
- оценка состояния информационной безопасности РФ, выявление источников внутренних и внешних угроз информационной безопасности, определение приоритетных направлений предотвращения, отражения и нейтрализации этих угроз;
- координация деятельности федеральных органов государственной власти и других государственных органов, решающих задачи обеспечения информационной безопасности РФ;
- контроль деятельности федеральных органов государственной власти и органов государственной власти субъектов РФ, государственных и межведомственных комиссий, участвующих в решении задач обеспечения информационной безопасности РФ;
- предупреждение, выявление и пресечение правонарушений, связанных с посягательствами на законные интересы граждан, общества и государства в информационной сфере, на осуществление судопроизводства по делам о преступлениях в этой области;
- развитие отечественной информационной инфраструктуры, а также индустрии телекоммуникационных и информационных средств, повышение их конкурентоспособности на внутреннем и внешнем рынке;
- организация разработки федеральной и региональных программ обеспечения информационной безопасности и координация деятельности по их реализации;
- проведение единой технической политики в области обеспечения информационной безопасности РФ;
- организация фундаментальных и прикладных научных исследований в области обеспечения информационной безопасности РФ;
- защита государственных информационных ресурсов, прежде всего в федеральных органах государственной власти и органах государственной власти субъектов РФ, на предприятиях оборонного комплекса;
- обеспечение контроля за созданием и использованием средств защиты информации посредством обязательного лицензирования деятельности в данной сфере и сертификации средств защиты информации;
- совершенствование и развитие единой системы подготовки кадров, используемых в области информационной безопасности РФ;

- осуществление международного сотрудничества в сфере обеспечения информационной безопасности, представление интересов РФ в соответствующих международных организациях.

Компетенция федеральных органов государственной власти, органов государственной власти субъектов РФ, других государственных органов, входящих в состав системы обеспечения информационной безопасности РФ и ее подсистем, определяется федеральными законами, нормативными правовыми актами Президента РФ и Правительства РФ.

Функции органов, координирующих деятельность федеральных органов государственной власти, органов государственной власти субъектов РФ, других государственных органов, входящих в состав системы обеспечения информационной безопасности РФ и ее подсистем, определяются отдельными нормативными правовыми актами РФ.

## 11. Основные элементы организационной основы системы обеспечения информационной безопасности Российской Федерации

Система обеспечения информационной безопасности РФ является частью системы обеспечения национальной безопасности страны.

Система обеспечения информационной безопасности РФ строится на основе разграничения полномочий органов законодательной, исполнительной и судебной власти в данной сфере, а также предметов ведения федеральных органов государственной власти и органов государственной власти субъектов РФ.

Основными элементами организационной основы системы обеспечения информационной безопасности РФ являются: Президент РФ, Совет Федерации Федерального Собрания РФ, Государственная Дума Федерального Собрания РФ, Правительство РФ, Совет Безопасности РФ, федеральные органы исполнительной власти, межведомственные и государственные комиссии, создаваемые Президентом РФ и Правительством РФ, органы исполнительной власти субъектов РФ, органы местного самоуправления, органы судебной власти, общественные объединения, граждане, принимающие в соответствии с законодательством РФ участие в решении задач обеспечения информационной безопасности РФ.

Президент РФ руководит в пределах своих конституционных полномочий органами и силами по обеспечению информационной безопасности РФ; санкционирует действия по обеспечению информационной безопасности РФ; в соответствии с законодательством РФ формирует, реорганизует и упраздняет подчиненные ему органы и силы по обеспечению

информационной безопасности РФ; определяет в своих ежегодных посланиях Федеральному Собранию приоритетные направления государственной политики в области обеспечения информационной безопасности РФ, а также меры по реализации настоящей Доктрины.

Палаты Федерального Собрания РФ на основе Конституции РФ по представлению Президента РФ и Правительства РФ формируют законодательную базу в области обеспечения информационной безопасности РФ.

Правительство РФ в пределах своих полномочий и с учетом сформулированных в ежегодных посланиях Президента РФ Федеральному Собранию приоритетных направлений в области обеспечения информационной безопасности РФ координирует деятельность федеральных органов исполнительной власти и органов исполнительной власти субъектов РФ, а также при формировании в установленном порядке проектов федерального бюджета на соответствующие годы предусматривает выделение средств, необходимых для реализации федеральных программ в этой области.

Совет Безопасности РФ проводит работу по выявлению и оценке угроз информационной безопасности РФ, оперативно подготавливает проекты решений Президента РФ по предотвращению таких угроз, разрабатывает предложения в области обеспечения информационной безопасности РФ, а также предложения по уточнению отдельных положений настоящей Доктрины, координирует деятельность органов и сил по обеспечению информационной безопасности РФ, контролирует реализацию федеральными органами исполнительной власти и органами исполнительной власти субъектов РФ решений Президента РФ в этой области.

Федеральные органы исполнительной власти обеспечивают исполнение законодательства РФ, решений Президента РФ и Правительства РФ в области обеспечения информационной безопасности РФ; в пределах своей компетенции разрабатывают нормативные правовые акты в этой области и представляют их в установленном порядке Президенту РФ и в Правительство РФ.

Межведомственные и государственные комиссии, создаваемые Президентом РФ и Правительством РФ, решают в соответствии с предоставленными им полномочиями задачи обеспечения информационной безопасности РФ.

Органы исполнительной власти субъектов РФ взаимодействуют с федеральными органами исполнительной власти по вопросам исполнения законодательства РФ, решений Президента РФ и Правительства РФ в области обеспечения информационной безопасности РФ, а также по вопросам реализации федеральных программ в этой области; совместно с органами местного самоуправления осуществляют мероприятия

по привлечению граждан, организаций и общественных объединений к оказанию содействия в решении проблем обеспечения информационной безопасности РФ; вносят в федеральные органы исполнительной власти предложения по совершенствованию системы обеспечения информационной безопасности РФ.

Органы местного самоуправления обеспечивают соблюдение законодательства РФ в области обеспечения информационной безопасности РФ.

Органы судебной власти осуществляют правосудие по делам о преступлениях, связанных с посягательствами на законные интересы личности, общества и государства в информационной сфере, и обеспечивают судебную защиту граждан и общественных объединений, чьи права были нарушены в связи с деятельностью по обеспечению информационной безопасности РФ.

В состав системы обеспечения информационной безопасности РФ могут входить подсистемы (системы), ориентированные на решение локальных задач в данной сфере.

Реализация первоочередных мероприятий по обеспечению информационной безопасности РФ, перечисленных в настоящей Доктрине, предполагает разработку соответствующей федеральной программы. Конкретизация некоторых положений настоящей Доктрины применительно к отдельным сферам деятельности общества и государства может быть осуществлена в соответствующих документах, утверждаемых Президентом РФ.

# Приложение 5

# ФЕДЕРАЛЬНЫЙ ЗАКОН РОССИЙСКОЙ ФЕДЕРАЦИИ «ОБ ИНФОРМАЦИИ, ИНФОРМАТИЗАЦИИ И ЗАЩИТЕ ИНФОРМАЦИИ»

от 20 февраля 1995 г. № 24-ФЗ
Принят Государственной Думой 25 января 1995 г.

## Глава 1. Общие положения

### 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 РФ «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 РФ;
- **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, осуществляющий 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 РФ.

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 РФ;
- 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 реализация 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 РФ.

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

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. Право удостоверять идентичность электронной цифровой подписи осуществляется на основании лицензии. Порядок выдачи лицензий определяется законодательством РФ.

## 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 РФ.

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. РФ и субъекты РФ являются собственниками информационных ресурсов, создаваемых, приобретаемых, накапливаемых за счет средств федерального бюджета, бюджетов субъектов РФ, 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 разрешением 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 информаци-

онные 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 РФ.

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 РФ.

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

- назначать 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 РФ формируются в соответствии со сферами ведения как:

- федеральные информационные ресурсы;
- информационные ресурсы, находящиеся в совместном ведении РФ и субъектов РФ (далее - информационные ресурсы совместного ведения);
- информационные ресурсы субъектов РФ.

2. Формирование государственных информационных ресурсов в соответствии с пунктом 1 статьи 8 настоящего Федерального закона осуще-

ствляется гражданами, органами государственной власти, органами местного самоуправления, организациями и общественными объединениями.

Федеральные органы государственной власти, органы государственной власти субъектов РФ 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 РФ финансируется из федерального бюджета и бюджетов субъектов РФ по статье расходов «Информатика» («Информационное обеспечение»).

4. Организации, которые специализируются на формировании федеральных информационных ресурсов и (или) информационных ресурсов совместного ведения на основе договора, обязаны получить лицензию на этот вид деятельности в органах государственной власти. Порядок лицензирования определяется законодательством РФ.

## 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 РФ.

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 обяза-

тельном 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 РФ 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 потребностях 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 РФ «О государственной тайне».

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

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

1. Перечни персональных данных, включаемых в состав федеральных информационных ресурсов, информационных ресурсов совместного ведения, информационных ресурсов субъектов РФ, 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.

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 РФ. Ограничение прав граждан РФ 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 РФ за нарушение режима защиты, обработки и порядка использования этой информации.

4. Подлежит обязательному лицензированию деятельность негосударственных организаций и частных лиц, связанная с обработкой и предоставлением пользователям персональных данных. Порядок лицензирования определяется законодательством РФ.

5. 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 владельцем этих ресурсов необходимость получения запрашиваемой ими информации. Исключение составляет информация с ограниченным доступом.

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

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

Информация, полученная на законных основаниях из государственных информационных ресурсов гражданами и организациями, может быть использована ими для создания производной 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 п. 1 настоящей статьи, может быть обжалован в суд.

3. Комитет при Президенте РФ 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 РФ.

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

## 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 РФ.

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 РФ 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 РФ.

# 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 РФ 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 РФ 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, приобретены 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 РФ.

## Статья 19. Сертификация информационных систем, технологий, средств их обеспечения и лицензирование деятельности по формированию и использованию информационных ресурсов

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

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

3. Организации, выполняющие работы в области проектирования, производства средств защиты информации и обработки персональных данных, получают лицензии на этот вид деятельности. Порядок лицензирования определяется законодательством РФ.

4. Интересы потребителя информации при использовании импортной продукции в информационных системах защищаются таможенными органами РФ 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 РФ «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 использовани информационных ресурсов с ограниченным доступом, руководствуются в своей деятельности законодательством РФ.

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 РФ.

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 РФ. 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 РФ.

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 РФ и субъектов РФ.

Для рассмотрения конфликтных ситуаций и зашиты 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 дн его официального опубликования.

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

3. Поручить Правительству РФ:

- 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 РФ в связи с принятием настоящего Федерального закона;
- принять нормативные правовые акты, обеспечивающие реализацию настоящего Федерального закона.

*Президент РФ*
*Б.ЕЛЬЦИН*
*Москва, Дом Советов России*
*20 февраля 1995 г. № 24-ФЗ*

## Приложение 6

# ФЕДЕРАЛЬНЫЙ ЗАКОН РОССИЙСКОЙ ФЕДЕРАЦИИ «ОБ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ»

от 10 января 2002 г. № 1-ФЗ
Принят Государственной Думой 13 декабря 2001 г.
Одобрен Советом Федераций 26 декабря 2001 г.

## Глава 1. Общие положения

### Статья 1. Цель и сфера применения настоящего Федерального закона

1. Целью настоящего Федерального закона является обеспечение правовых условий использования электронной цифровой подписи в электронных документах, при соблюдении которых электронная цифровая подпись в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе.

2. Действие настоящего Федерального закона распространяется на отношения, возникающие при совершении гражданско-правовых сделок и в других предусмотренных законодательством РФ случаях. Действие настоящего Федерального закона не распространяется на отношения, возникающие при использовании иных аналогов собственноручной подписи.

### Статья 2. Правовое регулирование отношений в области использования электронной цифровой подписи

Правовое регулирование отношений в области использования электронной цифровой подписи осуществляется в соответствии с настоящим Федеральным законом, Гражданским кодексом РФ, Федеральным законом «Об информации, информатизации и защите информации», Федеральным законом «О связи», другими федеральными законами и принимаемыми в соответствии с ними иными нормативными правовыми актами РФ, а также осуществляется соглашением сторон.

## Статья 3. Основные понятия, используемые в настоящем Федеральном законе

Для целей настоящего Федерального закона используются следующие основные понятия:

- **электронный документ** - документ, в котором информация представлена в электронно-цифровой форме;
- **электронная цифровая подпись** - реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе;
- **владелец сертификата ключа подписи** - физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы);
- **средства электронной цифровой подписи** - аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций - создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей;
- **сертификат средств электронной цифровой подписи** - документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной цифровой подписи установленным требованиям;
- **закрытый ключ электронной цифровой подписи** - уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи;
- **открытый ключ электронной цифровой подписи** - уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю

информационной системы и предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе;

- **сертификат ключа подписи** - документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и которые выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи;
- **подтверждение подлинности электронной цифровой подписи в электронном документе** - положительный результат проверки соответствующим сертифицированным средством электронной цифровой подписи с использованием сертификата ключа подписи принадлежности электронной цифровой подписи в электронном документе владельцу сертификата ключа подписи и отсутствия искажений в подписанном данной электронной цифровой подписью электронном документе;
- **пользователь сертификата ключа подписи** - физическое лицо, использующее полученные в удостоверяющем центре сведения о сертификате ключа подписи для проверки принадлежности электронной цифровой подписи владельцу сертификата ключа подписи;
- **информационная система общего пользования** - информационная система, которая открыта для использования всеми физическими и юридическими лицами и в услугах которой этим лицам не может быть отказано;
- **корпоративная информационная система** - информационная система, участниками которой может быть ограниченный круг лиц, определенный ее владельцем или соглашением участников этой информационной системы.

# Глава 2. Условия использования электронной цифровой подписи

## Статья 4. Условия признания равнозначности электронной цифровой подписи и собственноручной подписи

1. Электронная цифровая подпись в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе при одновременном соблюдении следующих условий:

- сертификат ключа подписи, относящийся к этой электронной цифровой подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;
- подтверждена подлинность электронной цифровой подписи в электронном документе;
- электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи.

2. Участник информационной системы может быть одновременно владельцем любого количества сертификатов ключей подписей. При этом электронный документ с электронной цифровой подписью имеет юридическое значение при осуществлении отношений, указанных в сертификате ключа подписи.

### Статья 5. Использование средств электронной цифровой подписи

1. Создание ключей электронных цифровых подписей осуществляется для использования в:

- информационной системе общего пользования ее участником или по его обращению удостоверяющим центром;
- корпоративной информационной системе в порядке, установленном в этой системе.

2. При создании ключей электронных цифровых подписей для использования в информационной системе общего пользования должны применяться только сертифицированные средства электронной цифровой подписи. Возмещение убытков, причиненных в связи с созданием ключей электронных цифровых подписей несертифицированными средствами электронной цифровой подписи, может быть возложено на создателей и распространителей этих средств в соответствии с законодательством РФ.

3. Использование несертифицированных средств электронной цифровой подписи и созданных ими ключей электронных цифровых подписей в корпоративных информационных системах федеральных органов государственной власти, органов государственной власти субъектов РФ и органов местного самоуправления не допускается.

4. Сертификация средств электронной цифровой подписи осуществляется в соответствии с законодательством РФ о сертификации продукции и услуг.

## Статья 6. Сертификат ключа подписи

1. Сертификат ключа подписи должен содержать следующие сведения:

- уникальный регистрационный номер сертификата ключа подписи, даты начала и окончания срока действия сертификата ключа подписи, находящегося в реестре удостоверяющего центра;
- фамилия, имя и отчество владельца сертификата ключа подписи или псевдоним владельца. В случае использования псевдонима удостоверяющим центром вносится запись об этом в сертификат ключа подписи;
- открытый ключ электронной цифровой подписи;
- наименование средств электронной цифровой подписи, с которыми используется данный открытый ключ электронной цифровой подписи;
- наименование и место нахождения удостоверяющего центра, выдавшего сертификат ключа подписи;
- сведения об отношениях, при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение.

2. В случае необходимости в сертификате ключа подписи на основании подтверждающих документов указываются должность (с указанием наименования и места нахождения организации, в которой установлена эта должность) и квалификация владельца сертификата ключа подписи, а по его заявлению в письменной форме - иные сведения, подтверждаемые соответствующими документами.

3. Сертификат ключа подписи должен быть внесен удостоверяющим центром в реестр сертификатов ключей подписей не позднее даты начала действия сертификата ключа подписи.

4. Для проверки принадлежности электронной цифровой подписи соответствующему владельцу сертификат ключа подписи выдается пользователям с указанием даты и времени его выдачи, сведений о действии сертификата ключа подписи (действует, действие приостановлено, сроки приостановления его действия, аннулирован, дата и время аннулирования сертификата ключа подписи) и сведений о реестре сертификатов ключей подписей. В случае выдачи сертификата ключа подписи в форме документа на бумажном носителе этот сертификат оформляется на бланке удостоверяющего центра и заверяется собственноручной подписью уполномоченного лица и печатью удостоверяющего центра. В случае выдачи сертификата ключа подписи и указанных дополнительных данных в форме электронного документа этот сертификат должен быть подписан электронной цифровой подписью уполномоченного лица удостоверяющего центра.

### Статья 7. Срок и порядок хранения сертификата ключа подписи в удостоверяющем центре

1. Срок хранения сертификата ключа подписи в форме электронного документа в удостоверяющем центре определяется договором между удостоверяющим центром и владельцем сертификата ключа подписи. При этом обеспечивается доступ участников информационной системы в удостоверяющий центр для получения сертификата ключа подписи.

2. Срок хранения сертификата ключа подписи в форме электронного документа в удостоверяющем центре после аннулирования сертификата ключа подписи должен быть не менее установленного федеральным законом срока исковой давности для отношений, указанных в сертификате ключа подписи.

По истечении указанного срока хранения сертификат ключа подписи исключается из реестра сертификатов ключей подписей и переводится в режим архивного хранения. Срок архивного хранения составляет не менее чем пять лет. Порядок выдачи копий сертификатов ключей подписей в этот период устанавливается в соответствии с законодательством РФ.

3. Сертификат ключа подписи в форме документа на бумажном носителе хранится в порядке, установленном законодательством РФ об архивах и архивном деле.

## Глава 3. Удостоверяющие центры

### Статья 8. Статус удостоверяющего центра

1. Удостоверяющим центром, выдающим сертификаты ключей подписей для использования в информационных системах общего пользования, должно быть юридическое лицо, выполняющее функции, предусмотренные настоящим Федеральным законом. При этом удостоверяющий центр должен обладать необходимыми материальными и финансовыми возможностями, позволяющими ему нести гражданскую ответственность перед пользователями сертификатов ключей подписей за убытки, которые могут быть понесены ими вследствие недостоверности сведений, содержащихся в сертификатах ключей подписей.

Требования, предъявляемые к материальным и финансовым возможностям удостоверяющих центров, определяются Правительством РФ по представлению уполномоченного федерального органа исполнительной власти.

Статус удостоверяющего центра, обеспечивающего функционирование корпоративной информационной системы, определяется ее владельцем или соглашением участников этой системы.

2. Деятельность удостоверяющего центра подлежит лицензированию в соответствии с законодательством РФ о лицензировании отдельных видов деятельности.

### Статья 9. Деятельность удостоверяющего центра

1. Удостоверяющий центр:

- изготавливает сертификаты ключей подписей;
- создает ключи электронных цифровых подписей по обращению участников информационной системы с гарантией сохранения в тайне закрытого ключа электронной цифровой подписи;
- приостанавливает и возобновляет действие сертификатов ключей подписей, а также аннулирует их;
- ведет реестр сертификатов ключей подписей, обеспечивает его актуальность и возможность свободного доступа к нему участников информационных систем;
- проверяет уникальность открытых ключей электронных цифровых подписей в реестре сертификатов ключей подписей и архиве удостоверяющего центра;
- выдает сертификаты ключей подписей в форме документов на бумажных носителях и (или) в форме электронных документов с информацией об их действии;
- осуществляет по обращениям пользователей сертификатов ключей подписей подтверждение подлинности электронной цифровой подписи в электронном документе в отношении выданных им сертификатов ключей подписей;
- может предоставлять участникам информационных систем иные связанные с использованием электронных цифровых подписей услуги.

2. Изготовление сертификатов ключей подписей осуществляется на основании заявления участника информационной системы, которое содержит сведения, указанные в статье 6 настоящего Федерального закона и необходимые для идентификации владельца сертификата ключа подписи и передачи ему сообщений. Заявление подписывается собственноручно владельцем сертификата ключа подписи. Содержащиеся в заявлении сведения подтверждаются предъявлением соответствующих документов.

3. При изготовлении сертификатов ключей подписей удостоверяющим центром оформляются в форме документов на бумажных носителях два экземпляра сертификата ключа подписи, которые заверяются собственноручными подписями владельца сертификата ключа подписи и уполномоченного лица удостоверяющего центра, а также печатью удостоверяющего центра. Один экземпляр сертификата ключа подписи выдается владельцу сертификата ключа подписи, второй - остается в удостоверяющем центре.

4. Услуги по выдаче участникам информационных систем сертификатов ключей подписей, зарегистрированных удостоверяющим центром, одновременно с информацией об их действии в форме электронных документов оказываются безвозмездно.

## Статья 10. Отношения между удостоверяющим центром и уполномоченным федеральным органом исполнительной власти

1. Удостоверяющий центр до начала использования электронной цифровой подписи уполномоченного лица удостоверяющего центра для заверения от имени удостоверяющего центра сертификатов ключей подписей обязан представить в уполномоченный федеральный орган исполнительной власти сертификат ключа подписи уполномоченного лица удостоверяющего центра в форме электронного документа, а также этот сертификат в форме документа на бумажном носителе с собственноручной подписью указанного уполномоченного лица, заверенный подписью руководителя и печатью удостоверяющего центра.

2. Уполномоченный федеральный орган исполнительной власти ведет единый государственный реестр сертификатов ключей подписей, которыми удостоверяющие центры, работающие с участниками информационных систем общего пользования, заверяют выдаваемые ими сертификаты ключей подписей, обеспечивает возможность свободного доступа к этому реестру и выдает сертификаты ключей подписей соответствующих уполномоченных лиц удостоверяющих центров.

3. Электронные цифровые подписи уполномоченных лиц удостоверяющих центров могут использоваться только после включения их в единый государственный реестр сертификатов ключей подписей. Использование этих электронных цифровых подписей для целей, не связанных с заверением сертификатов ключей подписей и сведений об их действии, не допускается.

4. Уполномоченный федеральный орган исполнительной власти:

- осуществляет по обращениям физических лиц, организаций, федеральных органов государственной власти, органов государственной власти субъектов РФ и органов местного самоуправления подтверждение подлинности электронных цифровых подписей уполномоченных лиц удостоверяющих центров в выданных ими сертификатах ключей подписей;
- осуществляет в соответствии с положением об уполномоченном федеральном органе исполнительной власти иные полномочия по обеспечению действия настоящего Федерального закона.

### Статья 11. Обязательства удостоверяющего центра по отношению к владельцу сертификата ключа подписи

Удостоверяющий центр при изготовлении сертификата ключа подписи принимает на себя следующие обязательства по отношению к владельцу сертификата ключа подписи:

- вносить сертификат ключа подписи в реестр сертификатов ключей подписей;
- обеспечивать выдачу сертификата ключа подписи обратившимся к нему участникам информационных систем;
- приостанавливать действие сертификата ключа подписи по обращению его владельца;
- уведомлять владельца сертификата ключа подписи о фактах, которые стали известны удостоверяющему центру и которые существенным образом могут сказаться на возможности дальнейшего использования сертификата ключа подписи;
- иные установленные нормативными правовыми актами или соглашением сторон обязательства.

### Статья 12. Обязательства владельца сертификата ключа подписи

1. Владелец сертификата ключа подписи обязан:

- не использовать для электронной цифровой подписи открытые и закрытые ключи электронной цифровой подписи, если ему известно, что эти ключи используются или использовались ранее;
- хранить в тайне закрытый ключ электронной цифровой подписи;

- немедленно требовать приостановления действия сертификата ключа подписи при наличии оснований полагать, что тайна закрытого ключа электронной цифровой подписи нарушена.

2. При несоблюдении требований, изложенных в настоящей статье, возмещение причиненных вследствие этого убытков возлагается на владельца сертификата ключа подписи.

### Статья 13. Приостановление действия сертификата ключа подписи

1. Действие сертификата ключа подписи может быть приостановлено удостоверяющим центром на основании указания лиц или органов, имеющих такое право в силу закона или договора, а в корпоративной информационной системе также в силу установленных для нее правил пользования.

2. Период от поступления в удостоверяющий центр указания о приостановлении действия сертификата ключа подписи до внесения соответствующей информации в реестр сертификатов ключей подписей должен устанавливаться в соответствии с общим для всех владельцев сертификатов ключей подписей правилом. По договоренности между удостоверяющим центром и владельцем сертификата ключа подписи этот период может быть сокращен.

3. Действие сертификата ключа подписи по указанию полномочного лица (органа) приостанавливается на исчисляемый в днях срок, если иное не установлено нормативными правовыми актами или договором. Удостоверяющий центр возобновляет действие сертификата ключа подписи по указанию полномочного лица (органа). В случае, если по истечении указанного срока не поступает указание о возобновлении действия сертификата ключа подписи, он подлежит аннулированию.

4. В соответствии с указанием полномочного лица (органа) о приостановлении действия сертификата ключа подписи удостоверяющий центр оповещает об этом пользователей сертификатов ключей подписей путем внесения в реестр сертификатов ключей подписей соответствующей информации с указанием даты, времени и срока приостановления действия сертификата ключа подписи, а также извещает об этом владельца сертификата ключа подписи и полномочное лицо (орган), от которого получено указание о приостановлении действия сертификата ключа подписи.

## Статья 14. Аннулирование сертификата ключа подписи

1. Удостоверяющий центр, выдавший сертификат ключа подписи, обязан аннулировать его:

- по истечении срока его действия;
- при утрате юридической силы сертификата соответствующих средств электронной цифровой подписи, используемых в информационных системах общего пользования;
- в случае, если удостоверяющему центру стало достоверно известно о прекращении действия документа, на основании которого оформлен сертификат ключа подписи;
- по заявлению в письменной форме владельца сертификата ключа подписи;
- в иных установленных нормативными правовыми актами или соглашением сторон случаях.

2. В случае аннулирования сертификата ключа подписи удостоверяющий центр оповещает об этом пользователей сертификатов ключей подписей путем внесения в реестр сертификатов ключей подписей соответствующей информации с указанием даты и времени аннулирования сертификата ключа подписи, за исключением случаев аннулирования сертификата ключа подписи по истечении срока его действия, а также извещает об этом владельца сертификата ключа подписи и полномочное лицо (орган), от которого получено указание об аннулировании сертификата ключа подписи.

## Статья 15. Прекращение деятельности удостоверяющего центра

1. Деятельность удостоверяющего центра, выдающего сертификаты ключей подписей для использования в информационных системах общего пользования, может быть прекращена в порядке, установленном гражданским законодательством.

2. В случае прекращения деятельности удостоверяющего центра, указанного в п. 1 настоящей статьи, сертификаты ключей подписей, выданные этим удостоверяющим центром, могут быть переданы другому удостоверяющему центру по согласованию с владельцами сертификатов ключей подписей.

Сертификаты ключей подписей, не переданные в другой удостоверяющий центр, аннулируются и передаются на хранение в соответствии со ст. 7 настоящего Федерального закона уполномоченному федеральному органу исполнительной власти.

3. Деятельность удостоверяющего центра, обеспечивающего функционирование корпоративной информационной системы, прекращается по решению владельца этой системы, а также по договоренности участников этой системы в связи с передачей обязательств данного удостоверяющего центра другому удостоверяющему центру или в связи с ликвидацией корпоративной информационной системы.

## Глава 4. Особенности использования электронной цифровой подписи

### Статья 16. Использование электронной цифровой подписи в сфере государственного управления

1. Федеральные органы государственной власти, органы государственной власти субъектов РФ, органы местного самоуправления, а также организации, участвующие в документообороте с указанными органами, используют для подписания своих электронных документов электронные цифровые подписи уполномоченных лиц указанных органов, организаций.

2. Сертификаты ключей подписей уполномоченных лиц федеральных органов государственной власти включаются в реестр сертификатов ключей подписей, который ведется уполномоченным федеральным органом исполнительной власти, и выдаются пользователям сертификатов ключей подписей из этого реестра в порядке, установленном настоящим Федеральным законом для удостоверяющих центров.

3. Порядок организации выдачи сертификатов ключей подписей уполномоченных лиц органов государственной власти субъектов РФ и уполномоченных лиц органов местного самоуправления устанавливается нормативными правовыми актами соответствующих органов.

### Статья 17. Использование электронной цифровой подписи в корпоративной информационной системе

1. Корпоративная информационная система, предоставляющая участникам информационной системы общего пользования услуги удостоверяющего центра корпоративной информационной системы, должна соответствовать требованиям, установленным настоящим Федеральным законом для информационных систем общего пользования.

2. Порядок использования электронных цифровых подписей в корпоративной информационной системе устанавливается решением владельца корпоративной информационной системы или соглашением участников этой системы.

3. Содержание информации в сертификатах ключей подписей, порядок ведения реестра сертификатов ключей подписей, порядок хранения аннулированных сертификатов ключей подписей, случаи утраты указанными сертификатами юридической силы в корпоративной информационной системе регламентируются решением владельца этой системы или соглашением участников корпоративной информационной системы.

### Статья 18. Признание иностранного сертификата ключа подписи

Иностранный сертификат ключа подписи, удостоверенный в соответствии с законодательством иностранного государства, в котором этот сертификат ключа подписи зарегистрирован, признается на территории РФ в случае выполнения установленных законодательством РФ процедур признания юридического значения иностранных документов.

### Статья 19. Случаи замещения печатей

1. Содержание документа на бумажном носителе, заверенного печатью и преобразованного в электронный документ, в соответствии с нормативными правовыми актами или соглашением сторон может заверяться электронной цифровой подписью уполномоченного лица.

2. В случаях, установленных законами и иными нормативными правовыми актами РФ или соглашением сторон, электронная цифровая подпись в электронном документе, сертификат которой содержит необходимые при осуществлении данных отношений сведения о правомочиях его владельца, признается равнозначной собственноручной подписи лица в документе на бумажном носителе, заверенном печатью.

## Глава 5. Заключительные и переходные положения

### Статья 20. Приведение нормативных правовых актов в соответствие с настоящим Федеральным законом

1. Нормативные правовые акты РФ подлежат приведению в соответствие с настоящим Федеральным законом в течение трех месяцев со дня вступления в силу настоящего Федерального закона.

2. Учредительные документы удостоверяющих центров, выдающих сертификаты ключей подписей для использования в информационных системах общего пользования, подлежат приведению в соответствие с настоящим Федеральным законом в течение шести месяцев со дня вступления в силу настоящего Федерального закона.

## Статья 21. Переходные положения

Удостоверяющие центры, создаваемые после вступления в силу настоящего Федерального закона до начала ведения уполномоченным федеральным органом исполнительной власти реестра сертификатов ключей подписей, должны отвечать требованиям настоящего Федерального закона, за исключением требования предварительно представлять сертификаты ключей подписей своих уполномоченных лиц уполномоченному федеральному органу исполнительной власти. Соответствующие сертификаты должны быть представлены указанному органу не позднее чем через три месяца со дня вступления в силу настоящего Федерального закона.

*Президент РФ*
*В. Путин*

## Приложение 7

# ФЕДЕРАЛЬНЫЙ ЗАКОН «О ТЕХНИЧЕСКОМ РЕГУЛИРОВАНИИ»

от 27 декабря 2002 г. № 184-ФЗ
Принят Государственной Думой 15 декабря 2002 г.
Одобрен Советом Федерации 18 декабря 2002 г.

## Глава 1. Общие положения

### Статья 1. Сфера применения настоящего Федерального закона

1. Настоящий Федеральный закон регулирует отношения, возникающие при:

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

Настоящий Федеральный закон также определяет права и обязанности участников регулируемых настоящим Федеральным законом отношений.

2. Требования к функционированию единой сети связи РФ и к продукции, связанные с обеспечением целостности, устойчивости функционирования указанной сети связи и ее безопасности, отношения, связанные с обеспечением целостности единой сети связи РФ и использованием радиочастотного спектра, соответственно устанавливаются и регулируются законодательством РФ в области связи.

3. Действие настоящего Федерального закона не распространяется на государственные образовательные стандарты, положения (стандарты) о бухгалтерском учете и правила (стандарты) аудиторской деятельности, стандарты эмиссии ценных бумаг и проспектов эмиссии ценных бумаг.

## Статья 2. Основные понятия

Для целей настоящего Федерального закона используются следующие основные понятия:

- **аккредитация** - официальное признание органом по аккредитации компетентности физического или юридического лица выполнять работы в определенной области оценки соответствия;
- **безопасность продукции, процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации (далее - безопасность)** - состояние, при котором отсутствует недопустимый риск, связанный с причинением вреда жизни или здоровью граждан, имуществу физических или юридических лиц, государственному или муниципальному имуществу, окружающей среде, жизни или здоровью животных и растений;
- **ветеринарно-санитарные и фитосанитарные меры** - обязательные для исполнения требования и процедуры, устанавливаемые в целях защиты от рисков, возникающих в связи с проникновением, закреплением или распространением вредных организмов, заболеваний, переносчиков болезней или болезнетворных организмов, в том числе в случае переноса или распространения их животными и (или) растениями, с продукцией, грузами, материалами, транспортными средствами, с наличием добавок, загрязняющих веществ, токсинов, вредителей, сорных растений, болезнетворных организмов, в том числе с пищевыми продуктами или кормами, а также обязательные для исполнения требования и процедуры, устанавливаемые в целях предотвращения иного связанного с распространением вредных организмов ущерба;
- **декларирование соответствия** - форма подтверждения соответствия продукции требованиям технических регламентов;
- **декларация о соответствии** - документ, удостоверяющий соответствие выпускаемой в обращение продукции требованиям технических регламентов;
- **заявитель** - физическое или юридическое лицо, осуществляющее обязательное подтверждение соответствия;
- **знак обращения на рынке** - обозначение, служащее для информирования приобретателей о соответствии выпускаемой в обращение продукции требованиям технических регламентов;

- **знак соответствия** - обозначение, служащее для информирования приобретателей о соответствии объекта сертификации требованиям системы добровольной сертификации или национальному стандарту;
- **идентификация продукции** - установление тождественности характеристик продукции ее существенным признакам;
- **контроль (надзор) за соблюдением требований технических регламентов** - проверка выполнения юридическим лицом или индивидуальным предпринимателем требований технических регламентов к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации и принятие мер по результатам проверки;
- **международный стандарт** - стандарт, принятый международной организацией;
- **национальный стандарт** - стандарт, утвержденный национальным органом РФ по стандартизации;
- **орган по сертификации** - юридическое лицо или индивидуальный предприниматель, аккредитованные в установленном порядке для выполнения работ по сертификации;
- **оценка соответствия** - прямое или косвенное определение соблюдения требований, предъявляемых к объекту;
- **подтверждение соответствия** - документальное удостоверение соответствия продукции или иных объектов, процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг требованиям технических регламентов, положениям стандартов или условиям договоров;
- **продукция** - результат деятельности, представленный в материально-вещественной форме и предназначенный для дальнейшего использования в хозяйственных и иных целях;
- **риск** - вероятность причинения вреда жизни или здоровью граждан, имуществу физических или юридических лиц, государственному или муниципальному имуществу, окружающей среде, жизни или здоровью животных и растений с учетом тяжести этого вреда;
- **сертификация** - форма осуществляемого органом по сертификации подтверждения соответствия объектов требованиям технических регламентов, положениям стандартов или условиям договоров;
- **сертификат соответствия** - документ, удостоверяющий соответствие объекта требованиям технических регламентов, положениям стандартов или условиям договоров;

- **система сертификации** - совокупность правил выполнения работ по сертификации, ее участников и правил функционирования системы сертификации в целом;
- **стандарт** - документ, в котором в целях добровольного многократного использования устанавливаются характеристики продукции, правила осуществления и характеристики процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг. Стандарт также может содержать требования к терминологии, символике, упаковке, маркировке или этикеткам и правилам их нанесения;
- **стандартизация** - деятельность по установлению правил и характеристик в целях их добровольного многократного использования, направленная на достижение упорядоченности в сферах производства и обращения продукции и повышение конкурентоспособности продукции, работ или услуг;
- **техническое регулирование** - правовое регулирование отношений в области установления, применения и исполнения обязательных требований к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, а также в области установления и применения на добровольной основе требований к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнению работ или оказанию услуг и правовое регулирование отношений в области оценки соответствия;
- **технический регламент** - документ, который принят международным договором РФ, ратифицированным в порядке, установленном законодательством РФ, или федеральным законом, или указом Президента РФ, или постановлением Правительства РФ, и устанавливает обязательные для применения и исполнения требования к объектам технического регулирования (продукции, в том числе зданиям, строениям и сооружениям, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации);

*Согласно постановлению Госстандарта РФ от 30 января 2004 г. № 4 со дня вступления в силу Федерального закона «О техническом регулировании» впредь до вступления в силу соответствующих технических регламентов требования, установленные действующими национальными стандартами, подлежат обязательному исполнению только в части, обеспечивающей достижение целей законодательства РФ о техническом регулировании*

- **форма подтверждения соответствия** - определенный порядок документального удостоверения соответствия продукции или иных объектов, процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг требованиям технических регламентов, положениям стандартов или условиям договоров.

### Статья 3. Принципы технического регулирования

Техническое регулирование осуществляется в соответствии с принципами:

- применения единых правил установления требований к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнению работ или оказанию услуг;
- соответствия технического регулирования уровню развития национальной экономики, развития материально-технической базы, а также уровню научно-технического развития;
- независимости органов по аккредитации, органов по сертификации от изготовителей, продавцов, исполнителей и приобретателей;
- единой системы и правил аккредитации;
- единства правил и методов исследований (испытаний) и измерений при проведении процедур обязательной оценки соответствия;
- единства применения требований технических регламентов независимо от видов или особенностей сделок;
- недопустимости ограничения конкуренции при осуществлении аккредитации и сертификации;
- недопустимости совмещения полномочий органа государственного контроля (надзора) и органа по сертификации;
- недопустимости совмещения одним органом полномочий на аккредитацию и сертификацию;
- недопустимости внебюджетного финансирования государственного контроля (надзора) за соблюдением требований технических регламентов.

### Статья 4. Законодательство Российской Федерации о техническом регулировании

1. Законодательство РФ о техническом регулировании состоит из настоящего Федерального закона, принимаемых в соответствии с ним федеральных законов и иных нормативных правовых актов РФ.

2. Положения федеральных законов и иных нормативных правовых актов РФ, касающиеся сферы применения настоящего Федерального закона (в том числе прямо или косвенно предусматривающие осуществление контроля (надзора) за соблюдением требований технических регламентов), применяются в части, не противоречащей настоящему Федеральному закону.

3. Федеральные органы исполнительной власти вправе издавать в сфере технического регулирования акты только рекомендательного характера, за исключением случаев, установленных ст. 5 настоящего Федерального закона.

4. Если международным договором РФ в сфере технического регулирования установлены иные правила, чем те, которые предусмотрены настоящим Федеральным законом, применяются правила международного договора, а в случаях, если из международного договора следует, что для его применения требуется издание внутригосударственного акта, применяются правила международного договора и принятое на его основе законодательство РФ.

### Статья 5. Особенности технического регулирования в отношении оборонной продукции (работ, услуг) и продукции (работ, услуг), сведения о которой составляют государственную тайну

1. В случае отсутствия требований технических регламентов в отношении оборонной продукции (работ, услуг), поставляемой для федеральных государственных нужд по государственному оборонному заказу, продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством РФ информации ограниченного доступа, продукции (работ, услуг), сведения о которой составляют государственную тайну, обязательными являются требования к продукции, ее характеристикам и требования к процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, установленные федеральными органами исполнительной власти, являющимися в пределах своей компетенции государственными заказчиками оборонного заказа, и (или) государственным контрактом.

2. Порядок разработки, принятия и применения документов о стандартизации в отношении продукции (работ, услуг), указанной в п. 1 настоящей статьи, устанавливается Правительством РФ.

3. Оценка соответствия (в том числе государственный контроль (надзор) за соблюдением обязательных требований к продукции (работам, услугам), указанной в п. 1 настоящей статьи) осуществляется в порядке, установленном Правительством РФ.

4. Обязательные требования к продукции (работам, услугам), указанной в п. 1 настоящей статьи, не должны противоречить требованиям технических регламентов.

# Глава 2. Технические регламенты

## Статья 6. Цели принятия технических регламентов

1. Технические регламенты принимаются в целях:

- защиты жизни или здоровья граждан, имущества физических или юридических лиц, государственного или муниципального имущества;
- охраны окружающей среды, жизни или здоровья животных и растений;
- предупреждения действий, вводящих в заблуждение приобретателей.

2. Принятие технических регламентов в иных целях не допускается.

## Статья 7. Содержание и применение технических регламентов

1. Технические регламенты с учетом степени риска причинения вреда устанавливают минимально необходимые требования, обеспечивающие:

- безопасность излучений;
- биологическую безопасность;
- взрывобезопасность;
- механическую безопасность;
- пожарную безопасность;
- промышленную безопасность;
- термическую безопасность;
- химическую безопасность;
- электрическую безопасность;
- ядерную и радиационную безопасность;

- электромагнитную совместимость в части обеспечения безопасности работы приборов и оборудования;
- единство измерений.

2. Требования технических регламентов не могут служить препятствием осуществлению предпринимательской деятельности в большей степени, чем это минимально необходимо для выполнения целей, указанных в п. 1 ст. 6 настоящего Федерального закона.

3. Технический регламент должен содержать исчерпывающий перечень продукции, процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, в отношении которых устанавливаются его требования, и правила идентификации объекта технического регулирования для целей применения технического регламента. В техническом регламенте в целях его принятия могут содержаться правила и формы оценки соответствия (в том числе схемы подтверждения соответствия), определяемые с учетом степени риска, предельные сроки оценки соответствия в отношении каждого объекта технического регулирования и (или) требования к терминологии, упаковке, маркировке или этикеткам и правилам их нанесения.

Оценка соответствия проводится в формах государственного контроля (надзора), аккредитации, испытания, регистрации, подтверждения соответствия, приемки и ввода в эксплуатацию объекта, строительство которого закончено, и в иной форме.

Содержащиеся в технических регламентах обязательные требования к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, правилам и формам оценки соответствия, правила идентификации, требования к терминологии, упаковке, маркировке или этикеткам и правилам их нанесения являются исчерпывающими, имеют прямое действие на всей территории РФ и могут быть изменены только путем внесения изменений и дополнений в соответствующий технический регламент.

Не включенные в технические регламенты требования к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, правилам и формам оценки соответствия, правила идентификации, требования к терминологии, упаковке, маркировке или этикеткам и правилам их нанесения не могут носить обязательный характер.

4. Технический регламент должен содержать требования к характеристикам продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, но не должен содержать требования к конструкции и исполнению, за исключением случаев, если из-за отсутствия требований к конструкции и исполнению с учетом степени риска причинения вреда не обеспечивается достижение указанных в п. 1 ста-

тьи 6 настоящего Федерального закона целей принятия технического регламента.

5. В технических регламентах с учетом степени риска причинения вреда могут содержаться специальные требования к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, требования к терминологии, упаковке, маркировке или этикеткам и правилам их нанесения, обеспечивающие защиту отдельных категорий граждан (несовершеннолетних, беременных женщин, кормящих матерей, инвалидов).

6. Технические регламенты применяются одинаковым образом и в равной мере независимо от страны и (или) места происхождения продукции, осуществления процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, видов или особенностей сделок и (или) физических и (или) юридических лиц, являющихся изготовителями, исполнителями, продавцами, приобретателями с учетом положений п. 9 настоящей статьи.

7. Технический регламент не может содержать требования к продукции, причиняющей вред жизни или здоровью граждан, накапливаемый при длительном использовании этой продукции и зависящий от других факторов, не позволяющих определить степень допустимого риска. В этих случаях технический регламент может содержать требование, касающееся информирования приобретателя о возможном вреде и о факторах, от которых он зависит.

8. Международные стандарты и (или) национальные стандарты могут использоваться полностью или частично в качестве основы для разработки проектов технических регламентов.

9. Технический регламент может содержать специальные требования к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, терминологии, упаковке, маркировке или этикеткам и правилам их нанесения, применяемые в отдельных местах происхождения продукции, если отсутствие таких требований в силу климатических и географических особенностей приведет к недостижению целей, указанных в п. 1 ст. 6 настоящего Федерального закона.

Технические регламенты устанавливают также минимально необходимые ветеринарно-санитарные и фитосанитарные меры в отношении продукции, происходящей из отдельных стран и (или) мест, в том числе ограничения ввоза, использования, хранения, перевозки, реализации и утилизации, обеспечивающие биологическую безопасность (независимо от способов обеспечения безопасности, использованных изготовителем).

Ветеринарно-санитарными и фитосанитарными мерами могут предусматриваться требования к продукции, методам ее обработки и производства, процедурам испытания продукции, инспектирования, подтверждения соответствия, карантинные правила, в том числе требования, связанные с перевозкой животных и растений, необходимых для обеспечения жизни или здоровья животных и растений во время их перевозки материалов, а также методы и процедуры отбора проб, методы исследования и оценки риска и иные содержащиеся в технических регламентах требования.

Ветеринарно-санитарные и фитосанитарные меры разрабатываются и применяются на основе научных данных, а также с учетом соответствующих международных стандартов, рекомендаций и других документов международных организаций в целях соблюдения необходимого уровня ветеринарно-санитарной и фитосанитарной защиты, который определяется с учетом степени фактического научно обоснованного риска. При оценке степени риска могут приниматься во внимание положения международных стандартов, рекомендации международных организаций, участником которых является РФ, распространенность заболеваний и вредителей, а также применяемые поставщиками меры по борьбе с заболеваниями и вредителями, экологические условия, экономические последствия, связанные с возможным причинением вреда, размеры расходов на предотвращение причинения вреда.

В случае, если безотлагательное применение ветеринарно-санитарных и фитосанитарных мер необходимо для достижения целей ветеринарно-санитарной и фитосанитарной защиты, а соответствующее научное обоснование является недостаточным или не может быть получено в необходимые сроки, ветеринарно-санитарные или фитосанитарные меры, предусмотренные техническими регламентами в отношении определенных видов продукции, могут быть применены на основе имеющейся информации, в том числе информации, полученной от соответствующих международных организаций, властей иностранных государств, информации о применяемых другими государствами соответствующих мерах или иной информации. До принятия соответствующих технических регламентов в случае, установленном настоящим абзацем, ветеринарно-санитарные и фитосанитарные меры действуют в соответствии с п. 5 ст. 46 настоящего Федерального закона.

Ветеринарно-санитарные и фитосанитарные меры должны применяться с учетом соответствующих экономических факторов - потенциального ущерба от уменьшения объема производства продукции или ее продаж в случае проникновения, закрепления или распространения какого-либо вредителя или заболевания, расходов на борьбу с ними или их

ликвидацию, эффективности применения альтернативных мер по ограничению рисков, а также необходимости сведения к минимуму воздействия вредителя или заболевания на окружающую среду, производство и обращение продукции.

10. Технический регламент, принимаемый федеральным законом или постановлением Правительства РФ, вступает в силу не ранее чем через шесть месяцев со дня его официального опубликования.

11. Правила и методы исследований (испытаний) и измерений, а также правила отбора образцов для проведения исследований (испытаний) и измерений, необходимые для применения технических регламентов, разрабатываются с соблюдением положений ст. 9 настоящего Федерального закона федеральными органами исполнительной власти в пределах их компетенции в течение шести месяцев со дня официального опубликования технических регламентов и утверждаются Правительством РФ.

12. Правительство РФ разрабатывает предложения об обеспечении соответствия технического регулирования интересам национальной экономики, уровню развития материально-технической базы и уровню научно-технического развития, а также международным нормам и правилам. В этих целях Правительством РФ утверждается программа разработки технических регламентов, которая должна ежегодно уточняться и опубликовываться.

Правительством РФ организуются постоянные учет и анализ всех случаев причинения вреда вследствие нарушения требований технических регламентов жизни или здоровью граждан, имуществу физических или юридических лиц, государственному или муниципальному имуществу, окружающей среде, жизни или здоровью животных и растений с учетом тяжести этого вреда, а также организуется информирование приобретателей, изготовителей и продавцов о ситуации в области соблюдения требований технических регламентов.

### Статья 8. Виды технических регламентов

1. В РФ действуют:

- общие технические регламенты;
- специальные технические регламенты.

Обязательные требования к отдельным видам продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации определяются совокупностью требований общих технических регламентов и специальных технических регламентов.

2. Требования общего технического регламента обязательны для применения и соблюдения в отношении любых видов продукции, процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации.

3. Требованиями специального технического регламента учитываются технологические и иные особенности отдельных видов продукции, процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации.

4. Общие технические регламенты принимаются по вопросам:

- безопасной эксплуатации и утилизации машин и оборудования;
- безопасной эксплуатации зданий, строений, сооружений и безопасного использования прилегающих к ним территорий;
- пожарной безопасности;
- биологической безопасности;
- электромагнитной совместимости;
- экологической безопасности;
- ядерной и радиационной безопасности.

5. Специальные технические регламенты устанавливают требования только к тем отдельным видам продукции, процессам производства, эксплуатации, хранения, перевозки реализации и утилизации, в отношении которых цели, определенные настоящим Федеральным законом для принятия технических регламентов, не обеспечиваются требованиями общих технических регламентов.

Специальные технические регламенты устанавливают требования только к тем отдельным видам продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, степень риска причинения вреда которыми выше степени риска причинения вреда, учтенной общим техническим регламентом.

## Статья 9. Порядок разработки, принятия, изменения и отмены технического регламента

1. Технический регламент принимается федеральным законом в порядке, установленном для принятия федеральных законов, с учетом положений настоящего Федерального закона.

2. Разработчиком проекта технического регламента может быть любое лицо.

3. О разработке проекта технического регламента должно быть опубликовано уведомление в печатном издании федерального органа исполнительной власти по техническому регулированию и в информационной системе общего пользования в электронно-цифровой форме.

Уведомление о разработке проекта технического регламента должно содержать информацию о том, в отношении какой продукции, процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации будут устанавливаться разрабатываемые требования, с кратким изложением цели этого технического регламента, обоснованием необходимости его разработки и указанием тех разрабатываемых требований, которые отличаются от положений соответствующих международных стандартов или обязательных требований, действующих на территории РФ в момент разработки проекта данного технического регламента, и информацию о способе ознакомления с проектом технического регламента, наименование или фамилию, имя, отчество разработчика проекта данного технического регламента, почтовый адрес и при наличии адрес электронной почты, по которым должен осуществляться прием в письменной форме замечаний заинтересованных лиц.

Постановлением *Правительства РФ от 2 июня 2003 г. №316 Государственный комитет РФ по стандартизации и метрологии определен органом, уполномоченным исполнять функции федерального органа исполнительной власти по техническому регулированию.*

4. С момента опубликования уведомления о разработке проекта технического регламента соответствующий проект технического регламента должен быть доступен заинтересованным лицам для ознакомления. Разработчик обязан по требованию заинтересованного лица предоставить ему копию проекта технического регламента. Плата, взимаемая за предоставление данной копии, не может превышать затраты на ее изготовление.

Разработчик дорабатывает проект технического регламента с учетом полученных в письменной форме замечаний заинтересованных лиц, проводит публичное обсуждение проекта технического регламента и составляет перечень полученных в письменной форме замечаний заинтересованных лиц с кратким изложением содержания данных замечаний и результатов их обсуждения.

Разработчик обязан сохранять полученные в письменной форме замечания заинтересованных лиц до дня вступления в силу принимаемого соответствующим нормативным правовым актом технического регламента и предоставлять их депутатам Государственной Думы, представителям федеральных органов исполнительной власти и указанным в п. 9 настоя-

щей статьи экспертным комиссиям по техническому регулированию по их запросам.

Срок публичного обсуждения проекта технического регламента со дня опубликования уведомления о разработке проекта технического регламента до дня опубликования уведомления о завершении публичного обсуждения не может быть менее чем два месяца.

5. Уведомление о завершении публичного обсуждения проекта технического регламента должно быть опубликовано в печатном издании федерального органа исполнительной власти по техническому регулированию и в информационной системе общего пользования в электронно-цифровой форме.

Уведомление о завершении публичного обсуждения проекта технического регламента должно включать в себя информацию о способе ознакомления с проектом технического регламента и перечнем полученных в письменной форме замечаний заинтересованных лиц, а также наименование или фамилию, имя, отчество разработчика проекта технического регламента, почтовый адрес и при наличии адрес электронной почты, по которым с разработчиком может быть осуществлена связь.

Со дня опубликования уведомления о завершении публичного обсуждения проекта технического регламента доработанный проект технического регламента и перечень полученных в письменной форме замечаний заинтересованных лиц должны быть доступны заинтересованным лицам для ознакомления.

6. Федеральный орган исполнительной власти по техническому регулированию обязан опубликовывать в своем печатном издании уведомления о разработке проекта технического регламента и завершении публичного обсуждения этого проекта в течение десяти дней с момента оплаты опубликования уведомлений. Порядок опубликования уведомлений и размер платы за их опубликование устанавливаются Правительством РФ.

7. Внесение субъектом права законодательной инициативы проекта федерального закона о техническом регламенте в Государственную Думу осуществляется при наличии следующих документов:

- обоснование необходимости принятия федерального закона о техническом регламенте с указанием тех требований, которые отличаются от положений соответствующих международных стандартов или обязательных требований, действующих на территории РФ в момент разработки проекта технического регламента;
- финансово-экономическое обоснование принятия федерального закона о техническом регламенте;

- документы, подтверждающие опубликование уведомления о разработке проекта технического регламента в соответствии с п. 3 настоящей статьи;
- документы, подтверждающие опубликование уведомления о завершении публичного обсуждения проекта технического регламента в соответствии с п. 5 настоящей статьи;
- перечень полученных в письменной форме замечаний заинтересованных лиц, указанный в п. 4 настоящей статьи.

Внесенный в Государственную Думу проект федерального закона о техническом регламенте с приложением документов, указанных в настоящем пункте, направляется Государственной Думой в Правительство РФ. На проект федерального закона о техническом регламенте Правительство РФ в течение месяца направляет в Государственную Думу отзыв, подготовленный с учетом заключения экспертной комиссии по техническому регулированию.

8. Проект федерального закона о техническом регламенте, принятый Государственной Думой в первом чтении, публикуется в печатном издании федерального органа исполнительной власти по техническому регулированию и в информационной системе общего пользования в электронно-цифровой форме.

Поправки к принятому в первом чтении проекту федерального закона о техническом регламенте после окончания срока их подачи публикуются в информационной системе общего пользования в электронно-цифровой форме не позднее чем за месяц до рассмотрения Государственной Думой проекта федерального закона о техническом регламенте во втором чтении.

Федеральный орган исполнительной власти по техническому регулированию обязан опубликовать в своем печатном издании проект федерального закона о техническом регламенте в течение десяти дней с момента оплаты его опубликования. Порядок опубликования проекта федерального закона о техническом регламенте и размер платы за его опубликование устанавливаются Правительством РФ.

Проект федерального закона о техническом регламенте, подготовленный ко второму чтению, направляется Государственной Думой в Правительство РФ не позднее чем за месяц до рассмотрения указанного проекта Государственной Думой во втором чтении. На проект федерального закона о техническом регламенте Правительство РФ в течение месяца направляет в Государственную Думу отзыв, подготовленный с учетом заключения экспертной комиссии по техническому регулированию.

9. Экспертиза проектов технических регламентов осуществляется экспертными комиссиями по техническому регулированию, в состав которых на паритетных началах включаются представители федеральных органов исполнительной власти, научных организаций, саморегулируемых организаций, общественных объединений предпринимателей и потребителей. Порядок создания и деятельности экспертных комиссий по техническому регулированию утверждается Правительством РФ. Федеральным органом исполнительной власти по техническому регулированию утверждается персональный состав экспертных комиссий по техническому регулированию и осуществляется обеспечение их деятельности. Заседания экспертных комиссий по техническому регулированию являются открытыми.

Заключения экспертных комиссий по техническому регулированию подлежат обязательному опубликованию в печатном издании федерального органа исполнительной власти по техническому регулированию и в информационной системе общего пользования в электронно-цифровой форме. Порядок опубликования таких заключений и размер платы за их опубликование устанавливаются Правительством РФ.

10. В случае несоответствия технического регламента интересам национальной экономики, развитию материально-технической базы и уровню научно-технического развития, а также международным нормам и правилам Правительство РФ обязано начать процедуру внесения изменений в технический регламент или отмены технического регламента.

Внесение изменений и дополнений в технический регламент или его отмена осуществляется в порядке, предусмотренном настоящей статьей и статьей 10 настоящего Федерального закона в части разработки и принятия технических регламентов.

## Статья 10. Особый порядок разработки и принятия технических регламентов

1. В исключительных случаях при возникновении обстоятельств, приводящих к непосредственной угрозе жизни или здоровью граждан, окружающей среде, жизни или здоровью животных и растений, и в случаях, если для обеспечения безопасности продукции, процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации необходимо незамедлительное принятие соответствующего нормативного правового акта о техническом регламенте, Президент РФ вправе издать технический регламент без его публичного обсуждения.

2. Технический регламент может быть принят международным договором (в том числе договором с государствами - участниками Содружества Независимых Государств), подлежащим ратификации в порядке, ус-

тановленном законодательством РФ. В этом случае проект технического регламента разрабатывается в порядке, установленном пп. 2-6 ст. 9 настоящего Федерального закона.

3. До вступления в силу федерального закона о техническом регламенте Правительство РФ вправе издать постановление о соответствующем техническом регламенте, разработанном в порядке, установленном пп. 2-6 ст. 9 настоящего Федерального закона.

Проект постановления Правительства РФ о техническом регламенте, подготовленный к рассмотрению на заседании Правительства РФ, не позднее чем за месяц до его рассмотрения направляется на экспертизу в соответствующую экспертную комиссию по техническому регулированию, которая создана и осуществляет свою деятельность в порядке, установленном п. 9 ст. 9 настоящего Федерального закона. Проект постановления Правительства РФ о техническом регламенте рассматривается на заседании Правительства РФ с учетом заключения соответствующей экспертной комиссии по техническому регулированию.

Проект постановления Правительства РФ о техническом регламенте должен быть опубликован в печатном издании федерального органа исполнительной власти по техническому регулированию и в информационной системе общего пользования в электронно-цифровой форме не позднее чем за месяц до его рассмотрения на заседании Правительства РФ. Порядок опубликования указанного проекта постановления устанавливается Правительством РФ.

4. Со дня вступления в силу федерального закона о техническом регламенте соответствующий технический регламент, изданный указом Президента РФ или постановлением Правительства РФ, утрачивает силу.

# Глава 3. Стандартизация

## Статья 11. Цели стандартизации

Стандартизация осуществляется в целях:

- повышения уровня безопасности жизни или здоровья граждан, имущества физических или юридических лиц, государственного или муниципального имущества, экологической безопасности, безопасности жизни или здоровья животных и растений и содействия соблюдению требований технических регламентов;
- повышения уровня безопасности объектов с учетом риска возникновения чрезвычайных ситуаций природного и техногенного характера;
- обеспечения научно-технического прогресса;

- повышения конкурентоспособности продукции, работ, услуг;
- рационального использования ресурсов;
- технической и информационной совместимости;
- сопоставимости результатов исследований (испытаний) и измерений, технических и экономико-статистических данных;
- взаимозаменяемости продукции.

### Статья 12. Принципы стандартизации

Стандартизация осуществляется в соответствии с принципами:

- добровольного применения стандартов;
- максимального учета при разработке стандартов законных интересов заинтересованных лиц;
- применения международного стандарта как основы разработки национального стандарта, за исключением случаев, если такое применение признано невозможным вследствие несоответствия требований международных стандартов климатическим и географическим особенностям РФ, техническим и (или) технологическим особенностям или по иным основаниям либо РФ в соответствии с установленными процедурами выступала против принятия международного стандарта или отдельного его положения;
- недопустимости создания препятствий производству и обращению продукции, выполнению работ и оказанию услуг в большей степени, чем это минимально необходимо для выполнения целей, указанных в ст. 11 настоящего Федерального закона;
- недопустимости установления таких стандартов, которые противоречат техническим регламентам;
- обеспечения условий для единообразного применения стандартов.

### Статья 13. Документы в области стандартизации

К документам в области стандартизации, используемым на территории РФ, относятся:

- национальные стандарты;
- правила стандартизации, нормы и рекомендации в области стандартизации;

- применяемые в установленном порядке классификации, общероссийские классификаторы технико-экономической и социальной информации;
- стандарты организаций.

### Статья 14. Национальный орган Российской Федерации по стандартизации, технические комитеты по стандартизации

1. Национальный орган РФ по стандартизации (далее - национальный орган по стандартизации):

- утверждает национальные стандарты;
- принимает программу разработки национальных стандартов;
- организует экспертизу проектов национальных стандартов;
- обеспечивает соответствие национальной системы стандартизации интересам национальной экономики, состоянию материально-технической базы и научно-техническому прогрессу;
- осуществляет учет национальных стандартов, правил стандартизации, норм и рекомендаций в этой области и обеспечивает их доступность заинтересованным лицам;
- создает технические комитеты по стандартизации и координирует их деятельность;
- организует опубликование национальных стандартов и их распространение;
- участвует в соответствии с уставами международных организаций в разработке международных стандартов и обеспечивает учет интересов РФ при их принятии;
- утверждает изображение знака соответствия национальным стандартам;
- представляет РФ в международных организациях, осуществляющих деятельность в области стандартизации.

2. Правительство РФ определяет орган, уполномоченный на исполнение функций национального органа по стандартизации.

Постановлением *Правительства РФ от 2 июня 2003 г. № 316 Государственный комитет РФ по стандартизации и метрологии определен органом, уполномоченным исполнять функции национального органа РФ по стандартизации.*

3. В целях настоящей статьи под **опубликованием национального стандарта национальным органом по стандартизации** понимается опубликование национального стандарта на русском языке в печатном издании и в информационной системе общего пользования в электронно-цифровой форме.

4. В состав технических комитетов по стандартизации на паритетных началах и добровольной основе могут включаться представители федеральных органов исполнительной власти, научных организаций, саморегулируемых организаций, общественных объединений предпринимателей и потребителей.

Порядок создания и деятельности технических комитетов по стандартизации утверждается национальным органом по стандартизации.

Заседания технических комитетов по стандартизации являются открытыми.

## Статья 15. Национальные стандарты, общероссийские классификаторы технико-экономической и социальной информации

1. Национальные стандарты и общероссийские классификаторы технико-экономической и социальной информации, в том числе правила их разработки и применения, представляют собой национальную систему стандартизации.

2. Национальные стандарты разрабатываются в порядке, установленном настоящим Федеральным законом. Национальные стандарты утверждаются национальным органом по стандартизации в соответствии с правилами стандартизации, нормами и рекомендациями в этой области.

Национальный стандарт применяется на добровольной основе равным образом и в равной мере независимо от страны и (или) места происхождения продукции, осуществления процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ и оказания услуг, видов или особенностей сделок и (или) лиц, являющихся изготовителями, исполнителями, продавцами, приобретателями.

Применение национального стандарта подтверждается знаком соответствия национальному стандарту.

*Об использовании знака соответствия национальным стандартам см.* **приказ** *Госстандарта РФ от 15 апреля 2003 г. № 225.*

3. Общероссийские классификаторы технико-экономической и социальной информации (далее - общероссийские классификаторы) - нормативные документы, распределяющие технико-экономическую и социаль-

ную информацию в соответствии с ее классификацией (классами, группами, видами и другим) и являющиеся обязательными для применения при создании государственных информационных систем и информационных ресурсов и межведомственном обмене информацией.

Порядок разработки, принятия, введения в действие, ведения и применения общероссийских классификаторов в социально-экономической области (в том числе в области прогнозирования, статистического учета, банковской деятельности, налогообложения, при межведомственном информационном обмене, создании информационных систем и информационных ресурсов) устанавливается Правительством РФ.

**Постановлением** *Правительства РФ от 10 ноября 2003 г. № 677 утверждено* **положение** *о разработке, принятии, введении в действие, ведении и применении общероссийских классификаторов технико-экономической и социальной информации в социально-экономической области.*

## Статья 16. Правила разработки и утверждения национальных стандартов

1. Национальный орган по стандартизации разрабатывает и утверждает программу разработки национальных стандартов. Национальный орган по стандартизации должен обеспечить доступность программы разработки национальных стандартов заинтересованным лицам для ознакомления.

2. Разработчиком национального стандарта может быть любое лицо.

3. Уведомление о разработке национального стандарта направляется в национальный орган по стандартизации и публикуется в информационной системе общего пользования в электронно-цифровой форме и в печатном издании федерального органа исполнительной власти по техническому регулированию. Уведомление о разработке национального стандарта должно содержать информацию об имеющихся в проекте национального стандарта положениях, которые отличаются от положений соответствующих международных стандартов.

Разработчик национального стандарта должен обеспечить доступность проекта национального стандарта заинтересованным лицам для ознакомления. Разработчик обязан по требованию заинтересованного лица предоставить ему копию проекта национального стандарта. Плата, взимаемая разработчиком за предоставление указанной копии, не может превышать затраты на ее изготовление.

В случае, если разработчиком национального стандарта является федеральный орган исполнительной власти, плата за предоставление копии проекта национального стандарта вносится в федеральный бюджет.

4. Разработчик дорабатывает проект национального стандарта с учетом полученных в письменной форме замечаний заинтересованных лиц, проводит публичное обсуждение проекта национального стандарта и составляет перечень полученных в письменной форме замечаний заинтересованных лиц с кратким изложением содержания данных замечаний и результатов их обсуждения.

Разработчик обязан сохранять полученные в письменной форме замечания заинтересованных лиц до утверждения национального стандарта и представлять их в национальный орган по стандартизации и технические комитеты по стандартизации по их запросам.

Срок публичного обсуждения проекта национального стандарта со дня опубликования уведомления о разработке проекта национального стандарта до дня опубликования уведомления о завершении публичного обсуждения не может быть менее чем два месяца.

5. Уведомление о завершении публичного обсуждения проекта национального стандарта должно быть опубликовано в печатном издании федерального органа исполнительной власти по техническому регулированию и в информационной системе общего пользования в электронно-цифровой форме.

Со дня опубликования уведомления о завершении публичного обсуждения проекта национального стандарта доработанный проект национального стандарта и перечень полученных в письменной форме замечаний заинтересованных лиц должны быть доступны заинтересованным лицам для ознакомления.

6. Порядок опубликования уведомления о разработке проекта национального стандарта и уведомления о завершении публичного обсуждения проекта национального стандарта и размер платы за их опубликование устанавливаются Правительством РФ.

7. Проект национального стандарта одновременно с перечнем полученных в письменной форме замечаний заинтересованных лиц представляется разработчиком в технический комитет по стандартизации, который организует проведение экспертизы данного проекта.

8. На основании указанных в п. 7 настоящей статьи документов и с учетом результатов экспертизы технический комитет по стандартизации готовит мотивированное предложение об утверждении или отклонении проекта национального стандарта. Данное предложение одновременно с указанными в п. 7 настоящей статьи документами и результатами экспертизы направляется в национальный орган по стандартизации.

Национальный орган по стандартизации на основании документов, представленных техническим комитетом по стандартизации, принимает решение об утверждении или отклонении национального стандарта.

Уведомление об утверждении национального стандарта подлежит опубликованию в печатном издании федерального органа исполнительной власти по техническому регулированию и в информационной системе общего пользования в электронно-цифровой форме в течение тридцати дней со дня утверждения национального стандарта.

В случае, если национальный стандарт отклонен, мотивированное решение национального органа по стандартизации с приложением указанных в п. 7 настоящей статьи документов направляется разработчику проекта национального стандарта.

9. Национальный орган по стандартизации утверждает и опубликовывает в печатном издании федерального органа исполнительной власти по техническому регулированию и в информационной системе общего пользования в электронно-цифровой форме перечень национальных стандартов, которые могут на добровольной основе применяться для соблюдения требований технических регламентов.

## Статья 17. Стандарты организаций

1. Стандарты организаций, в том числе коммерческих, общественных, научных организаций* саморегулируемых организаций, объединений юридических лиц могут разрабатываться и утверждаться ими самостоятельно исходя из необходимости применения этих стандартов для целей, указанных в ст. 11 настоящего Федерального закона, для совершенствования производства и обеспечения качества продукции, выполнения работ, оказания услуг, а также для распространения и использования полученных в различных областях знаний результатов исследований (испытаний), измерений и разработок.

Порядок разработки, утверждения, учета, изменения и отмены стандартов организаций устанавливается ими самостоятельно с учетом положений ст. 12 настоящего Федерального закона.

Проект стандарта организации может представляться разработчиком в технический комитет по стандартизации, который организует проведение экспертизы данного проекта. На основании результатов экспертизы данного проекта технический комитет по стандартизации готовит заключение, которое направляет разработчику проекта стандарта.

2. Стандарты организаций применяются равным образом и в равной мере независимо от страны и (или) места происхождения продукции,

осуществления процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ и оказания услуг, видов или особенностей сделок и (или) лиц, которые являются изготовителями, исполнителями, продавцами, приобретателями.

## Глава 4. Подтверждение соответствия

### Статья 18. Цели подтверждения соответствия

Подтверждение соответствия осуществляется в целях:

- удостоверения соответствия продукции, процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, работ, услуг или иных объектов техническим регламентам, стандартам, условиям договоров;
- содействия приобретателям в компетентном выборе продукции, работ, услуг;
- повышения конкурентоспособности продукции, работ, услуг на российском и международном рынках;
- создания условий для обеспечения свободного перемещения товаров по территории РФ, а также для осуществления международного экономического, научно-технического сотрудничества и международной торговли.

### Статья 19. Принципы подтверждения соответствия

1. Подтверждение соответствия осуществляется на основе принципов:

- доступности информации о порядке осуществления подтверждения соответствия заинтересованным лицам;
- недопустимости применения обязательного подтверждения соответствия к объектам, в отношении которых не установлены требования технических регламентов;
- установления перечня форм и схем обязательного подтверждения соответствия в отношении определенных видов продукции в соответствующем техническом регламенте;
- уменьшения сроков осуществления обязательного подтверждения соответствия и затрат заявителя;
- недопустимости принуждения к осуществлению добровольного подтверждения соответствия, в том числе в определенной системе добровольной сертификации;

- защиты имущественных интересов заявителей, соблюдения коммерческой тайны в отношении сведений, полученных при осуществлении подтверждения соответствия;
- недопустимости подмены обязательного подтверждения соответствия добровольной сертификацией.

2. Подтверждение соответствия разрабатывается и применяется равным образом и в равной мере независимо от страны и (или) места происхождения продукции, осуществления процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ и оказания услуг, видов или особенностей сделок и (или) лиц, которые являются изготовителями, исполнителями, продавцами, приобретателями.

### Статья 20. Формы подтверждения соответствия

1. Подтверждение соответствия на территории РФ может носить добровольный или обязательный характер.

2. Добровольное подтверждение соответствия осуществляется в форме добровольной сертификации.

3. Обязательное подтверждение соответствия осуществляется в формах:

- принятия декларации о соответствии (далее - декларирование соответствия);
- обязательной сертификации.

4. Порядок применения форм обязательного подтверждения соответствия устанавливается настоящим Федеральным законом.

### Статья 21. Добровольное подтверждение соответствия

1. Добровольное подтверждение соответствия осуществляется по инициативе заявителя на условиях договора между заявителем и органом по сертификации. Добровольное подтверждение соответствия может осуществляться для установления соответствия национальным стандартам, стандартам организаций, системам добровольной сертификации, условиям договоров.

Объектами добровольного подтверждения соответствия являются продукция, процессы производства, эксплуатации, хранения, перевозки, реализации и утилизации, работы и услуги, а также иные объекты, в отношении которых стандартами, системами добровольной сертификации и договорами устанавливаются требования.

Орган по сертификации:

- осуществляет подтверждение соответствия объектов добровольного подтверждения соответствия;
- выдает сертификаты соответствия на объекты, прошедшие добровольную сертификацию;
- предоставляет заявителям право на применение знака соответствия, если применение знака соответствия предусмотрено соответствующей системой добровольной сертификации;
- приостанавливает или прекращает действие выданных им сертификатов соответствия.

2. Система добровольной сертификации может быть создана юридическим лицом и (или) индивидуальным предпринимателем или несколькими юридическими лицами и (или) индивидуальными предпринимателями.

Лицо или лица, создавшие систему добровольной сертификации, устанавливают перечень объектов, подлежащих сертификации, и их характеристик, на соответствие которым осуществляется добровольная сертификация, правила выполнения предусмотренных данной системой добровольной сертификации работ и порядок их оплаты, определяют участников данной системы добровольной сертификации. Системой добровольной сертификации может предусматриваться применение знака соответствия.

3. Система добровольной сертификации может быть зарегистрирована федеральным органом исполнительной власти по техническому регулированию.

Для регистрации системы добровольной сертификации в федеральный орган исполнительной власти по техническому регулированию представляются:

- свидетельство о государственной регистрации юридического лица и (или) индивидуального предпринимателя;
- правила функционирования системы добровольной сертификации, которыми предусмотрены положения п. 2 настоящей статьи;
- изображение знака соответствия, применяемое в данной системе добровольной сертификации, если применение знака соответствия предусмотрено, и порядок применения знака соответствия;
- документ об оплате регистрации системы добровольной сертификации.

Регистрация системы добровольной сертификации осуществляется в течение пяти дней с момента представления документов, предусмотренных настоящим пунктом для регистрации системы добровольной сертификации, в федеральный орган исполнительной власти по техническому регулированию. Порядок регистрации системы добровольной сертификации и размер платы за регистрацию устанавливаются Правительством РФ. Плата за регистрацию системы добровольной сертификации подлежит зачислению в федеральный бюджет.

4. Отказ в регистрации системы добровольной сертификации допускается только в случае непредставления документов, предусмотренных п. 3 настоящей статьи, или совпадения наименования системы и (или) изображения знака соответствия с наименованием системы и (или) изображением знака соответствия зарегистрированной ранее системы добровольной сертификации. Уведомление об отказе в регистрации системы добровольной сертификации направляется заявителю в течение трех дней со дня принятия решения об отказе в регистрации этой системы с указанием оснований для отказа.

Отказ в регистрации системы добровольной сертификации может быть обжалован в судебном порядке.

5. Федеральный орган исполнительной власти по техническому регулированию ведет единый реестр зарегистрированных систем добровольной сертификации, содержащий сведения о юридических лицах и (или) об индивидуальных предпринимателях, создавших системы добровольной сертификации, о правилах функционирования систем добровольной сертификации, которыми предусмотрены положения п. 2 настоящей статьи, знаках соответствия и порядке их применения. Федеральный орган исполнительной власти по техническому регулированию должен обеспечить доступность сведений, содержащихся в едином реестре зарегистрированных систем добровольной сертификации, заинтересованным лицам.

Порядок ведения единого реестра зарегистрированных систем добровольной сертификации и порядок предоставления сведений, содержащихся в этом реестре, устанавливаются федеральным органом исполнительной власти по техническому регулированию.

## Статья 22. Знаки соответствия

1. Объекты сертификации, сертифицированные в системе добровольной сертификации, могут маркироваться знаком соответствия системы добровольной сертификации. Порядок применения такого знака соответствия устанавливается правилами соответствующей системы добровольной сертификации.

2. Применение знака соответствия национальному стандарту осуществляется заявителем на добровольной основе любым удобным для заявителя способом в порядке, установленном национальным органом по стандартизации.

3. Объекты, соответствие которых не подтверждено в порядке, установленном настоящим Федеральным законом, не могут быть маркированы знаком соответствия.

## Статья 23. Обязательное подтверждение соответствия

1. Обязательное подтверждение соответствия проводится только в случаях, установленных соответствующим техническим регламентом, и исключительно на соответствие требованиям технического регламента.

Объектом обязательного подтверждения соответствия может быть только продукция, выпускаемая в обращение на территории РФ.

2. Форма и схемы обязательного подтверждения соответствия могут устанавливаться только техническим регламентом с учетом степени риска недостижения целей технических регламентов.

3. Декларация о соответствии и сертификат соответствия имеют равную юридическую силу независимо от схем обязательного подтверждения соответствия и действуют на всей территории РФ.

4. Работы по обязательному подтверждению соответствия подлежат оплате заявителем.

Правительством РФ устанавливается методика определения стоимости работ по обязательному подтверждению соответствия, которая предусматривает применение единых правил и принципов установления цен на продукцию одинаковых или сходных видов независимо от страны и (или) места ее происхождения, а также лиц, которые являются заявителями.

## Статья 24. Декларирование соответствия

1. Декларирование соответствия осуществляется по одной из следующих схем:

- принятие декларации о соответствии на основании собственных доказательств;
- принятие декларации о соответствии на основании собственных доказательств, доказательств, полученных с участием органа по сертификации и (или) аккредитованной испытательной лаборатории (центра) (далее - третья сторона).

При декларировании соответствия заявителем может быть зарегистрированные в соответствии с законодательством РФ на ее территории юридическое лицо или физическое лицо в качестве индивидуального предпринимателя, либо являющиеся изготовителем или продавцом, либо выполняющие функции иностранного изготовителя на основании договора с ним в части обеспечения соответствия поставляемой продукции требованиям технических регламентов и в части ответственности за несоответствие поставляемой продукции требованиям технических регламентов (лицо, выполняющее функции иностранного изготовителя).

Круг заявителей устанавливается соответствующим техническим регламентом.

Схема декларирования соответствия с участием третьей стороны устанавливается в техническом регламенте в случае, если отсутствие третьей стороны приводит к недостижению целей подтверждения соответствия.

2. При декларировании соответствия на основании собственных доказательств заявитель самостоятельно формирует доказательственные материалы в целях подтверждения соответствия продукции требованиям технических регламентов. В качестве доказательственных материалов используются техническая документация, результаты собственных исследований (испытаний) и измерений и (или) другие документы, послужившие мотивированным основанием для подтверждения соответствия продукции требованиям технических регламентов. Состав доказательственных материалов определяется соответствующим техническим регламентом.

3. При декларировании соответствия на основании собственных доказательств и полученных с участием третьей стороны доказательств заявитель по своему выбору в дополнение к собственным доказательствам, сформированным в порядке, предусмотренном п. 2 настоящей статьи:

- включает в доказательственные материалы протоколы исследований (испытаний) и измерений, проведенных в аккредитованной испытательной лаборатории (центре);
- предоставляет сертификат системы качества, в отношении которого предусматривается контроль (надзор) органа по сертификации, выдавшего данный сертификат, за объектом сертификации.

4. Сертификат системы качества может использоваться в составе доказательств при принятии декларации о соответствии любой продукции, за исключением случая, если для такой продукции техническими регламентами предусмотрена иная форма подтверждения соответствия.

5. Декларация о соответствии оформляется на русском языке и должна содержать:

- наименование и местонахождение заявителя;
- наименование и местонахождение изготовителя;
- информацию об объекте подтверждения соответствия, позволяющую идентифицировать этот объект;
- наименование технического регламента, на соответствие требованиям которого подтверждается продукция;
- указание на схему декларирования соответствия;
- заявление заявителя о безопасности продукции при ее использовании в соответствии с целевым назначением и принятии заявителем мер по обеспечению соответствия продукции требованиям технических регламентов;
- сведения о проведенных исследованиях (испытаниях) и измерениях, сертификате системы качества, а также документах, послуживших основанием для подтверждения соответствия продукции требованиям технических регламентов;
- срок действия декларации о соответствии;
- иные предусмотренные соответствующими техническими регламентами сведения.

Срок действия декларации о соответствии определяется техническим регламентом.

Форма декларации о соответствии утверждается федеральным органом исполнительной власти по техническому регулированию.

6. Оформленная по установленным правилам декларация о соответствии подлежит регистрации федеральным органом исполнительной власти по техническому регулированию в течение трех дней.

Для регистрации декларации о соответствии заявитель представляет в федеральный орган исполнительной власти по техническому регулированию оформленную в соответствии с требованиями п. 5 настоящей статьи декларацию о соответствии.

Порядок ведения реестра деклараций о соответствии, порядок предоставления содержащихся в указанном реестре сведений и порядок оплаты за предоставление содержащихся в указанном реестре сведений определяются Правительством РФ.

7. Декларация о соответствии и составляющие доказательственные материалы документы хранятся у заявителя в течение трех лет с момента окончания срока действия декларации. Второй экземпляр декларации о соответствии хранится в федеральном органе исполнительной власти по техническому регулированию.

## Статья 25. Обязательная сертификация

1. Обязательная сертификация осуществляется органом по сертификации на основании договора с заявителем. Схемы сертификации, применяемые для сертификации определенных видов продукции, устанавливаются соответствующим техническим регламентом.

2. Соответствие продукции требованиям технических регламентов подтверждается сертификатом соответствия, выдаваемым заявителю органом по сертификации.

Сертификат соответствия включает в себя:

- наименование и местонахождение заявителя;
- наименование и местонахождение изготовителя продукции, прошедшей сертификацию;
- наименование и местонахождение органа по сертификации, выдавшего сертификат соответствия;
- информацию об объекте сертификации, позволяющую идентифицировать этот объект;
- наименование технического регламента, на соответствие требованиям которого проводилась сертификация;
- информацию о проведенных исследованиях (испытаниях) и измерениях;
- информацию о документах, представленных заявителем в орган по сертификации в качестве доказательств соответствия продукции требованиям технических регламентов;
- срок действия сертификата соответствия.

Срок действия сертификата соответствия определяется соответствующим техническим регламентом.

Форма сертификата соответствия утверждается федеральным органом исполнительной власти по техническому регулированию.

## Статья 26. Организация обязательной сертификации

1. Обязательная сертификация осуществляется органом по сертификации, аккредитованным в порядке, установленном Правительством РФ.

2. Орган по сертификации:

- привлекает на договорной основе для проведения исследований (испытаний) и измерений испытательные лаборатории (центры), аккре-

дитованные в порядке, установленном Правительством РФ (далее - аккредитованные испытательные лаборатории (центры);

- осуществляет контроль за объектами сертификации, если такой контроль предусмотрен соответствующей схемой обязательной сертификации и договором;
- ведет реестр выданных им сертификатов соответствия;
- информирует соответствующие органы государственного контроля (надзора) за соблюдением требований технических регламентов о продукции, поступившей на сертификацию, но не прошедшей ее;
- приостанавливает или прекращает действие выданного им сертификата соответствия;
- обеспечивает предоставление заявителям информации о порядке проведения обязательной сертификации;
- устанавливает стоимость работ по сертификации на основе утвержденной Правительством РФ методики определения стоимости таких работ.

3. Федеральный орган исполнительной власти по техническому регулированию ведет единый реестр выданных сертификатов соответствия.

Порядок ведения единого реестра выданных сертификатов соответствия, порядок предоставления содержащихся в едином реестре сведений и порядок оплаты за предоставление содержащихся в указанном реестре сведений устанавливаются Правительством РФ.

Порядок передачи сведений о выданных сертификатах соответствия в единый реестр выданных сертификатов устанавливается федеральным органом исполнительной власти по техническому регулированию.

4. Исследования (испытания) и измерения продукции при осуществлении обязательной сертификации проводятся аккредитованными испытательными лабораториями (центрами).

Аккредитованные испытательные лаборатории (центры) проводят исследования (испытания) и измерения продукции в пределах своей области аккредитации на условиях договоров с органами по сертификации. Органы по сертификации не вправе предоставлять аккредитованным испытательным лабораториям (центрам) сведения о заявителе.

Аккредитованная испытательная лаборатория (центр) оформляет результаты исследований (испытаний) и измерений соответствующими протоколами, на основании которых орган по сертификации принимает решение о выдаче или об отказе в выдаче сертификата соответствия. Аккредитованная испытательная лаборатория (центр) обязана обеспечить достоверность результатов исследований (испытаний) и измерений.

## Статья 27. Знак обращения на рынке

1. Продукция, соответствие которой требованиям технических регламентов подтверждено в порядке, предусмотренном настоящим Федеральным законом, маркируется знаком обращения на рынке. Изображение знака обращения на рынке устанавливается Правительством РФ. Данный знак не является специальным защищенным знаком и наносится в информационных целях.

2. Маркировка знаком обращения на рынке осуществляется заявителем самостоятельно любым удобным для него способом.

Продукция, соответствие которой требованиям технических регламентов не подтверждено в порядке, установленном настоящим Федеральным законом, не может быть маркирована знаком обращения на рынке.

## Статья 28. Права и обязанности заявителя в области обязательного подтверждения соответствия

1. Заявитель вправе:

- выбирать форму и схему подтверждения соответствия, предусмотренные для определенных видов продукции соответствующим техническим регламентом;
- обращаться для осуществления обязательной сертификации в любой орган по сертификации, область аккредитации которого распространяется на продукцию, которую заявитель намеревается сертифицировать;
- обращаться в орган по аккредитации с жалобами на неправомерные действия органов по сертификации и аккредитованных испытательных лабораторий (центров) в соответствии с законодательством РФ.

2. Заявитель обязан:

- обеспечивать соответствие продукции требованиям технических регламентов;
- выпускать в обращение продукцию, подлежащую обязательному подтверждению соответствия, только после осуществления такого подтверждения соответствия;
- указывать в сопроводительной технической документации и при маркировке продукции сведения о сертификате соответствия или декларации о соответствии;
- предъявлять в органы государственного контроля (надзора) за соблюдением требований технических регламентов, а также заинтересованным лицам документы, свидетельствующие о подтверждении

соответствия продукции требованиям технических регламентов (декларацию о соответствии, сертификат соответствия или их копии);

- приостанавливать или прекращать реализацию продукции, если срок действия сертификата соответствия или декларации о соответствии истек либо действие сертификата соответствия или декларации о соответствии приостановлено либо прекращено;
- извещать орган по сертификации об изменениях, вносимых в техническую документацию или технологические процессы производства сертифицированной продукции;
- приостанавливать производство продукции, которая прошла подтверждение соответствия и не соответствует требованиям технических регламентов, на основании решений органов государственного контроля (надзора) за соблюдением требований технических регламентов.

## Статья 29. Условия ввоза на территорию Российской Федерации продукции, подлежащей обязательному подтверждению соответствия

1. Для помещения продукции, подлежащей обязательному подтверждению соответствия, под таможенные режимы, предусматривающие возможность отчуждения или использования этой продукции в соответствии с ее назначением на таможенной территории РФ, в таможенные органы одновременно с таможенной декларацией заявителем либо уполномоченным заявителем лицом представляются декларация о соответствии или сертификат соответствия либо документы об их признании в соответствии со статьей 30 настоящего Федерального закона. Представление указанных документов не требуется в случае помещения продукции под таможенный режим отказа в пользу государства.

Для целей таможенного оформления продукции списки продукции, на которую распространяется действие абзаца первого настоящего пункта, с указанием кодов Товарной номенклатуры внешнеэкономической деятельности утверждаются Правительством РФ на основании технических регламентов.

2. Продукция, определяемая в соответствии с положениями абзаца второго п. 1 настоящей статьи, подлежащая обязательному подтверждению соответствия, ввозимая на таможенную территорию РФ и помещаемая под таможенные режимы, которыми не предусмотрена возможность ее отчуждения, выпускается таможенными органами РФ на территорию РФ без представления указанных в абзаце первом п. 1 настоящей статьи документов о соответствии.

3. Порядок ввоза на таможенную территорию РФ продукции, подлежащей обязательному подтверждению соответствия и определяемой в соответствии с положениями абзаца второго п. 1 настоящей статьи и с учетом положений п. 2 настоящей статьи, утверждается Правительством РФ.

### Статья 30. Признание результатов подтверждения соответствия

Полученные за пределами территории РФ документы о подтверждении соответствия, знаки соответствия, протоколы исследований (испытаний) и измерений продукции могут быть признаны в соответствии с международными договорами РФ.

## Глава 5. Аккредитация органов по сертификации и испытательных лабораторий (центров)

### Статья 31. Аккредитация органов по сертификации и испытательных лабораторий (центров)

1. Аккредитация органов по сертификации и испытательных лабораторий (центров) осуществляется в целях:

- подтверждения компетентности органов по сертификации и испытательных лабораторий (центров), выполняющих работы по подтверждению соответствия;
- обеспечения доверия изготовителей, продавцов и приобретателей к деятельности органов по сертификации и аккредитованных испытательных лабораторий (центров);
- создания условий для признания результатов деятельности органов по сертификации и аккредитованных испытательных лабораторий (центров).

2. Аккредитация органов по сертификации и испытательных лабораторий (центров), выполняющих работы по подтверждению соответствия, осуществляется на основе принципов:

- добровольности;
- открытости и доступности правил аккредитации;
- компетентности и независимости органов, осуществляющих аккредитацию;

- недопустимости ограничения конкуренции и создания препятствий пользованию услугами органов по сертификации и аккредитованных испытательных лабораторий (центров);
- обеспечения равных условий лицам, претендующим на получение аккредитации;
- недопустимости совмещения полномочий на аккредитацию и подтверждение соответствия;
- недопустимости установления пределов действия документов об аккредитации на отдельных территориях.

3. Аккредитация органов по сертификации и испытательных лабораторий (центров), выполняющих работы по подтверждению соответствия, осуществляется в порядке, установленном Правительством РФ.

## Глава 6. Государственный контроль (надзор) за соблюдением требований технических регламентов

### Статья 32. Органы государственного контроля (надзора) за соблюдением требований технических регламентов

1. Государственный контроль (надзор) за соблюдением требований технических регламентов осуществляется федеральными органами исполнительной власти, органами исполнительной власти субъектов РФ, подведомственными им государственными учреждениями, уполномоченными на проведение государственного контроля (надзора) в соответствии с законодательством РФ (далее - органы государственного контроля (надзора).

2. Государственный контроль (надзор) за соблюдением требований технических регламентов осуществляется должностными лицами органов государственного контроля (надзора) в порядке, установленном законодательством РФ.

**Постановлением** *Правительства РФ от 17 июня 2004 г. № 294 установлено, что Федеральное агентство по техническому регулированию и метрологии осуществляет контроль и надзор за соблюдением обязательных требований государственных стандартов и технических регламентов до принятия Правительством РФ решения о передаче этих функций другим федеральным органам исполнительной власти.*

## Статья 33. Объекты государственного контроля (надзора) за соблюдением требований технических регламентов

1. Государственный контроль (надзор) за соблюдением требований технических регламентов осуществляется в отношении продукции, процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации исключительно в части соблюдения требований соответствующих технических регламентов.

2. В отношении продукции государственный контроль (надзор) за соблюдением требований технических регламентов осуществляется исключительно на стадии обращения продукции.

3. При осуществлении мероприятий по государственному контролю (надзору) за соблюдением требований технических регламентов используются правила и методы исследований (испытаний) и измерений, установленные для соответствующих технических регламентов в порядке, предусмотренном п. 11 ст. 7 настоящего Федерального закона.

## Статья 34. Полномочия органов государственного контроля (надзора)

1. На основании положений настоящего Федерального закона и требований технических регламентов органы государственного контроля (надзора) вправе:

- требовать от изготовителя (продавца, лица, выполняющего функции иностранного изготовителя) предъявления декларации о соответствии или сертификата соответствия, подтверждающих соответствие продукции требованиям технических регламентов, или их копий, если применение таких документов предусмотрено соответствующим техническим регламентом;
- осуществлять мероприятия по государственному контролю (надзору) за соблюдением требований технических регламентов в порядке, установленном законодательством РФ;
- выдавать предписания об устранении нарушений требований технических регламентов в срок, установленный с учетом характера нарушения;
- принимать мотивированные решения о запрете передачи продукции, а также о полном или частичном приостановлении процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, если иными мерами невозможно устранить нарушения требований технических регламентов;

- приостановить или прекратить действие декларации о соответствии или сертификата соответствия;
- привлекать изготовителя (исполнителя, продавца, лицо, выполняющее функции иностранного изготовителя) к ответственности, предусмотренной законодательством РФ;
- принимать иные предусмотренные законодательством РФ меры в целях недопущения причинения вреда.

2. Органы государственного контроля (надзора) обязаны:

- проводить в ходе мероприятий по государственному контролю (надзору) за соблюдением требований технических регламентов разъяснительную работу по применению законодательства РФ о техническом регулировании, информировать о существующих технических регламентах;
- соблюдать коммерческую тайну и иную охраняемую законом тайну;
- соблюдать порядок осуществления мероприятий по государственному контролю (надзору) за соблюдением требований технических регламентов и оформления результатов таких мероприятий, установленный законодательством РФ;
- принимать на основании результатов мероприятий по государственному контролю (надзору) за соблюдением требований технических регламентов меры по устранению последствий нарушений требований технических регламентов;
- направлять информацию о несоответствии продукции требованиям технических регламентов в соответствии с положениями гл. 7 настоящего Федерального закона;
- осуществлять другие предусмотренные законодательством РФ полномочия.

### Статья 35. Ответственность органов государственного контроля (надзора) и их должностных лиц при осуществлении государственного контроля (надзора) за соблюдением требований технических регламентов

1. Органы государственного контроля (надзора) и их должностные лица в случае ненадлежащего исполнения своих служебных обязанностей при проведении мероприятий по государственному контролю (надзору) за соблюдением требований технических регламентов и в случае совер-

шения противоправных действий (бездействия) несут ответственность в соответствии с законодательством РФ.

2. О мерах, принятых в отношении виновных в нарушении законодательства РФ должностных лиц органов государственного контроля (надзора), органы государственного контроля (надзора) в течение месяца обязаны сообщить юридическому лицу и (или) индивидуальному предпринимателю, права и законные интересы которых нарушены.

## Глава 7. Информация о нарушении требований технических регламентов и отзыв продукции

### Статья 36. Ответственность за несоответствие продукции, процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации требованиям технических регламентов

1. За нарушение требований технических регламентов изготовитель (исполнитель, продавец, лицо, выполняющее функции иностранного изготовителя) несет ответственность в соответствии с законодательством РФ.

2. В случае неисполнения предписаний и решений органа государственного контроля (надзора) изготовитель (исполнитель, продавец, лицо, выполняющее функции иностранного изготовителя) несет ответственность в соответствии с законодательством РФ.

3. В случае, если в результате несоответствия продукции требованиям технических регламентов, нарушений требований технических регламентов при осуществлении процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации причинен вред жизни или здоровью граждан, имуществу физических или юридических лиц, государственному или муниципальному имуществу, окружающей среде, жизни или здоровью животных и растений или возникла угроза причинения такого вреда, изготовитель (исполнитель, продавец, лицо, выполняющее функции иностранного изготовителя) обязан возместить причиненный вред и принять меры в целях недопущения причинения вреда другим лицам, их имуществу, окружающей среде в соответствии с законодательством РФ.

4. Обязанность возместить вред не может быть ограничена договором или заявлением одной из сторон. Соглашения или заявления об ограничении ответственности ничтожны.

## Статья 37. Информация о несоответствии продукции требованиям технических регламентов

1. Изготовитель (исполнитель, продавец, лицо, выполняющее функции иностранного изготовителя), которому стало известно о несоответствии выпущенной в обращение продукции требованиям технических регламентов, обязан сообщить об этом в орган государственного контроля (надзора) в соответствии с его компетенцией в течение десяти дней с момента получения указанной информации.

Продавец (исполнитель, лицо, выполняющее функции иностранного изготовителя), получивший указанную информацию, в течение десяти дней обязан довести ее до изготовителя.

2. Лицо, которое не является изготовителем (исполнителем, продавцом, лицом, выполняющим функции иностранного изготовителя) и которому стало известно о несоответствии выпущенной в обращение продукции требованиям технических регламентов, вправе направить информацию о несоответствии продукции требованиям технических регламентов в орган государственного контроля (надзора).

При получении такой информации орган государственного контроля (надзора) в течение пяти дней обязан известить изготовителя (продавца, лицо, выполняющее функции иностранного изготовителя) о ее поступлении.

## Статья 38. Обязанности изготовителя (продавца, лица, выполняющего функции иностранного изготовителя) в случае получения информации о несоответствии продукции требованиям технических регламентов

1. В течение десяти дней с момента получения информации о несоответствии продукции требованиям технических регламентов, если необходимость установления более длительного срока не следует из существа проводимых мероприятий, изготовитель (продавец, лицо, выполняющее функции иностранного изготовителя) обязан провести проверку достоверности полученной информации. По требованию органа государственного контроля (надзора) изготовитель (продавец, лицо, выполняющее функции иностранного изготовителя) обязан представить материалы указанной проверки в орган государственного контроля (надзора).

В случае получения информации о несоответствии продукции требованиям технических регламентов изготовитель (продавец, лицо, выполняющее функции иностранного изготовителя) обязан принять необходимые меры для того, чтобы до завершения проверки, предусмотренной абзацем первым настоящего пункта, возможный вред, связанный с обращением данной продукции, не увеличился.

2. При подтверждении достоверности информации о несоответствии продукции требованиям технических регламентов изготовитель (продавец, лицо, выполняющее функции иностранного изготовителя) в течение десяти дней с момента подтверждения достоверности такой информации обязан разработать программу и согласовать ее с органом государственного контроля (надзора) в соответствии с его компетенцией.

Программа должна включать в себя мероприятия по оповещению приобретателей о наличии угрозы причинения вреда и способах его предотвращения, а также сроки реализации таких мероприятий. В случае, если для предотвращения причинения вреда необходимо произвести дополнительные расходы, изготовитель (продавец, лицо, выполняющее функции иностранного изготовителя) обязан осуществить все мероприятия по предотвращению причинения вреда своими силами, а при невозможности их осуществления объявить об отзыве продукции и возместить убытки, причиненные приобретателям в связи с отзывом продукции.

Устранение недостатков, а также доставка продукции к месту устранения недостатков и возврат ее приобретателям осуществляются изготовителем (продавцом, лицом, выполняющим функции иностранного изготовителя) и за его счет.

3. В случае, если угроза причинения вреда не может быть устранена путем проведения мероприятий, указанных в п. 2 настоящей статьи, изготовитель (продавец, лицо, выполняющее функции иностранного изготовителя) обязан незамедлительно приостановить производство и реализацию продукции, отозвать продукцию и возместить приобретателям убытки, возникшие в связи с отзывом продукции.

4. На весь период действия программы мероприятий по предотвращению причинения вреда изготовитель (продавец, лицо, выполняющее функции иностранного изготовителя) за свой счет обязан обеспечить приобретателям возможность получения оперативной информации о необходимых действиях.

### Статья 39. Права органов государственного контроля (надзора) в случае получения информации о несоответствии продукции требованиям технических регламентов

1. Органы государственного контроля (надзора) в случае получения информации о несоответствии продукции требованиям технических регламентов в возможно короткие сроки проводят проверку достоверности полученной информации.

В ходе проведения проверки органы государственного контроля (надзора) вправе:

- требовать от изготовителя (продавца, лица, выполняющего функции иностранного изготовителя) материалы проверки достоверности информации о несоответствии продукции требованиям технических регламентов;
- запрашивать у изготовителя (исполнителя, продавца, лица, выполняющего функции иностранного изготовителя) и иных лиц дополнительную информацию о продукции, процессах производства, эксплуатации, хранения, перевозки, реализации и утилизации, в том числе результаты исследований (испытаний) и измерений, проведенных при осуществлении обязательного подтверждения соответствия;
- направлять запросы в другие федеральные органы исполнительной власти;
- при необходимости привлекать специалистов для анализа полученных материалов.

2. При признании достоверности информации о несоответствии продукции требованиям технических регламентов орган государственного контроля (надзора) в соответствии с его компетенцией в течение десяти дней выдает предписание о разработке изготовителем (продавцом, лицом, выполняющим функции иностранного изготовителя) программы мероприятий по предотвращению причинения вреда, оказывает содействие в ее реализации и осуществляет контроль за ее выполнением.

Орган государственного контроля (надзора):

- способствует распространению информации о сроках и порядке проведения мероприятий по предотвращению причинения вреда;
- запрашивает у изготовителя (продавца, лица, выполняющего функции иностранного изготовителя) и иных лиц документы, подтверждающие проведение мероприятий, указанных в программе мероприятий по предотвращению причинения вреда;
- проверяет соблюдение сроков, указанных в программе мероприятий по предотвращению причинения вреда;
- принимает решение об обращении в суд с иском о принудительном отзыве продукции.

## Статья 40. Принудительный отзыв продукции

1. В случае невыполнения предписания, предусмотренного п. 2 ст. 39 настоящего Федерального закона, или невыполнения программы мероприятий по предотвращению причинения вреда орган государственного контроля (надзора) в соответствии с его компетенцией, а также иные лица, которым стало известно о невыполнении изготовителем (продавцом,

лицом, выполняющим функции иностранного изготовителя) программы мероприятий по предотвращению причинения вреда, вправе обратиться в суд с иском о принудительном отзыве продукции.

2. В случае удовлетворения иска о принудительном отзыве продукции суд обязывает ответчика совершить определенные действия, связанные с отзывом продукции, в установленный судом срок, а также довести решение суда не позднее одного месяца со дня его вступления в законную силу до сведения приобретателей через средства массовой информации или иным способом.

В случае, если ответчик не исполнит решение суда в установленный срок, истец вправе совершить эти действия за счет ответчика с взысканием с него необходимых расходов.

3. За нарушение требований настоящего Федерального закона об отзыве продукции могут быть применены меры уголовного и административного воздействия в соответствии с законодательством РФ.

### Статья 41. Ответственность за нарушение правил выполнения работ по сертификации

Орган по сертификации и должностное лицо органа по сертификации, нарушившие правила выполнения работ по сертификации, если такое нарушение повлекло за собой выпуск в обращение продукции, не соответствующей требованиям технических регламентов, несут ответственность в соответствии с законодательством РФ и договором о проведении работ по сертификации.

### Статья 42. Ответственность аккредитованной испытательной лаборатории (центра)

Аккредитованная испытательная лаборатория (центр), эксперты в соответствии с законодательством РФ и договором несут ответственность за недостоверность или необъективность результатов исследований (испытаний) и измерений.

## Глава 8. Информация о технических регламентах и документах по стандартизации

### Статья 43. Информация о документах по стандартизации

1. Национальные стандарты и общероссийские классификаторы, а также информация об их разработке должны быть доступны заинтересованным лицам.

2. Официальное опубликование в установленном порядке национальных стандартов и общероссийских классификаторов осуществляется национальным органом по стандартизации. Порядок опубликования национальных стандартов и общероссийских классификаторов определяется Правительством РФ.

### Статья 44. Федеральный информационный фонд технических регламентов и стандартов

1. Технические регламенты, документы национальной системы стандартизации, международные стандарты, правила стандартизации, нормы стандартизации и рекомендации по стандартизации, национальные стандарты других государств и информация о международных договорах в области стандартизации и подтверждения соответствия и о правилах их применения составляют Федеральный информационный фонд технических регламентов и стандартов.

Федеральный информационный фонд технических регламентов и стандартов является государственным информационным ресурсом.

Порядок создания и ведения Федерального информационного фонда технических регламентов и стандартов, а также правила пользования этим фондом устанавливаются Правительством РФ.

2. В РФ в порядке и на условиях, которые установлены Правительством РФ, создается и функционирует единая информационная система, предназначенная для обеспечения заинтересованных лиц информацией о документах, входящих в состав Федерального информационного фонда технических регламентов и стандартов.

Заинтересованным лицам обеспечивается свободный доступ к создаваемым информационным ресурсам, за исключением случаев, если в интересах сохранения государственной, служебной или коммерческой тайны такой доступ должен быть ограничен.

## Глава 9. Финансирование в области технического регулирования

### Статья 45. Порядок финансирования за счет средств федерального бюджета расходов в области технического регулирования

1. За счет средств федерального бюджета могут финансироваться расходы на:

- проведение на федеральном уровне государственного контроля (надзора) за соблюдением требований технических регламентов;

- создание и ведение Федерального информационного фонда технических регламентов и стандартов;
- реализацию программы разработки технических регламентов и программы разработки национальных стандартов, предусмотренных п. 12 ст. 7 и п. 1 ст. 16 настоящего Федерального закона, а также проведение экспертизы отдельных проектов технических регламентов и национальных стандартов;
- разработку общероссийских классификаторов;
- уплату взносов международным организациям по стандартизации.

2. Порядок финансирования расходов, указанных в п. 1 настоящей статьи, определяется Правительством РФ.

## Глава 10. Заключительные и переходные положения

### Статья 46. Переходные положения

1. Со дня вступления в силу настоящего Федерального закона впредь до вступления в силу соответствующих технических регламентов требования к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, установленные нормативными правовыми актами РФ и нормативными документами федеральных органов исполнительной власти, подлежат обязательному исполнению только в части, соответствующей целям:

- защиты жизни или здоровья граждан, имущества физических или юридических лиц, государственного или муниципального имущества;
- охраны окружающей среды, жизни или здоровья животных и растений;
- предупреждения действий, вводящих в заблуждение приобретателей.

2. Со дня вступления в силу настоящего Федерального закона обязательное подтверждение соответствия осуществляется только в отношении продукции, выпущенной в обращение на территории РФ.

3. Правительством РФ до вступления в силу соответствующих технических регламентов определяется и ежегодно дополняется перечень отдельных видов продукции, в отношении которых обязательная сертификация заменяется декларированием соответствия, осуществляемым в порядке, установленном настоящим Федеральным законом.

4. До вступления в силу соответствующих технических регламентов схема декларирования соответствия на основе собственных доказательств

допускается для применения только изготовителями или только лицами, выполняющими функции иностранного изготовителя.

5. До принятия соответствующих технических регламентов техническое регулирование в области применения ветеринарно-санитарных и фитосанитарных мер осуществляется в соответствии с Федеральным законом «О карантине растений» и Законом РФ «О ветеринарии».

6. До принятия общего технического регламента по ядерной и радиационной безопасности техническое регулирование в области ядерной и радиационной безопасности осуществляется в соответствии с Федеральным законом «Об использовании атомной энергии» и Федеральным законом «О радиационной безопасности населения».

7. Технические регламенты должны быть приняты в течение семи лет со дня вступления в силу настоящего Федерального закона.

Обязательные требования к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, в отношении которых технические регламенты в указанный срок не были приняты, прекращают действие по его истечении.

8. Документы об аккредитации, выданные в установленном порядке органам по сертификации и аккредитованным испытательным лабораториям (центрам) до вступления в силу настоящего Федерального закона, а также документы, подтверждающие соответствие (сертификат соответствия, декларация о соответствии) и принятые до вступления в силу настоящего Федерального закона, считаются действительными до окончания срока, установленного в них.

### Статья 47. Приведение нормативных правовых актов в соответствие с настоящим Федеральным законом

Со дня вступления в силу настоящего Федерального закона признать утратившими силу:

- Закон РФ от 10 июня 1993 г. № 5151-I «О сертификации продукции и услуг» (Ведомости Съезда народных депутатов и Верховного Совета РФ, 1993, №26, ст. 966);
- постановление Верховного Совета РФ от 10 июня 1993 г. №5153-I «О введении в действие Закона РФ «О сертификации продукции и услуг» (Ведомости Съезда народных депутатов и Верховного Совета РФ, 1993, №26, ст. 967);
- Закон РФ от 10 июня 1993 г. № 5154-I «О стандартизации» (Ведомости Съезда народных депутатов и Верховного Совета РФ, 1993, № 25, ст. 917);

- постановление Верховного Совета РФ от 10 июня 1993 г. №5156-I «О введении в действие Закона РФ «О стандартизации» (Ведомости Съезда народных депутатов и Верховного Совета РФ, 1993, №25, ст. 918);
- пункты 12 и 13 статьи 1 Федерального закона от 27 декабря 1995 г. №211-ФЗ «О внесении изменений и дополнений в отдельные законодательные акты РФ в связи с принятием Федерального закона «О пожарной безопасности» (Собрание законодательства РФ, 1996, № 1, ст. 4);
- пункт 2 статьи 1 Федерального закона от 2 марта 1998 г. № 30-ФЗ «О внесении изменений и дополнений в отдельные законодательные акты РФ в связи с принятием Федерального закона «О рекламе» (Собрание законодательства РФ, 1998, № 10, ст. 1143);
- Федеральный закон от 31 июля 1998 г. № 154-ФЗ «О внесении изменений и дополнений в Закон РФ «О сертификации продукции и услуг» (Собрание законодательства РФ, 1998, № 31, ст. 3832);
- статью 2 Федерального закона от 10 июля 2002 г. № 87-ФЗ «О внесении изменения в статью 6 Федерального закона «Об основах социального обслуживания населения в РФ» и дополнения в статью 2 Закона РФ «О стандартизации» (Собрание законодательства РФ, 2002, №28, ст. 2791);
- статьи 13 и 14 Федерального закона от 25 июля 2002 г. № 116-ФЗ «О внесении изменений и дополнений в некоторые законодательные акты РФ в связи с совершенствованием государственного управления в области пожарной безопасности» (Собрание законодательства РФ, 2002, № 30, ст. 3033).

### Статья 48. Вступление в силу настоящего Федерального закона

Настоящий Федеральный закон вступает в силу по истечении шести месяцев со дня его официального опубликования.

*Президент РФ*
*В. Путин*
*Москва, Кремль*
*27 декабря 2002 г. № 184-ФЗ*

## Приложение 8

# ФЕДЕРАЛЬНЫЙ ЗАКОН «О ЛИЦЕНЗИРОВАНИИ ОТДЕЛЬНЫХ ВИДОВ ДЕЯТЕЛЬНОСТИ»

от 8 августа 2001 г. № 128-ФЗ
(с изменениями от 13, 21 марта,
9 декабря 2002 г., 10 января, 27 февраля,
11, 26 марта, 23 декабря 2003 г., 2 ноября 2004 г.)
Принят Государственной Думой 13 июля 2001 г.
Одобрен Советом Федерации 20 июля 2001 г.

### Статья 1. Сфера применения настоящего Федерального закона

1. Настоящий Федеральный закон регулирует отношения, возникающие между федеральными органами исполнительной власти, органами исполнительной власти субъектов РФ, юридическими лицами и индивидуальными предпринимателями в связи с осуществлением лицензирования отдельных видов деятельности в соответствии с перечнем, предусмотренным п. 1 ст. 17 настоящего Федерального закона.

2. Действие настоящего Федерального закона не распространяется на следующие виды деятельности:

- деятельность кредитных организаций;
- деятельность, связанная с защитой государственной тайны;
- деятельность в области производства и оборота этилового спирта, алкогольной и спиртосодержащей продукции;
- деятельность в области связи;
- биржевая деятельность;
- деятельность в области таможенного дела;
- нотариальная деятельность;
- страховая деятельность, за исключением пенсионного страхования, осуществляемого негосударственными пенсионными фондами;
- деятельность профессиональных участников рынка ценных бумаг;

- осуществление внешнеэкономических операций;
- осуществление международных автомобильных перевозок грузов и пассажиров;
- приобретение оружия и патронов к нему;
- использование результатов интеллектуальной деятельности;
- использование орбитально-частотных ресурсов и радиочастот для осуществления телевизионного вещания и радиовещания (в том числе вещания дополнительной информации);
- использование природных ресурсов, в том числе недр, лесного фонда, объектов растительного и животного мира;
- деятельность, работы и услуги в области использования атомной энергии;
- образовательная деятельность.

## Статья 2. Основные понятия

В целях настоящего Федерального закона применяются следующие основные понятия:

- **лицензия** - специальное разрешение на осуществление конкретного вида деятельности при обязательном соблюдении лицензионных требований и условий, выданное лицензирующим органом юридическому лицу или индивидуальному предпринимателю;
- **лицензируемый вид деятельности** - вид деятельности, на осуществление которого на территории РФ требуется получение лицензии в соответствии с настоящим Федеральным законом;
- **лицензирование** - мероприятия, связанные с предоставлением лицензий, переоформлением документов, подтверждающих наличие лицензий, приостановлением и возобновлением действия лицензий, аннулированием лицензий и контролем лицензирующих органов за соблюдением лицензиатами при осуществлении лицензируемых видов деятельности соответствующих лицензионных требований и условий;
- **лицензионные требования и условия** - совокупность установленных положениями о лицензировании конкретных видов деятельности требований и условий, выполнение которых лицензиатом обязательно при осуществлении лицензируемого вида деятельности;

- **лицензирующие органы** - федеральные органы исполнительной власти, органы исполнительной власти субъектов РФ, осуществляющие лицензирование в соответствии с настоящим Федеральным законом;
- **лицензиат** - юридическое лицо или индивидуальный предприниматель, имеющие лицензию на осуществление конкретного вида деятельности;
- **соискатель лицензии** - юридическое лицо или индивидуальный предприниматель, обратившиеся в лицензирующий орган с заявлением о предоставлении лицензии на осуществление конкретного вида деятельности;
- **реестр лицензий** - совокупность данных о предоставлении лицензий, переоформлении документов, подтверждающих наличие лицензий, приостановлении и возобновлении действия лицензий и об аннулировании лицензий.

### Статья 3. Основные принципы осуществления лицензирования

Основными принципами осуществления лицензирования являются:

- обеспечение единства экономического пространства на территории РФ;
- установление единого перечня лицензируемых видов деятельности;
- установление единого порядка лицензирования на территории РФ;
- установление лицензионных требований и условий положениями о лицензировании конкретных видов деятельности;
- гласность и открытость лицензирования;
- соблюдение законности при осуществлении лицензирования.

### Статья 4. Критерии определения лицензируемых видов деятельности

К лицензируемым видам деятельности относятся виды деятельности, осуществление которых может повлечь за собой нанесение ущерба правам, законным интересам, здоровью граждан, обороне и безопасности государства, культурному наследию народов РФ и регулирование которых не может осуществляться иными методами, кроме как лицензированием.

### Статья 5. Определение полномочий Правительства Российской Федерации при осуществлении лицензирования

В целях обеспечения единства экономического пространства на территории РФ Правительство РФ в соответствии с определенными Президентом РФ основными направлениями внутренней политики государства:

- утверждает положения о лицензировании конкретных видов деятельности;
- определяет федеральные органы исполнительной власти, осуществляющие лицензирование конкретных видов деятельности;
- устанавливает виды деятельности, лицензирование которых осуществляется органами исполнительной власти субъектов РФ.

### Статья 6. Полномочия лицензирующих органов

1. Лицензирующие органы осуществляют следующие полномочия:

- предоставление лицензий;
- переоформление документов, подтверждающих наличие лицензий;
- приостановление действия лицензий;
- возобновление действия лицензий;
- аннулирование лицензий (в случае, предусмотренном п. 3 ст. 13 настоящего Федерального закона);
- ведение реестра лицензий;
- контроль за соблюдением лицензиатами при осуществлении лицензируемых видов деятельности соответствующих лицензионных требований и условий.

Порядок осуществления полномочий лицензирующих органов устанавливается положениями о лицензировании конкретных видов деятельности.

2. Федеральные органы исполнительной власти по соглашению с органами исполнительной власти субъектов РФ могут передавать им осуществление своих полномочий, предусмотренных п. 1 настоящей статьи.

### Статья 7. Действие лицензии

1. На каждый вид деятельности, указанный в п. 1 ст. 17 настоящего Федерального закона, предоставляется лицензия.

Вид деятельности, на осуществление которого предоставлена лицензия, может выполняться только получившим лицензию юридическим лицом или индивидуальным предпринимателем.

2. Деятельность, на осуществление которой лицензия предоставлена федеральным органом исполнительной власти или органом исполнительной власти субъекта РФ, может осуществляться на всей территории РФ. Деятельность, на осуществление которой лицензия предоставлена лицензирующим органом субъекта РФ, может осуществляться на территориях иных субъектов РФ при условии уведомления лицензиатом лицензирующих органов соответствующих субъектов РФ в порядке, установленном Правительством РФ.

## Статья 8. Срок действия лицензии

Срок действия лицензии не может быть менее чем пять лет. Срок действия лицензии по его окончании может быть продлен по заявлению лицензиата.

Продление срока действия лицензии осуществляется в порядке переоформления документа, подтверждающего наличие лицензии.

Положениями о лицензировании конкретных видов деятельности может быть предусмотрено бессрочное действие лицензии.

## Статья 9. Принятие решения о предоставлении лицензии

1. Для получения лицензии соискатель лицензии представляет в соответствующий лицензирующий орган следующие документы:

- заявление о предоставлении лицензии с указанием наименования и организационно-правовой формы юридического лица, места его нахождения - для юридического лица; фамилии, имени, отчества, места жительства, данных документа, удостоверяющего личность, - для индивидуального предпринимателя; лицензируемого вида деятельности, который юридическое лицо или индивидуальный предприниматель намерены осуществлять;
- копии учредительных документов и копия документа о государственной регистрации соискателя лицензии в качестве юридического лица (с предъявлением оригиналов в случае, если копии не заверены нотариусом) - для юридического лица;
- копия свидетельства о государственной регистрации гражданина в качестве индивидуального предпринимателя (с предъявлением ори-

гинала в случае, если копия не заверена нотариусом) - для индивидуального предпринимателя;

- копия свидетельства о постановке соискателя лицензии на учет в налоговом органе (с предъявлением оригинала в случае, если копия не заверена нотариусом);
- документ, подтверждающий уплату лицензионного сбора за рассмотрение лицензирующим органом заявления о предоставлении лицензии;
- сведения о квалификации работников соискателя лицензии.

Кроме указанных документов в положениях о лицензировании конкретных видов деятельности может быть предусмотрено представление иных документов, наличие которых при осуществлении конкретного вида деятельности установлено соответствующими федеральными законами, а также иными нормативными правовыми актами, принятие которых предусмотрено соответствующими федеральными законами.

Не допускается требовать от соискателя лицензии представления документов, не предусмотренных настоящим Федеральным законом и иными федеральными законами.

Все документы, представленные в соответствующий лицензирующий орган для предоставления лицензии, принимаются по описи, копия которой направляется (вручается) соискателю лицензии с отметкой о дате приема документов указанным органом.

За предоставление недостоверных или искаженных сведений соискатель лицензии несет ответственность в соответствии с законодательством РФ.

2. Лицензирующий орган принимает решение о предоставлении или об отказе в предоставлении лицензии в срок, не превышающий шестидесяти дней со дня поступления заявления о предоставлении лицензии со всеми необходимыми документами. Соответствующее решение оформляется приказом лицензирующего органа.

Более короткие сроки принятия решения о предоставлении или об отказе в предоставлении лицензии могут устанавливаться положениями о лицензировании конкретных видов деятельности.

Лицензирующий орган обязан в указанный срок уведомить соискателя лицензии о принятии решения о предоставлении или об отказе в предоставлении лицензии.

Уведомление о предоставлении лицензии направляется (вручается) соискателю лицензии в письменной форме с указанием реквизитов банковского счета и срока уплаты лицензионного сбора за предоставление лицензии.

Уведомление об отказе в предоставлении лицензии направляется (вручается) соискателю лицензии в письменной форме с указанием причин отказа.

В течение трех дней после представления соискателем лицензии документа, подтверждающего уплату лицензионного сбора за предоставление лицензии, лицензирующий орган бесплатно выдает лицензиату документ, подтверждающий наличие лицензии.

Лицензиат имеет право на получение дубликатов указанного документа. Дубликаты указанного документа предоставляются лицензиату за плату, равную плате, установленной за предоставление информации, содержащейся в реестре лицензий.

3. Основанием отказа в предоставлении лицензии является:

- наличие в документах, представленных соискателем лицензии, недостоверной или искаженной информации;
- несоответствие соискателя лицензии, принадлежащих ему или используемых им объектов лицензионным требованиям и условиям.

Не допускается отказ в выдаче лицензии на основании величины объема продукции (работ, услуг), производимой или планируемой для производства соискателем лицензии.

4. Соискатель лицензии имеет право обжаловать в порядке, установленном законодательством РФ, отказ лицензирующего органа в предоставлении лицензии или его бездействие.

### Статья 10. Содержание подтверждающего наличие лицензии документа и решения о предоставлении лицензии

В решении о предоставлении лицензии и в подтверждающем наличие лицензии документе указываются:

- наименование лицензирующего органа;
- наименование и организационно-правовая форма юридического лица, место его нахождения, основной государственный регистрационный номер юридического лица - для юридического лица;
- фамилия, имя, отчество, место жительства, данные документа, удостоверяющего личность, основной государственный регистрационный номер записи о государственной регистрации индивидуального предпринимателя - для индивидуального предпринимателя;
- лицензируемый вид деятельности;

- срок действия лицензии;
- идентификационный номер налогоплательщика;
- номер лицензии;
- дата принятия решения о предоставлении лицензии.

### Статья 11. Переоформление документа, подтверждающего наличие лицензии

1. В случае преобразования юридического лица, изменения его наименования или места его нахождения, либо изменения имени или места жительства индивидуального предпринимателя, либо утраты документа, подтверждающего наличие лицензии, а также в иных предусмотренных федеральными законами случаях, лицензиат - юридическое лицо (его правопреемник) или индивидуальный предприниматель - обязан не позднее чем через пятнадцать дней подать заявление о переоформлении документа, подтверждающего наличие лицензии, с приложением документов, подтверждающих указанные изменения или утрату документа, подтверждающего наличие лицензии.

2. При переоформлении документа, подтверждающего наличие лицензии, лицензирующий орган вносит соответствующие изменения в реестр лицензий. Переоформление документа, подтверждающего наличие лицензии, осуществляется в течение десяти дней со дня получения лицензирующим органом соответствующего заявления.

3. За переоформление документа, подтверждающего наличие лицензии, взимается плата в размере 100 рублей, которая зачисляется в соответствующий бюджет.

### Статья 12. Осуществление контроля

1. Контроль за соблюдением лицензиатом лицензионных требований и условий, определенных положением о лицензировании конкретного вида деятельности, осуществляется лицензирующими органами в пределах их компетенции.

2. Лицензирующие органы имеют право:

- проводить проверки деятельности лицензиата на предмет ее соответствия лицензионным требованиям и условиям;
- запрашивать у лицензиата необходимые объяснения и документы при проведении проверок;

- составлять на основании результатов проверок акты (протоколы) с указанием конкретных нарушений;
- выносить решения, обязывающие лицензиата устранить выявленные нарушения, устанавливать сроки устранения таких нарушений;
- выносить предупреждение лицензиату.

### Статья 13. Приостановление действия лицензии и аннулирование лицензии

1. Лицензирующие органы вправе приостанавливать действие лицензии в случае выявления лицензирующими органами неоднократных нарушений или грубого нарушения лицензиатом лицензионных требовании и условии.

Лицензирующий орган обязан установить срок устранения лицензиатом нарушений, повлекших за собой приостановление действия лицензии. Указанный срок не может превышать шесть месяцев. В случае, если в установленный срок лицензиат не устранил указанные нарушения, лицензирующий орган обязан обратиться в суд с заявлением об аннулировании лицензии.

Лицензиат обязан уведомить в письменной форме лицензирующий орган об устранении им нарушений, повлекших за собой приостановление действия лицензии. Лицензирующий орган, приостановивший действие лицензии, принимает решение о возобновлении ее действия и сообщает об этом в письменной форме лицензиату в течение трех дней после получения соответствующего уведомления и проверки устранения лицензиатом нарушений, повлекших за собой приостановление действия лицензии.

Плата за возобновление действия лицензии не взимается. Срок действия лицензии на время приостановления ее действия не продлевается.

2. Лицензия теряет юридическую силу в случае ликвидации юридического лица или прекращения его деятельности в результате реорганизации, за исключением его преобразования, либо прекращения действия свидетельства о государственной регистрации гражданина в качестве индивидуального предпринимателя.

3. Лицензирующие органы могут аннулировать лицензию без обращения в суд в случае неуплаты лицензиатом в течение трех месяцев лицензионного сбора за предоставление лицензии.

4. Лицензия может быть аннулирована решением суда на основании заявления лицензирующего органа в случае, если нарушение лицензиа-

том лицензионных требований и условий повлекло за собой нанесение ущерба правам, законным интересам, здоровью граждан, обороне и безопасности государства, культурному наследию народов РФ и (или) в случае, предусмотренном абзацем вторым п. 1 настоящей статьи. Одновременно с подачей заявления в суд лицензирующий орган вправе приостановить действие указанной лицензии на период до вступления в силу решения суда.

5. Решение о приостановлении действия лицензии, об аннулировании лицензии или о направлении заявления об аннулировании лицензии в суд доводится лицензирующим органом до лицензиата в письменной форме с мотивированным обоснованием такого решения не позднее чем через три дня после его принятия.

6. Решение о приостановлении действия лицензии и об аннулировании лицензии может быть обжаловано в порядке, установленном законодательством РФ.

7. Лицензирующий орган не вправе проводить проверки по предмету ведения иных органов государственной власти и органов местного самоуправления.

### Статья 14. Ведение реестров лицензий

1. Лицензирующие органы ведут реестры лицензий на виды деятельности, лицензирование которых они осуществляют.

В реестре лицензий помимо сведений, указанных в ст. 10 настоящего Федерального закона, должны быть указаны:

- сведения о регистрации лицензии в реестре лицензий;
- основания и даты приостановления и возобновления действия лицензии;
- основание и дата аннулирования лицензии;
- иные сведения, определенные положениями о лицензировании конкретных видов деятельности.

2. Информация, содержащаяся в реестре лицензий, является открытой для ознакомления с ней физических и юридических лиц.

Информация, содержащаяся в реестре лицензий, в виде выписок о конкретных лицензиатах предоставляется физическим и юридическим лицам за плату. Размер платы за предоставление указанной информации составляет 10 рублей.

Плата за предоставление информации, содержащейся в реестре лицензий, зачисляется в соответствующий бюджет.

Информация из реестра лицензий органам государственной власти и органам местного самоуправления предоставляется бесплатно.

Срок предоставления информации из реестра лицензий не может превышать три дня со дня поступления соответствующего заявления.

### Статья 15. Лицензионные сборы

За рассмотрение лицензирующим органом заявления о предоставлении лицензии взимается лицензионный сбор в размере 300 рублей.

За предоставление лицензии взимается лицензионный сбор в размере 1000 рублей.

Суммы указанных в настоящей статье лицензионных сборов зачисляются в соответствующие бюджеты.

### Статья 16. Финансирование лицензирования

Финансирование лицензирования осуществляется в пределах средств, выделяемых из соответствующих бюджетов на содержание лицензирующих органов.

### Статья 17. Перечень видов деятельности, на осуществление которых требуются лицензии

1. В соответствии с настоящим Федеральным законом лицензированию подлежат следующие виды деятельности:

- разработка авиационной техники, в том числе авиационной техники двойного назначения;
- производство авиационной техники, в том числе авиационной техники двойного назначения;
- ремонт авиационной техники, в том числе авиационной техники двойного назначения;
- испытание авиационной техники, в том числе авиационной техники двойного назначения;
- деятельность по распространению шифровальных (криптографических) средств;
- деятельность по техническому обслуживанию шифровальных (криптографических) средств;

- предоставление услуг в области шифрования информации;
- разработка, производство шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных систем, телекоммуникационных систем;
- деятельность по выдаче сертификатов ключей электронных цифровых подписей, регистрации владельцев электронных цифровых подписей, оказанию услуг, связанных с использованием электронных цифровых подписей, и подтверждению подлинности электронных цифровых подписей;
- деятельность по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
- деятельность по разработке и (или) производству средств защиты конфиденциальной информации;
- деятельность по технической защите конфиденциальной информации;
- разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации, индивидуальными предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность;
- деятельность по изготовлению защищенной от подделок полиграфической продукции, в том числе бланков ценных бумаг, а также торговля указанной продукцией;
- разработка вооружения и военной техники;
- производство вооружения и военной техники;
- ремонт вооружения и военной техники;
- утилизация вооружения и военной техники;
- торговля вооружением и военной техникой;
- производство оружия и основных частей огнестрельного оружия;
- производство патронов к оружию и составных частей патронов;
- торговля оружием и основными частями огнестрельного оружия;
- торговля патронами к оружию;

- экспонирование оружия, основных частей огнестрельного оружия, патронов к оружию;
- коллекционирование оружия, основных частей огнестрельного оружия, патронов к оружию;
- разработка и производство боеприпасов;
- утилизация боеприпасов;
- выполнение работ и оказание услуг по хранению, перевозкам и уничтожению химического оружия;
- эксплуатация взрывоопасных производственных объектов;
- эксплуатация пожароопасных производственных объектов;
- эксплуатация химически опасных производственных объектов;
- эксплуатация магистрального трубопроводного транспорта;
- эксплуатация нефтегазодобывающих производств;
- переработка нефти, газа и продуктов их переработки;
- транспортировка по магистральным трубопроводам нефти, газа и продуктов их переработки;
- хранение нефти, газа и продуктов их переработки;
- деятельность по проведению экспертизы промышленной безопасности;
- производство взрывчатых материалов промышленного назначения;
- хранение взрывчатых материалов промышленного назначения;
- применение взрывчатых материалов промышленного назначения;
- деятельность по распространению взрывчатых материалов промышленного назначения;
- производство пиротехнических изделий;
- деятельность по распространению пиротехнических изделий IV и V класса в соответствии с государственным стандартом;
- деятельность по предупреждению и тушению пожаров;
- производство работ по монтажу, ремонту и обслуживанию средств обеспечения пожарной безопасности зданий и сооружений;
- деятельность по эксплуатации электрических сетей (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);

- деятельность по эксплуатации газовых сетей;
- деятельность по эксплуатации тепловых сетей (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
- проектирование зданий и сооружений I и II уровней ответственности в соответствии с государственным стандартом;
- строительство зданий и сооружений I и II уровней ответственности в соответствии с государственным стандартом;
- инженерные изыскания для строительства зданий и сооружений I и II уровней ответственности в соответствии с государственным стандартом;
- производство маркшейдерских работ;
- деятельность по реставрации объектов культурного наследия (памятников истории и культуры);
- геодезическая деятельность;
- картографическая деятельность;
- выполнение работ по активному воздействию на гидрометеорологические процессы и явления;
- выполнение работ по активному воздействию на геофизические процессы и явления;
- деятельность в области гидрометеорологии и смежных с ней областях;
- фармацевтическая деятельность;
- производство лекарственных средств;
- производство медицинской техники;
- деятельность по распространению лекарственных средств и изделий медицинского назначения;
- техническое обслуживание медицинской техники (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
- деятельность по оказанию протезно-ортопедической помощи;
- культивирование растений, используемых для производства наркотических средств и психотропных веществ;

- деятельность, связанная с оборотом наркотических средств и психотропных веществ (разработка, производство, изготовление, переработка, хранение, перевозки, отпуск, реализация, распределение, приобретение, использование, уничтожение), внесенных в Список II в соответствии с Федеральным законом «О наркотических средствах и психотропных веществах»;
- деятельность, связанная с оборотом психотропных веществ (разработка, производство, изготовление, переработка, хранение, перевозки, отпуск, реализация, распределение, приобретение, использование, уничтожение), внесенных в Список III в соответствии с Федеральным законом «О наркотических средствах и психотропных веществах»;
- деятельность, связанная с использованием возбудителей инфекционных заболеваний;
- производство дезинфекционных, дезинсекционных и дератизационных средств;
- перевозки морским транспортом пассажиров;
- перевозки морским транспортом грузов;
- перевозки внутренним водным транспортом пассажиров;
- перевозки внутренним водным транспортом грузов;
- перевозки воздушным транспортом пассажиров;
- перевозки воздушным транспортом грузов;
- перевозки пассажиров автомобильным транспортом, оборудованным для перевозок более 8 человек (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
- перевозки пассажиров на коммерческой основе легковым автомобильным транспортом;
- перевозки грузов автомобильным транспортом грузоподъемностью свыше 3,5 тонны (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
- сюрвейерское обслуживание морских судов в морских портах;
- погрузочно-разгрузочная деятельность на внутреннем водном транспорте;
- погрузочно-разгрузочная деятельность в морских портах;

- погрузочно-разгрузочная деятельность на железнодорожном транспорте;
- деятельность по осуществлению буксировок морским транспортом (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
- деятельность по техническому обслуживанию воздушного движения;
- деятельность по техническому обслуживанию воздушных судов;
- деятельность по ремонту воздушных судов;
- деятельность по применению авиации в отраслях экономики;
- деятельность по техническому обслуживанию и ремонту подвижного состава на железнодорожном транспорте;
- деятельность по техническому обслуживанию и ремонту технических средств, используемых на железнодорожном транспорте;
- деятельность по обращению с опасными отходами;
- организация и содержание тотализаторов и игорных заведений;
- оценочная деятельность;
- туроператорская деятельность;
- турагентская деятельность;
- деятельность по продаже прав на клубный отдых;
- негосударственная (частная) охранная деятельность;
- негосударственная (частная) сыскная деятельность;
- заготовка, переработка и реализация лома цветных металлов;
- заготовка, переработка и реализация лома черных металлов;
- деятельность, связанная с трудоустройством граждан РФ за пределами РФ;
- деятельность по разведению племенных животных (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
- деятельность по производству и использованию племенной продукции (материала) (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);

- публичный показ аудиовизуальных произведений, если указанная деятельность осуществляется в кинозале;
- воспроизведение (изготовление экземпляров) аудиовизуальных произведений и фонограмм на любых видах носителей;
- аудиторская деятельность;
- деятельность инвестиционных фондов;
- деятельность по управлению инвестиционными фондами, паевыми инвестиционными фондами и негосударственными пенсионными фондами;
- деятельность специализированных депозитариев инвестиционных фондов, паевых инвестиционных фондов и негосударственных пенсионных фондов;
- деятельность негосударственных пенсионных фондов по пенсионному обеспечению и пенсионному страхованию;
- деятельность по производству элитных семян (семян элиты);
- производство табачных изделий;
- деятельность по изготовлению и ремонту средств измерений;
- осуществляемая в море деятельность по приемке и транспортировке уловов водных биологических ресурсов, включая рыб, а также других водных животных и растений;
- деятельность по хранению зерна и продуктов его переработки;
- космическая деятельность;
- ветеринарная деятельность;
- медицинская деятельность;
- деятельность арбитражных управляющих.

*Согласно* п. 4 ст. 18 настоящего Федерального закона *лицензирование деятельности арбитражных управляющих прекращается с 1 июля 2002 г.:*

- перевозка пассажиров и багажа железнодорожным транспортом;
- перевозка грузов железнодорожным транспортом;
- перевозка грузобагажа железнодорожным транспортом;
- деятельность по предоставлению инфраструктуры железнодорожного транспорта общего пользования для осуществления перевозок;
- транспортировка грузов (перемещение грузов без заключения договора перевозки) по железнодорожным путям общего пользования,

за исключением уборки прибывших грузов с железнодорожных выставочных путей, возврата их на железнодорожные выставочные пути;

- деятельность по продаже электрической энергии гражданам.

2. Перечень работ и услуг по космической деятельности, ветеринарной деятельности и медицинской деятельности устанавливается положениями о лицензировании указанных видов деятельности.

3. Введение лицензирования иных видов деятельности возможно только путем внесения дополнений в предусмотренный настоящим Федеральным законом перечень видов деятельности, на осуществление которых требуются лицензии.

### Статья 18. Переходные положения

1. Федеральные законы и иные нормативные правовые акты, регулирующие порядок лицензирования отдельных видов деятельности, за исключением видов деятельности, предусмотренных п. 2 ст. 1 настоящего Федерального закона, действуют в части, не противоречащей настоящему Федеральному закону, и подлежат приведению в соответствие с настоящим Федеральным законом.

2. Лицензирование видов деятельности, не указанных в п. 1 ст. 17 настоящего Федерального закона, прекращается со дня вступления в силу настоящего Федерального закона.

3. Федеральные авиационные правила лицензирования деятельности в области гражданской авиации действуют до момента вступления в силу федерального закона о внесении соответствующих изменений в Воздушный кодекс РФ.

4. Лицензирование деятельности арбитражных управляющих прекращается с 1 июля 2002 г.

### Статья 19. Признание утратившими силу некоторых законодательных актов в связи с принятием настоящего Федерального закона

Со дня вступления в силу настоящего Федерального закона признать утратившими силу:

- Федеральный закон от 25 сентября 1998 г. № 158-ФЗ «О лицензировании отдельных видов деятельности» (Собрание законодательства РФ, 1998, №39, ст. 4857);

- Федеральный закон от 26 ноября 1998 года № 178-ФЗ «О внесении дополнений» в Федеральный закон «О лицензировании отдельных видов деятельности» (Собрание законодательства РФ, 1998, № 48, ст. 5853);
- Федеральный закон от 22 декабря 1999 года № 215-ФЗ «О внесении дополнений» в ст. 17 Федерального закона «О лицензировании отдельных видов деятельности» (Собрание законодательства РФ, 1999, № 52, ст. 6365);
- Федеральный закон от 22 декабря 1999 года № 216-ФЗ «О внесении дополнения в ст. 17 Федерального закона «О лицензировании отдельных видов деятельности» (Собрание законодательства РФ, 1999, № 52, ст. 6366);
- Федеральный закон от 12 мая 2000 года № 69-ФЗ «О внесении изменения» в ст. 17 Федерального закона «О лицензировании отдельных видов деятельности» (Собрание законодательства РФ, 2000, № 20, ст. 2104);
- статью 2 Федерального закона от 29 декабря 2000 г. № 169-ФЗ «О внесении изменений и дополнений в Федеральный закон «Об отходах производства и потребления» и Федеральный закон «О лицензировании отдельных видов деятельности» (Собрание законодательства РФ, 2001, № 1, ст. 21).

### Статья 20. Вступление в силу настоящего Федерального закона

Настоящий Федеральный закон вступает в силу по истечении шести месяцев со дня его официального опубликования.

Президенту РФ и Правительству РФ привести свои нормативные правовые акты в соответствие с настоящим Федеральным законом.

*Президент РФ*
*В. Путин*
*Москва*
*8 августа 2001 г.*
*№ 128-ФЗ*

## Приложение 9

# ФЕДЕРАЛЬНЫЙ ЗАКОН «О КОММЕРЧЕСКОЙ ТАЙНЕ»

от 29 июля 2004 г. № 98-ФЗ
Принят Государственной Думой 9 июля 2004 г.
Одобрен Советом Федерации 15 июля 2004 г.

### Статья 1. Цели и сфера действия настоящего Федерального закона

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

2. Положения настоящего Федерального закона распространяются на информацию, составляющую коммерческую тайну, независимо от вида носителя, на котором она зафиксирована.

3. Положения настоящего Федерального закона не распространяются на сведения, отнесенные в установленном порядке к государственной тайне, в отношении которой применяются положения законодательства РФ о государственной тайне.

### Статья 2. Законодательство Российской Федерации о коммерческой тайне

Законодательство РФ о коммерческой тайне состоит из Гражданского кодекса РФ, настоящего Федерального закона, других федеральных законов.

### Статья 3. Основные понятия, используемые в настоящем Федеральном законе

Для целей настоящего Федерального закона используются следующие основные понятия:

**1) коммерческая тайна** - конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходом, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду;

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

3) **режим коммерческой тайны** - правовые, организационные, технические и иные принимаемые обладателем информации, составляющей коммерческую тайну, меры по охране ее конфиденциальности;

4) **обладатель информации, составляющей коммерческую тайну,** - лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании, ограничило доступ к этой информации и установило в отношении ее режим коммерческой тайны;

5) **доступ к информации, составляющей коммерческую тайну,** ознакомление определенных лиц с информацией, составляющей коммерческую тайну, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации;

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

7) **контрагент** - сторона гражданско-правового договора, которой обладатель информации, составляющей коммерческую тайну, передал эту информацию;

8) **предоставление информации, составляющей коммерческую тайну,** - передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем органам государственной власти, иным государственным органам, органам местного самоуправления в целях выполнения их функций;

9) **разглашение информации, составляющей коммерческую тайну,** - действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических

средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.

### Статья 4. Право на отнесение информации к информации, составляющей коммерческую тайну, и способы получения такой информации

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

2. Информация, самостоятельно полученная лицом при осуществлении исследований, систематических наблюдений или иной деятельности, считается полученной законным способом несмотря на то, что содержание указанной информации может совпадать с содержанием информации, составляющей коммерческую тайну, обладателем которой является другое лицо.

3. Информация, составляющая коммерческую тайну, полученная от ее обладателя на основании договора или другом законном основании, считается полученной законным способом.

4. Информация, составляющая коммерческую тайну, обладателем которой является другое лицо, считается полученной незаконно, если ее получение осуществлялось с умышленным преодолением принятых обладателем информации, составляющей коммерческую тайну, мер по охране конфиденциальности этой информации, а также если получающее эту информацию лицо знало или имело достаточные основания полагать, что эта информация составляет коммерческую тайну, обладателем которой является другое лицо, и что осуществляющее передачу этой информации лицо не имеет на передачу этой информации законного основания.

### Статья 5. Сведения, которые не могут составлять коммерческую тайну

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

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

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

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

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

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

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

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

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

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

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

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

### Статья 6. Предоставление информации, составляющей коммерческую тайну

1. Обладатель информации, составляющей коммерческую тайну, по мотивированному требованию органа государственной власти, иного государственного органа, органа местного самоуправления предоставляет им на безвозмездной основе информацию, составляющую коммерческую

тайну. Мотивированное требование должно быть подписано уполномоченным должностным лицом, содержать указание цели и правового основания затребования информации, составляющей коммерческую тайну, и срок предоставления этой информации, если иное не установлено федеральными законами.

2. В случае отказа обладателя информации, составляющей коммерческую тайну, предоставить ее органу государственной власти, иному государственному органу, органу местного самоуправления данные органы вправе затребовать эту информацию в судебном порядке.

3. Обладатель информации, составляющей коммерческую тайну, а также органы государственной власти, иные государственные органы, органы местного самоуправления, получившие такую информацию в соответствии с частью 1 настоящей статьи, обязаны предоставить эту информацию по запросу судов, органов прокуратуры, органов предварительного следствия, органов дознания по делам, находящимся в их производстве, в порядке и на основаниях, которые предусмотрены законодательством РФ.

4. На документах, предоставляемых указанным в ч. 1 и 3 настоящей статьи органам и содержащих информацию, составляющую коммерческую тайну, должен быть нанесен гриф «Коммерческая тайна» с указанием ее обладателя (для юридических лиц - полное наименование и место нахождения, для индивидуальных предпринимателей - фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

## Статья 7. Права обладателя информации, составляющей коммерческую тайну

1. Права обладателя информации, составляющей коммерческую тайну, возникают с момента установления им в отношении такой информации режима коммерческой тайны в соответствии со ст. 10 настоящего Федерального закона.

2. Обладатель информации, составляющей коммерческую тайну, имеет право:

1) устанавливать, изменять и отменять в письменной форме режим коммерческой тайны в соответствии с настоящим Федеральным законом и гражданско-правовым договором;

2) использовать информацию, составляющую коммерческую тайну, для собственных нужд в порядке, не противоречащем законодательству РФ;

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

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

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

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

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

## Статья 8. Обладатель информации, составляющей коммерческую тайну, полученной в рамках трудовых отношений

1. Обладателем информации, составляющей коммерческую тайну, полученной в рамках трудовых отношений, является работодатель.

2. В случае получения работником в связи с выполнением своих трудовых обязанностей или конкретного задания работодателя результата, способного к правовой охране в качестве изобретения, полезной модели, промышленного образца, топологии интегральной микросхемы, программы для электронных вычислительных машин или базы данных, отношения между работником и работодателем регулируются в соответствии с законодательством РФ об интеллектуальной собственности.

## Статья 9. Порядок установления режима коммерческой тайны при выполнении государственного контракта для государственных нужд

Государственным контрактом на выполнение научно-исследовательских, опытно-конструкторских, технологических или иных работ для федеральных государственных нужд или нужд субъекта РФ должен быть определен объем сведений, признаваемых конфиденциальными, а также должны быть урегулированы вопросы, касающиеся установления в отношении полученной информации режима коммерческой тайны.

## Статья 10. Охрана конфиденциальности информации

1. Меры по охране конфиденциальности информации, принимаемые ее обладателем, должны включать в себя:

1) определение перечня информации, составляющей коммерческую тайну;

2) ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;

3) учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;

4) регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;

5) нанесение на материальные носители (документы), содержащие информацию, составляющую коммерческую тайну, грифа «Коммерческая тайна» с указанием обладателя этой информации (для юридических лиц - полное наименование и место нахождения, для индивидуальных предпринимателей - фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

2. Режим коммерческой тайны считается установленным после принятия обладателем информации, составляющей коммерческую тайну, мер, указанных в части 1 настоящей статьи.

3. Индивидуальный предприниматель, являющийся обладателем информации, составляющей коммерческую тайну, и не имеющий работников, с которыми заключены трудовые договоры, принимает меры по охране конфиденциальности информации, указанные в части 1 настоящей статьи, за исключением пп. 1 и 2, а также положений п. 4, касающихся регулирования трудовых отношений.

4. Наряду с мерами, указанными в части 1 настоящей статьи, обладатель информации, составляющей коммерческую тайну, вправе применять при необходимости средства и методы технической защиты конфиденциальности этой информации, другие не противоречащие законодательству РФ меры.

5. Меры по охране конфиденциальности информации признаются разумно достаточными, если:

1) исключается доступ к информации, составляющей коммерческую тайну, любых лиц без согласия ее обладателя;

2) обеспечивается возможность использования информации, составляющей коммерческую тайну, работниками и передачи ее контрагентам без нарушения режима коммерческой тайны.

6. Режим коммерческой тайны не может быть использован в целях, противоречащих требованиям защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

## Статья 11. Охрана конфиденциальности информации в рамках трудовых отношений

1. В целях охраны конфиденциальности информации работодатель обязан:

1) ознакомить под расписку работника, доступ которого к информации, составляющей коммерческую тайну, необходим для выполнения им своих трудовых обязанностей, с перечнем информации, составляющей коммерческую тайну, обладателями которой является работодатель и его контрагенты;

2) ознакомить под расписку работника с установленным работодателем режимом коммерческой тайны и с мерами ответственности за его нарушение;

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

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

3. В целях охраны конфиденциальности информации работник обязан:

1) выполнять установленный работодателем режим коммерческой тайны;

2) не разглашать информацию, составляющую коммерческую тайну, обладателями которой являются работодатель и его контрагенты, и без их согласия не использовать эту информацию в личных целях;

3) не разглашать информацию, составляющую коммерческую тайну, обладателями которой являются работодатель и его контрагенты, после прекращения трудового договора в течение срока, предусмотренного соглашением между работником и работодателем, заключенным в период срока действия трудового договора, или в течение трех лет после прекращения трудового договора, если указанное соглашение не заключалось;

4) возместить причиненный работодателю ущерб, если работник виновен в разглашении информации, составляющей коммерческую тайну, ставшей ему известной в связи с исполнением им трудовых обязанностей;

5) передать работодателю при прекращении или расторжении трудового договора имеющиеся в пользовании работника материальные носители информации, содержащие информацию, составляющую коммерческую тайну.

4. Работодатель вправе потребовать возмещения причиненных убытков лицом, прекратившим с ним трудовые отношения, в случае, если это лицо виновно в разглашении информации, составляющей коммерческую тайну, доступ к которой это лицо получило в связи с исполнением им трудовых обязанностей, если разглашение такой информации последовало в течение срока, установленного в соответствии с п. 3 ч. 3 настоящей статьи.

5. Причиненные ущерб либо убытки не возмещаются работником или прекратившим трудовые отношения лицом, если разглашение информации, составляющей коммерческую тайну, явилось следствием непреодолимой силы, крайней необходимости или неисполнения работодателем обязанности по обеспечению режима коммерческой тайны.

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

7. Руководитель организации возмещает организации убытки, причиненные его виновными действиями в связи с нарушением законодательства РФ о коммерческой тайне. При этом убытки определяются в соответствии с гражданским законодательством.

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

## Статья 12. Охрана конфиденциальности информации в рамках гражданско-правовых отношений

1. Отношения между обладателем информации, составляющей коммерческую тайну, и его контрагентом в части, касающейся охраны конфиденциальности информации, регулируются законом и договором.

2. В договоре должны быть определены условия охраны конфиденциальности информации, в том числе в случае реорганизации или ликвидации одной из сторон договора в соответствии с гражданским законодательством, а также обязанность контрагента по возмещению убытков при разглашении им этой информации вопреки договору.

3. В случае, если иное не установлено договором между обладателем информации, составляющей коммерческую тайну, и контрагентом, контрагент в соответствии с законодательством РФ самостоятельно определяет способы защиты информации, составляющей коммерческую тайну, переданной ему по договору.

4. Контрагент обязан незамедлительно сообщить обладателю информации, составляющей коммерческую тайну, о допущенном контрагентом либо ставшем ему известном факте разглашения или угрозы разглашения, незаконном получении или незаконном использовании информации, составляющей коммерческую тайну, третьими лицами.

5. Обладатель информации, составляющей коммерческую тайну, переданной им контрагенту, до окончания срока действия договора не может разглашать информацию, составляющую коммерческую тайну, а также в одностороннем порядке прекращать охрану ее конфиденциальности, если иное не установлено договором.

6. Сторона, не обеспечившая в соответствии с условиями договора охраны конфиденциальности информации, переданной по договору, обязана возместить другой стороне убытки, если иное не предусмотрено договором.

### Статья 13. Охрана конфиденциальности информации при ее предоставлении

1. Органы государственной власти, иные государственные органы, органы местного самоуправления в соответствии с настоящим Федеральным законом и иными федеральными законами обязаны создать условия, обеспечивающие охрану конфиденциальности информации, предоставленной им юридическими лицами или индивидуальными предпринимателями.

2. Должностные лица органов государственной власти, иных государственных органов, органов местного самоуправления, государственные или муниципальные служащие указанных органов без согласия обладателя информации, составляющей коммерческую тайну, не вправе разглашать или передавать другим лицам, органам государственной власти, иным государственным органам, органам местного самоуправления ставшую известной им в силу выполнения должностных (служебных) обязанностей информацию, составляющую коммерческую тайну, за исключением случаев, предусмотренных настоящим Федеральным законом, а также не вправе использовать эту информацию в корыстных или иных личных целях.

3. В случае нарушения конфиденциальности информации должностными лицами органов государственной власти, иных государственных органов, органов местного самоуправления, государственными и муниципальными служащими указанных органов эти лица несут ответственность в соответствии с законодательством РФ.

### Статья 14. Ответственность за нарушение настоящего Федерального закона

1. Нарушение настоящего Федерального закона влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством РФ.

2. Работник, который в связи с исполнением трудовых обязанностей, получил доступ к информации, составляющей коммерческую тайну, обладателями которой являются работодатель и его контрагенты, в случае

умышленного или неосторожного разглашения этой информации при отсутствии в действиях такого работника состава преступления несет дисциплинарную ответственность в соответствии с законодательством РФ.

*Согласно* ГК РФ *работники, разгласившие служебную или коммерческую тайну вопреки трудовому договору, обязаны возместить причиненные убытки.*

3. Органы государственной власти, иные государственные органы, органы местного самоуправления, получившие доступ к информации, составляющей коммерческую тайну, несут перед обладателем информации, составляющей коммерческую тайну, гражданско-правовую ответственность за разглашение или незаконное использование этой информации их должностными лицами, государственными или муниципальными служащими указанных органов, которым она стала известна в связи с выполнением ими должностных (служебных) обязанностей.

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

5. По требованию обладателя информации, составляющей коммерческую тайну, лицо, указанное в части 4 настоящей статьи, обязано принять меры по охране конфиденциальности информации. При отказе такого лица принять указанные меры обладатель информации, составляющей коммерческую тайну, вправе требовать в судебном порядке защиты своих прав.

### Статья 15. Ответственность за непредоставление органам государственной власти, иным государственным органам, органам местного самоуправления информации, составляющей коммерческую тайну

Невыполнение обладателем информации, составляющей коммерческую тайну, законных требований органов государственной власти, иных государственных органов, органов местного самоуправления о предоставлении им информации, составляющей коммерческую тайну, а равно воспрепятствование получению должностными лицами этих органов указанной информации влечет за собой ответственность в соответствии с законодательством РФ.

### Статья 16. Переходные положения

Грифы, нанесенные до вступления в силу настоящего Федерального закона на материальные носители и указывающие на содержание в них информации, составляющей коммерческую тайну, сохраняют свое действие при условии, если меры по охране конфиденциальности указанной информации будут приведены в соответствие с требованиями настоящего Федерального закона.

*Президент РФ*
*В. Путин*
*Москва, Кремль*
*29 июля 2004 г.*
*№ 98-ФЗ*

# Приложение 10

# ГЛОССАРИЙ

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Автор | Физическое лицо, творческим трудом которого создано произведение | *Закон РФ от 09.17.93 №5351-1 «Об авторском праве и смежных правах», ст. 4* |
| Автор аудиовизуального произведения | Режиссер-постановщик; автор сценария (сценарист); автор музыкального произведения (с текстом или текста), специально созданного для этого аудиовизуального произведения (композитор) | *Закон РФ от 09.07.93 №5351-1 «Об авторском праве и смежных правах», ст. 13* |
| Автор изобретения, полезной модели, промышленного образца | Физическое лицо, творческим трудом которого они созданы | *Закон РФ от 33.09.92 №3517-1 «Патентный закон Российской Федерации», ст. 7* |
| Автор программы для ЭВМ или базы данных | Физическое лицо, в результате творческой деятельности которого они созданы | *Закон РФ от 23.09.92 №3523-1 «О правовой охране программ для электронных вычислительных машин и баз данных», ст. 8* |
| Автор топологии | Физическое лицо, в результате творческой деятельности которого эта топология была создана | *Закон РФ от 23.09.92 №3326-1 «О правовой охране топологий интегральных микросхем», ст. 4* \ |
| Авторское право | Авторское право - совокупность правовых норм, регулирующих отношения, возникающие в связи с созданием и использованием произведений науки, литературы и искусства. | *Закон РФ от 09.07.93 №3331-1 «Об авторском праве и смежных правах»* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| | Авторское право распространяется на произведения науки, литературы и искусства, являющиеся результатом творческой деятельности, независимо от назначения и достоинства произведения, а также от способа его выражения. Авторское право не распространяется на идеи, методы, процессы, системы, способы, концепции, принципы, открытия, факты. *Примечание.* Объекты авторского права - литературные произведения (включая программы для ЭВМ); драматические и музыкально-драматические произведения, сценарные произведения; хореографические произведения и пантомимы; музыкальные произведения с текстом или без текста; аудиовизуальные произведения (кино-, теле- и видеофильмы, слайдфильмы, диафильмы и другие кино- и телепроизведения); произведения живописи, скульптуры, графики, дизайна, графические рассказы, комиксы и другие произведения изобразительного искусства, произведения декоративно-прикладного и сценографического искусства; произведения архитектуры, градостроительства и садово-паркового искусства; фотографические произведения и произведения, полученные способами, аналогичными фотографии; географические, геологические и другие карты, планы, эскизы и пластические произведения, относящиеся к географии, топографии и к другим наукам; производные произведения (переводы, обработки, аннотации, рефераты, резюме, обзоры, инсценировки, аранжи- | |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| | ровки и другие переработки произведений науки, литературы и искусства); сборники (энциклопедии, антологии, базы данных) и другие составные произведения, представляющие собой по подбору или расположению материалов результат творческого труда; другие произведения.<br>Не являются объектами авторского права: официальные документы (законы, судебные решения, иные тексты законодательного, административного и судебного характера), а также их официальные переводы; государственные символы и знаки (флаги, гербы, ордена, денежные знаки и иные государственные символы и знаки); произведения народного творчества; сообщения о событиях и фактах, имеющие информационный характер | |
| Адаптация программы для ЭВМ или базы данных | Это внесение изменений, осуществляемых исключительно в целях обеспечения функционирования программы для ЭВМ или базы данных на конкретных технических средствах пользователя или под управлением конкретных программ пользователя | *Закон РФ от 23.09.92 №3323-1 «О правовой охране программ для электронных вы числительных машин и баз данных»* |
| Адресные данные пользователей услуг почтовой связи | Информация о гражданах (фамилия, имя, отчество, почтовый адрес), а также о других пользователях услуг почтовой связи (наименование и почтовый адрес) | *Федеральный закон от 17.07.99 №176-ФЗ «О почтовой связи», ст. 2* |
| Архив | Совокупность архивных документов, а также архивное учреждение или структурное подразделение учреждения, организации или предприятия, осуществляющее прием и хранение архивных документов в интересах пользователей | *Основы законодательства РФ об Архивном фонде РФ и архивах от 07.0793 №5341-1, ст. 1* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Архивное дело | Деятельность по организации хранения, учета и использования архивных документов | *Основы законодательства РФ об Архивном фонде РФ и архивах от 07.07.93 № 5341-1, ст. 1* |
| Архивный документ | Документ, сохраняемый или подлежащий сохранению в силу его значимости для общества, а равно имеющий ценность для собственника | *Основы законодательства РФ об Архивном фонде РФ и архивах от 07.07.93 № 5341-1, ст. 1* |
| Архивный фонд РФ | Совокупность документов, отражающих материальную и духовную жизнь ее народов, имеющих историческое, научное, социальное экономическое, политическое или культурное значение и являющихся неотъемлемой частью историко-культурного наследия народов РФ | *Основы законодательства РФ об Архивном фонде РФ и архивах от 07.07.93 № 5341-1, ст. 1* |
| Аудиовизуальное произведение | Произведение, состоящее из зафиксированной серии связанных между собой кадров (с сопровождением или без сопровождения их звуком) предназначенное для зрительного и слухового (в случае сопровождения звуком) восприятия с помощью соответствующих технических устройств; аудиовизуальные произведения включают кинематографические произведения и все произведения, выраженные средствами аналогичными кинематографическим (теле- и видеофильмы, диафильмы и слайд-фильмы и тому подобные произведения), независимо от способа их первоначальной или последующей фиксации | *Закон РФ от 09.07.93 №5351-1 «Об авторском праве и смежных правах, ст. 4* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Аутентификация | Проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности | *Сборник руководящих документов по защите информации от несанкционированного доступа Государственной технической комиссии при Президенте РФ, 1998 г.* |
| База данных | Объективная форма представления и организации совокупности данных (например: статей, расчетов), систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны с помощью ЭВМ | *Закон РФ от 23.09.92 №3523-1 «О правовой охране программ для электронных вычислительных машин и баз данных», ст. 1* |
| База данных | Объективная форма представления и организации совокупности данных (статей, расчетов и так далее), систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны с помощью электронной вычислительной машины (ЭВМ) | *Закон РФ от 09.07.93 №5351-1 «Об авторском праве и смежных правах», ст. 4* |
| База данных | Совокупность организованных взаимосвязанных данных на машиночитаемых носителях | *Временное положение о государственном учете и регистрации баз и банков данных», утвержденное постановлением правительства РФ от 28.02.96 № 226, п. 2* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Банковская тайна | Кредитная организация. Банк России гарантируют тайну об операциях, о счетах и вкладах своих клиентов и корреспондентов. Все служащие кредитной организации обязаны хранить тайну об операциях, счетах и вкладах ее клиентов и корреспондентов, а также об иных сведениях, устанавливаемых кредитной организацией, если это не противоречит федеральному закону | *Закон РСФСР от 02.12.90 №395-1 «О зачете прав потребителей», ст. 26 (в ред. Федерального закона от 03.02.96 М17-ФЗ, ст. 1)* |
| Банк гарантирует тайну | Банковского счета и банковского вклада, операций по счету и сведений о клиенте | *Гражданский кодекс РФ от 26.01. 96 № 14-ФЗ, ст. 857* |
| Безопасность | Состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз | *Закон РФ от 05.03.92 №2446-1 «О безопасности», ст. 1; Федеральная программа РФ по усилению борьбы с преступностью па 1994-1995 гг., утвержденная Указом Президента РФ от 24.05.94 №1016* |
| Библиотека | Информационное, культурное, образовательное учреждение, располагающее организованным фондом тиражированных документов и предоставляющее их во временное пользование физическим и юридическим лицам; библиотека может быть самостоятельным учреждением или структурным подразделением предприятия, учреждения, организации | *Федеральный закон от 29.12.94 № 78-ФЗ «О библиотечном деле», ст. 1* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Ведомственные сети связи | Сети электросвязи министерств и иных федеральных органов исполнительной власти, создаваемые для удовлетворения производственных и специальных нужд, имеющие выход на сеть связи общего пользования | *Федеральный закон от 16.02.95 № 15-ФЗ «О связи», ст. 2* |
| Верификация | Процесс сравнения двух уровней спецификации средств вычислительной техники или автоматизированных систем на надлежащее соответствие | *Сборник руководящих документов по защите информации от несанкционированного доступа Государственной технической комиссии при Президенте РФ, 1998 г.* |
| Владелец сертификата ключа подписи | Физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы | *Федеральный закон РФ от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи»* |
| Владелец информации | Субъект, осуществляющий владение и пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации | *ГОСТ Р 50922-96. Защита информации. Основные термины и определения. (Прил. А)* |
| Владелец информационных ресурсов, информационных систем, технологий и средств их обеспечения | Субъект, осуществляющий владение и пользование указанными объектами и реализующий полномочия распоряжения в пределах, установленных законом | *Федеральный закон от 20.02.95 № 24-ФЗ «Об информации, информатизации и защите информации», ст. 2* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Войска Федерального агентства правительственной связи и информации при Президенте РФ | Войска правительственной связи, части радиоразведки и инженерно-строительные части, которые создаются, содержатся и используются, в том числе за пределами РФ, в соответствии с законодательством РФ | *Закон РФ от 19.02.93 №4524-1 «О федеральных органах правительственной связи и информации», ст. 8* |
| Воспроизведение программы для ЭВМ или базы данных | Это изготовление одного или более экземпляров программы для ЭВМ или базы данных в любой материальной форме, а также их запись в память ЭВМ | *Закон РФ от 23.09.92 №3523-1 «О правовой охране программ для электронных вычислительных машин и баз данных»* |
| Воспроизведение произведения | Изготовление одного или более экземпляров произведения или его части в любой материальной форме, в том числе в форме звуко- и видеозаписи, изготовление в трех измерениях одного или более экземпляров двухмерного произведения и в двух измерениях - одного или более экземпляров трехмерного произведения; запись произведения в память ЭВМ также является воспроизведением | *Закон РФ от 09.07.93 №5351-1 «Об авторском праве и смежных правах», ст. 4* |
| Воспроизведение фонограммы | Изготовление одного или более экземпляров фонограммы или ее части на любом материальном носителе | *Закон РФ от 09.07.93 №5351-1 «Об авторском праве и смежных правах», ст. 4* |
| Выпуск в свет (опубликование) программы для ЭВМ или базы данных | Это предоставление экземпляров программы для ЭВМ или базы данных с согласия автора неопределенному кругу лиц (в том числе путем записи в память ЭВМ и выпуска печатного текста), при условии, что количество таких экземпляров должно удовлетворять потребности этого круга лиц, принимая во внимание характер указанных произведений | *Закон РФ от 23.09.92 №352 3-1 «О правовой охране программ для электронных вычислительных машин и баз данных», ст. 1* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Государственная база данных | База данных, созданная, приобретенная или накапливаемая за счет или с привлечением средств федерального бюджета | *Временное положение о государственном учете и регистрации баз и банков данных», утвержденное постановлением Правительства РФ от 28.02.96 № 226, п. 3* |
| Государственная измена | Шпионаж, выдача государственной тайны либо иное оказание помощи иностранному государству, иностранной организации или их представителям в проведении враждебной деятельности в ущерб внешней безопасности РФ | *Уголовный кодекс РФ от 13.06.96 № 63-ФЗ, ст. 275* |
| Государственная поддержка средств массовой информаци | Совокупность организационных, организационно-технических, правовых, экономических иных мер, устанавливаемых государством в целях обеспечения прав граждан на получение объективной информации, на свободу слова, а также в целях обеспечения независимости средств массовой информации | *Федеральный закон от 01.12.95 № 191-ФЗ «О государственной поддержке средств массовой информации и книгоиздания РФ», ст. 1* |
| Государственная тайна | Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ | *Закон РФ от 21.07.93 №5485-1 «О государственной тайне» вред. Федерального закона от 06.10.97 № 131-ФЗ, ст. 2* |
| Государственная техническая комиссия при Президенте РФ (Гостехкомиссия России) | Федеральный орган исполнительной власти, осуществляющий межотраслевую координацию и функциональное регулирование деятельности по обеспечению защиты (некриптографическими методами) информации, содержащей сведения, составляющие государ- | *Указ Президента РФ от 19.02.99 №212 «Вопросы Государст венной технической комиссии при Президенте Российской Федерации»* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| | ственную или служебную тайну, от ее утечки по техническим каналам, от несанкционированного доступа к ней, от специальных воздействий на информацию в целях ее уничтожения, искажения и блокирования и по противодействию техническим средствам разведки на территории РФ, а также единую государственную научно-техническую политику в области защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств.<br>*Примечание.* Гостехкомиссия России организует деятельность государственной системы защиты информации в РФ от технических разведок и от ее утечки по техническим каналам Гостехкомиссия России и региональные центры входят в состав государственных органов обеспечения безопасности РФ | |
| Государственная часть Архивного фонда РФ | Архивные фонды и архивные документы, являющиеся федеральной собственностью, государственной собственностью республик в составе РФ, краев, областей, автономной области, автономных округов, городов Москвы и Санкт-Петербурга и муниципальной собственностью | *Основы законодательства РФ об Архивном фонде РФ и архивах от 07.07.93 №5341-1. ст. 6* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Государственное региональное средство массовой информации | Средство массовой информации, учредителями которого выступают федеральные органы государственной власти совместно с органами государственной власти субъектов РФ либо только органы государственной власти субъектов РФ | *Федеральный закон от 13.01.95 № 7-ФЗ «О порядке освещения деятельности органов государственной власти в государственных средствах массовой информации», ст. 3* |
| Государственное федеральное средство массовой информации | Средство массовой информации, учредителем которого выступает федеральный орган государственной власти | *Федеральный закон от 13.01.95 № 7-ФЗ «О порядке освещения деятельности органов государственной власти в государственных средствах массовой информации», ст. 3* |
| Государственные органы обеспечения безопасности | Органы, предназначенные для непосредственного выполнения функций по обеспечению безопасности личности, общества и государства в системе исполнительной власти | *Закон РФ от 05.03.92 №2446-1 «О безопасности», ст. 4* |
| Гриф секретности | Реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него | *Закон РФ от 21.07.93 №5485-1 «О государственной тайне» в ред. Федерального закона от 06.10.97 № 131-ФЗ, ст. 2* |
| Декомпилирование программы для ЭВМ | Технический прием, включающий преобразование объектного кода в исходный текст в целях изучения структуры и кодирования программы для ЭВМ | *Закон РФ от 23.09 92 №3523-1 «О правовой охране программ для электронных вычислительных машин и баз данных», ст. 1* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Деятельность по поддержанию или восстановлению международного мира и безопасности с участием РФ | Операции по поддержанию мира и другие меры, предпринимаемые Советом Безопасности Организации Объединенных Наций в соответствии с Уставом ООН, региональными органами либо в рамках региональных органов или соглашений РФ, либо на основании двусторонних и многосторонних международных договоров РФ и не являющиеся согласно Уставу ООН принудительными действиями, а также международные принудительные действия с использованием вооруженных сил, осуществляемые по решению Совета Безопасности ООН, принятому в соответствии с Уставом ООН для устранения угрозы миру, нарушений мира или акта агрессии | *Федеральный закон от 23.06.95 № 93-ФЗ «О порядке предоставления Российской Федерацией военного и гражданского персонала для участия в деятельности по поддержанию или восстановлению международного мира и безопасности», ст. 2* |
| Документ | Материальный объект с зафиксированной на нем информацией в виде текста, звукозаписи или изображения, предназначенный для передачи во времени и пространстве в целях хранения и общественного использования. - см. Документированная информация (документ) | *Федеральный закон от 29.1.94 № 77-ФЗ «Об обязательном экземпляре документов», ст. 1; Федеральный закон от 29.12.94 №78-ФЗ «О библиотечном деле», ст. 1* |
| Документированная информация (документ) | Зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать | *Федеральный закон от 20.02.95 № 24-ФЗ «Об информации, информатизации и защите информации», ст. 2; Федеральный закон от 04.07.96 №85-ФЗ «Об участии в международном информационном обмене», ст. 2* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Документированная информация с ограниченным доступом | По условиям ее правового режима подразделяется на информацию, отнесенную к государственной тайне, и конфиденциальную. 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 потребностях 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 | *Федеральный закон от 20.02.95 № 24-ФЗ «Об информации, информатизации и займите информации», ст. 10* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Допуск к государственной тайне | Процедура оформления права граждан На доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций - на проведение работ с использованием таких сведений.<br>Примечание. Допуск должностных лиц и граждан к государственной тайне предусматривает: принятие на себя обязательств перед государством по нераспространению доверенных им сведений, составляющих государственную тайну; согласие на частичные, временные ограничения их прав в соответствии со статьей 24 Закона РФ от 21.07.93 № 5485-1 в редакции Федерального закона РФ от 06.10.97 № 131 -ФЗ «О государственной тайне», письменное согласие на проведение в отношении их полномочными органами проверочных мероприятий; определение видов, размеров и порядка предоставления льгот, предусмотренных Законом РФ от 21.07.93 № 5485-1 в редакции Федерального закона РФ от 06.10.97 № 131-ФЗ «О государственной тайне»; ознакомление с нормами законодательства РФ о государственной тайне, предусматривающими ответственность за его нарушение; принятие решения руководителем органа государственной власти, предприятия, учреждения или организации о допуске оформляемого лица к сведениям, составляющим государственную тайну. Льготы для должностных лиц и граждан, допущенных к государственной тайне на постоянной основе: процентные надбавки | *Закон РФ от 21.07.93 №5485-1 «О государственной тайне» вред. Федерального закона от 06.10.97 № 131-ФЗ, ст. 21* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| | к заработной плате в зависимости от степени секретности сведений, к которым они имеют доступ, преимущественное право при прочих равных условиях на оставление на работе при проведении органами государственной власти, предприятиями, учреждениями и организациями организационных и (или) штатных мероприятий. Для сотрудников структурных подразделений по защите государственной тайны дополнительно к льготам, установленным для должностных лиц и граждан, допущенных к государственной тайне на постоянной основе, устанавливается процентная надбавка к заработной плате за стаж работы в указанных структурных подразделениях. Устанавливаются три формы допуска к государственной тайне должностных лиц и граждан, соответствующие трем степеням секретности сведений, составляющих государственную тайну: сведения особой важности, совершенно секретные или секретные | |
| Доступ к информации | Ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации | *Сборник руководящих документов по защите информации от несанкционированного доступа Государственной технической комиссии при Президенте РФ, 1998 г.* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Доступ к информации | Получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств | *ГОСТ Р 50922-96. Защита информации. Основные термины и определения. (Прил. А)* |
| Доступ к сведениям, составляющим государственную тайну | Санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну | *Закон РФ от 21.07.93 №5485-1 «О государственной тайне» в ред. Федерального закона от 06.10.97 №131-ФЗ, ст. 2* |
| Доступность (санкционированная доступность) информации | Состояние информации, характеризуемое способностью технических средств и информационных технологий обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия | |
| Единая система федеральных органов правительственной связи и информации | Федеральное агентство правительственной связи и информации при Президенте РФ; органы правительственной связи и информации (центры правительственной связи, информационно-аналитические органы) в субъектах РФ; войска; учебные заведения, научно-исследовательские организации, предприятия | *Закон РФ от 19.02.93 № 4324-1 «О федеральных органах правительственной связи и информации», ст. 5* |
| Жизненно важные интересы | Совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства | *Закон РФ от 05.03.92 №2446-1 «О безопасности», ст. 1* |
| Запись [в области авторского права] | Фиксация звуков и (или) изображений с помощью технических средств в какой-либо материальной форме, позволяющей осуществлять их неоднократное восприятие, воспроизведение или сообщение | *Закон РФ от 09.07.93 №5351-1 «Об авторском праве и смежных правах», ст. 4* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Защита информации | Защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу.<br>*Примечание.* Защита информации имеет целью: 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 | *Федеральный закон от 20.02.95 № 24-ФЗ «Об информации, информатизации и защите информации», ст. 20, 21* |
| Защита информации от агентурной разведки | Деятельность по предотвращению получения защищаемой информации агентурной разведкой | *ГОСТ Р 50922-96. Защита информации. Основные термины и определения* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Защита информации от непреднамеренного воздействия | Деятельность по предотвращению воздействия на защищаемую информацию от ошибок пользователей информации, сбоев технических и программных средств информационных систем, а также природных явлений или иных нецеленаправленных на изменение информации воздействий, связанных с функционированием технических средств, систем или с деятельностью людей, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации | *ГОСТ Р 30922-96. «Защита информации. Основные термины и определения»* |
| Защита информации от несанкционированного воздействия | Деятельность по предотвращению воздействия на защищаемую информацию с нарушением установленных правил и правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации | *ГОСТ Р 50922-96. «Защита информации. Основные термины и определения»* |
| Защита информации от несанкционированного доступа | Деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации | *ГОСТ Р 50922-96. «Защита информации. Основные термины и определения»* |
| Защита информации от утечки | Деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения и несанкционированного доступа к защищаемой информации и от получения защищаемой информации (иностранными) разведками | *ГОСТ Р 50922-96. «Защита информации. Основные термины и определения»* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Защита информации от разглашения | Деятельность по предотвращению несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации | *ГОСТ Р 50922-96. «Защита информации. Основные термины и определения»* |
| Защита информации от (иностранной) разведки | Деятельность по предотвращению получения защищаемой информации (иностранной) разведкой | *ГОСТ Р 50922-96. «Защита информации. Основные термины и определения»* |
| Защита информации от (иностранной) технической разведки | Деятельность по предотвращению получения защищаемой информации (иностранной) технической разведкой с помощью технических средств | *ГОСТ Р 50922-96. «Защита информации. Основные термины и определения»* |
| Защита прав субъектов в сфере информационных процессов и информатизации | Осуществляется в целях предупреждения правонарушений, пресечения неправомерных действии, восстановления нарушенных прав и возмещения причиненного ущерба | *Федеральный закон от 20.02.95 № 24-ФЗ «Об информации, информатизации и защите информации», ст. 23* |
| Защищаемая информация | Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, установленными собственником информации | *ГОСТ Р 50922-96. «Защита информации. Основные термины и определения»* |
| Знак охраны авторского права | Помещается на каждом экземпляре произведения и состоит из трех элементов: латинской буквы «С» в окружности; имени (наименования) обладателя исключительных авторских прав; года первого опубликования произведения | *Закон РФ от 09.07.93 №5331-1 «Об авторском праве и смежных правах», ст. 9* |
| Знак охраны смежных прав | Помещается на каждом экземпляре фонограммы и (или) на каждом содержащем ее футляре и состоит из трех элементов: латинской буквы «Р» в окружности; имени (наименования) обладателя исключительных смежных прав; года первого опубликования фонограммы | *Закон РФ от 09.07.93 №5351-1 «Об авторском праве и смежных правах», ст. 36.* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Идентификатор доступа | Уникальный признак субъекта или объекта доступа | *Сборник руководящих документов по защите информации от несанкционированного доступа Государственной технической комиссии при Президенте РФ, 1998 г.* |
| Идентификация | Присвоение субъектам или объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов | *Сборник руководящих документов по защите информации от несанкционированного доступа Государственной технической комиссии при Президенте РФ, 1998 г.* |
| Изготовитель аудиовизуального произведения | Физическое или юридическое лицо, взявшее на себя инициативу и ответственность за изготовление такого произведения, при отсутствии доказательств иного изготовителем аудиовизуального произведения признается физическое или юридическое лицо, имя или наименование которого обозначено на этом произведении обычным образом | *Закон РФ от 09.07.93 №5351-1 «Об авторском праве и смежных правах», ст. 4* |
| Изготовитель фонограммы | Физическое или юридическое лицо, взявшее на себя инициативу и ответственность за первую звуковую запись исполнения или иных звуков, при отсутствии доказательств иного изготовителем фонограммы признается физическое или юридическое лицо, имя или наименование которого обозначено на этой фонограмме и(или) на содержащем ее футляре обычным образом | *Закон РФ от 09.07.93 №5351-1 «Об авторском праве и смежных правах», ст. 4* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Издатель | Издательство, иное учреждение, предприятие (предприниматель), осуществляющее материально-техническое обеспечение производства продукции средства массовой информации, а также приравненное к издателю юридическое лицо или гражданин, для которого эта деятельность не является основной либо не служит главным источником дохода | *Закон РФ от 27.12.91 №2124-1 «О средствах массовой информации», ст. 2* |
| Издательство | Предприятие государственной формы собственности или организация иной формы собственности, осуществляющие подготовку, производство и выпуск книжной и другой печатной продукции | *Федеральный закон от 01.12.95 № 191-ФЗ «О государственной поддержке средств массовой информации и книгоиздания Российской Федерации», ст. 1* |
| Интегральная микросхема | Это микроэлектронное изделие окончательной или промежуточной формы, предназначенное для выполнения функций электронной схемы, элементы и связи которого нераздельно сформированы в объеме и (или) на поверхности материала, на основе которого изготовлено изделие | *Закон РФ от 23.09.92 №3526-1 «О правовой охране топологии интегральных микросхем», ст. 1* |
| Интересы государства | Незыблемость конституционного строя, суверенитета и территориальной целостности России, политическая, экономическая и социальная» стабильность, безусловное обеспечение законности и поддержание правопорядка, развитие равноправного и взаимовыгодного международного сотрудничества | *Указ Президента РФ от 10 января 2000 г. № 24 «О концепции национальной безопасности»* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Интересы государства в информационной сфере | Создание условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества | *Доктрина информационной безопасности РФ, 2000 г.* |
| Интересы личности | Реализация конституционных прав и свобод, обеспечение личной безопасности, повышение качества и уровня жизни, физическое, духовное и интеллектуальное развитии человека и гражданина | *Указ Президента РФ от 10 января 2000 г. №24 «О концепции национальной безопасности»* |
| Интересы личности в информационной сфере | Реализация конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также защита информации, обеспечивающей личную безопасность | *Доктрина информационной безопасности РФ, 2000 г.* |
| Интересы общества | Упрочение демократии, создание правового, социального государства, достижение и поддержание общественного согласия, духовное обновление России | *Указ Президента РФ от 10 января 2000 г. №24 «О концепции национальной безопасности»* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Интересы общества в информационной сфере | Обеспечение интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении России | *Доктрина информационной безопасности РФ, 2000 г.* |
| 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 | *Федеральный закон от 20.02.95 № 24-ФЗ «Об информации, информатизации и защите информации», ст. 2* |
| Информационная безопасность | Состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства | *Федеральный закон от 04.07.96 № 85-ФЗ «Об участии в международном информационном обмене», ст. 2* |
| Информационная война | Особый вид отношений между государствами, при котором для разрешения существующих межгосударственных противоречий используются методы, средства и технологии силового воздействия на информационную сферу этих государств | *Концепция продвижения идеи формирования международной системы информационной безопасности. Проект, 1999 г.* |
| Информационная система | Организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы | *Федеральный закон от 20.02.95 №2-1-ФЗ«Об информации, информатизации и защите информации», ст. 2* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Информационная сфера | Совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений | *Доктрина информационной безопасности РФ, 2000 г.* |
| Информационная сфера (среда) | Сфера деятельности субъектов, связанная с созданием, преобразованием и потреблением информации | *Федеральный закон от 04.07.96 № 85-ФЗ «Об участии в международном информационном обмене», ст. 2* |
| Информационное агентство | Организация, осуществляющая сбор и оперативное распространение информации | *Федеральный закон от 01.12.95 № 191-ФЗ «О государственной поддержке средств массовой информации и книгоиздания Российской Федерации», ст. I* |
| Информационные программы [в сфере деятельности средств массовой информации] | Ежедневные теле- и радиопрограммы новостей, за исключением авторских информационно-аналитических программ | *Федеральный закон от 13.01.95 № 7-ФЗ «О порядке освещения деятельности органов государственной власти в государственных средствах массовой информации»,* |
| Информационные продукты (продукция) | Документированная информация, подготовленная в соответствии с потребностями пользователей и предназначенная или применяемая для удовлетворения потребностей пользователей | *Федеральный закон от 04.07.96 № 85-ФЗ «Об участии в международном информационном обмене», ст. 2* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Информационные процессы | Процессы сбора, обработки, накопления, хранения, поиска и распространения информации | *Федеральный закон от 20.02.95 № 24-ФЗ «Об информации, информатизации и защите информации», ст. 2* |
| Информационные процессы | Процессы создания, сбора, обработки, накопления, хранения, поиска, распространения и потребления информации | *Федеральный закон от 04.07.96 № 85-ФЗ «Об участии в международном информационном обмене», ст. 2* |
| Информационные процессы | Процессы создания, обработки, хранения, защиты от внутренних и внешних угроз, передачи, получения, использования и уничтожения информации | *ГОСТ Р 50922-96. Защита информации. Основные термины и определения. (Прил. А)* |
| Информационные ресурсы | Отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах).<br>*Примечание.* Государственные информационные ресурсы РФ являются открытыми и общедоступными. Исключение составляет документированная информация, отнесенная законом к категории ограниченного доступа. 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 | *Федеральный закон от 20.02.95 № 24-ФЗ «Об информации, информатизации и защите информации».*<br>*Федеральный закон от 04.07.96 № 85-ФЗ «Об участии в международном информационном обмене», ст. 2* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Информационные услуги | Действия субъектов (собственников и владельцев) по обеспечению пользователей информационными продуктами | *Федеральный закон от 04.07.96 № 85-ФЗ «Об участии в международном информационном обмене», ст. 2* |
| Информация | Сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления | *Федеральный закон от 20.02.95 №24-ФЗ «Об информации, информатизации и защите информации», ст. 2; ГОСТ Р 50922-96. Защита информации. Основные термины и определения. (Прил. А)* |
| Информация | Свойство объекта уменьшать неопределенность процесса, изменения его состояния во времени | *БриллюэнЛ.. Наука и теория информации. М.,1958* |
| Информация о гражданах (персональные данные) | Сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность. Персональные данные относятся к категории конфиденциальной информации. 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 | *Федеральный закон от 20.02.95 №24-ФЗ «Об информации, информатизации и защите информации», ст. 2, 11* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Информирование общественности о террористической акции | Не допускается распространение информации: 1) раскрывающей специальные технические приемы и тактику проведения контртеррористической операции; 2) способной затруднить проведение контртеррористической операции и создать угрозу жизни и здоровью людей, оказавшихся в зоне проведения контртеррористической операции или находящихся за пределами указанной зоны; 3) служащей пропаганде или оправданию терроризма и экстремизма; 4) о сотрудниках специальных подразделений, членах оперативного штаба по управлению контртеррористической операцией при ее проведении, а также о лицах, оказывающих содействие в проведении указанной операции | *Федеральный закон от 25.07.98 № 130-ФЗ «О борьбе с терроризмом», ст. 15* |
| Исключительные права автора на использование произведения | Право осуществлять или разрешать следующие действия: воспроизводить произведение (право на воспроизведение); распространять экземпляры произведения любым способом: продавать, сдавать в прокат и т. д. (право на распространение); импортировать экземпляры произведения в целях распространения, включая экземпляры, изготовленные с разрешения обладателя исключительных авторских прав (право на импорт); публично показывать произведение (право па публичный показ); публично исполнять произведение (право на публичное исполнение); сообщать произведение (включая показ, исполнение или передачу в эфир) для всеобщего сведения путей передачи в эфир и(или) последующей передачи в эфир (право | *Закон РФ от 09.07.93 №5351-1 «Об авторском праве и смежных правах», ст. 16* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| | на передачу в эфир); сообщать произведение (включая показ, исполнение или передачу в эфир) для всеобщего сведения по кабелю, проводам или с помощью иных аналогичных средств (право на сообщение для всеобщего сведения по кабелю); переводить произведение (право на перевод): переделывать, аранжировать или другим образом перерабатывать произведение (право на переработку) | |
| Исключительные права на результаты интеллектуальной деятельности (интеллектуальная собственность) | Исключительные права на литературные, художественны и научные произведения, программы для электронно-вычислительных машин и базы данных; смежные права; на изобретения, промышленные образцы, полезные модели, а также приравненные к результатам интеллектуальной деятельности средства индивидуализации юридического лица (фирменные наименования, товарные знаки, знаки обслуживания) и другие результаты интеллектуальной деятельности и средства индивидуализации, охрана которых предусмотрена законом | *Федеральный закон от 13.10.95 №157-ФЗ «О государст венной охране», ст. 2* |
| Исполнение [в области авторского права и смежных прав] | Представление произведений, фонограмм, исполнении, постановок посредством игры, декламации, пения, танца в живом исполнении или с помощью технических средств (телерадиовещания, кабельного телевидения и иных технических средств); показ кадров аудиовизуального произведения в их последовательности (с сопровождением или без сопровождения звуком) | *Закон РФ от 09.07.93 №5351-1 «Об авторском праве и смежных правах», ст. 4* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Исполнитель | Актер, певец, музыкант, танцор или иное лицо, которое играет роль, читает, декламирует, поет, играет на музыкальном инструменте или иным образом исполняет произведения литературы или искусства (в том числе эстрадный, цирковой или кукольный номер), а также режиссер-постановщик спектакля и дирижер | *Закон РФ от 09.07.93 №5351-1 «Об авторском праве и смежных правах», ст. 4* |
| Использование в коммерческих целях | Это продажа, сдача внаем или иной способ коммерческого распространения, а также предложение осуществлять эти действия | *Закон РФ от 23.09.92 №3526-1 «О правовой охране топологии интегральных микросхем», ст. 1* |
| Использование программы для ЭВМ или базы данных | Это выпуск в свет, воспроизведение, распространение и иные действия по их введению в хозяйственный оборот (в том числе в модифицированной форме). Не признается использованием программы для ЭВМ или базы данных передача средствами массовой информации сообщений о выпущенной в свет программе для ЭВМ или базе данных | *Закон РФ от 23.09.92 №3523-1 «О правовой охране программ для электронных вычислительных машин и баз данных», ст. 1* |
| Источники угроз информационной безопасности РФ | Внешние и внутренние.<br>Внешние источники: деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов РФ в информационной сфере; стремление ряда стран к доминированию и ущемлению интересов России в мировом информационном пространстве, вытеснению ее с внешнего и внутреннего информационных рынков; обострение международной конкуренции за обладание информационными технологиями и ресур- | *Доктрина информационной безопасности РФ, 2000 г.* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| | сами; деятельность международных террористических организаций; увеличение технологического отрыва ведущих держав мира и наращивание их возможностей по противодействию созданию конкурентоспособных российских информационных технологий; деятельность космических, воздушных, морских и наземных технических и иных средств (видов) разведки иностранных государств; разработка рядом государств концепции информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним.<br>Внутренние источники: критическое состояние отечественных отраслей промышленности; неблагоприятная криминогенная обстановка, сопровождающаяся тенденциями сращивания государственных и криминальных структур в информационной сфере, получения криминальными структурами доступа к конфиденциальной информации, усиления влияния организованной преступности на жизнь общества, снижения степени защищенности законных интересов граждан, общества и государства в информационной сфере; недостаточная координация деятельности федеральных органов государственной власти, органов государственной власти субъектов РФ по формированию | |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| | и реализации единой государственной политики в области обеспечения информационной безопасности РФ; недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика; неразвитость институтов гражданского общества и недостаточный государственный контроль за развитием информационного рынка России;<br>недостаточное финансирование мероприятий по обеспечению информационной безопасности РФ; недостаточная экономическая мощь государства; снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности; недостаточная активность федеральных органов государственной власти, органов государственной власти субъектов РФ в информировании общества о своей деятельности, в разъяснении принимаемых решений, в формировании открытых государственных ресурсов и развитии системы доступа к ним граждан; отставание России от ведущих стран мира по уровню информатизации федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления, кредитно-финансовой сферы, промышленности, сельского хозяйства, образования, здравоохранения, сферы услуг и быта граждан | |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Категорирование защищаемой информации (объекта зашиты) | Установление градации важности защищаемой информации (объекта защиты) | *ГОСТ Р 50922-96. Защита информации. Основные термины и определения* |
| Контроль организации защиты информации | Проверка соответствия состояния организации, наличия и содержания документов требованиям правовых, организационно-распорядительных и нормативных документов по защите информации | *ГОСТ Р 50922-96. Защита информации. Основные термины и определения* |
| Контроль состояния защиты информации | Проверка соответствия состояния организации и эффективности защиты информации установленным требованиям и (или) нормам защиты информации | *ГОСТ Р 50922-96. Защита информации. Основные термины и определения* |
| Контроль эффективности защиты информации | Проверка соответствия эффективности мероприятий по защите информации установленным требованиям или нормам эффективности защиты информации | *ГОСТ Р 50922-96. Защита информации. Основные термины и определения* |
| Конфиденциальная информация | Документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ | *Федеральный закон от 20.02.95 № 24-ФЗ, ст. 2; Федеральный закон от 04.07 96 №85-ФЗ «Об участии в международном информационном обмене», ст. 2* |
| Контрафактные экземпляры произведения и фонограммы | Экземпляры произведения и фонограммы, изготовление или распространение которых влечет за собой нарушение авторских и смежных прав, а также экземпляры охраняемых в РФ в соответствии с настоящим Законом произведений и фонограмм, импортируемые без согласия обладателей авторских и смежных прав в РФ из государства, в котором эти произведения и фонограммы никогда не охранялись или перестали охраняться | *Закон РФ от 09.07.93 №5351-1 «Об авторском праве и смежных правах», ст. 48* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Контрразведывательная деятельность | Деятельность органов федеральной службы безопасности в пределах своих полномочий по выявлению, предупреждению, пресечению разведывательной и иной деятельности специальных служб и организаций иностранных государств, а также отдельных лиц, направленной на нанесение ущерба безопасности РФ. *Примечание.* Основаниями для осуществления органами федеральной службы безопасности контрразведывательной деятельности являются... необходимость обеспечения защиты сведений, составляющих государственную тайну. Осуществление контрразведывательной деятельности,затрагивающей тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений граждан, допускается только на основании судебного решения | *Федеральный закон от 03.04.95 №40-ФЗ «Об органах Федеральной службы безопасности в Российской Федерации», ст. 9* |
| Концепция национальной безопасности РФ | Система взглядов на обеспечение в РФ безопасности личности, общества и государства от внешних и внутренних угроз во всех сферах жизнедеятельности. В Концепции сформулированы важнейшие направления государственной политики РФ | *Указ Президента РФ от 10 января 2000 г. №24 «О концепции национальной безопасности»* |
| Корпоративная информационная система | Информационная система, участниками которой может быть ограниченный круг лиц, определенный ее владельцем или соглашением участников этой информационной системы | *Федеральный закон РФ от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи»* |
| Лицензия | Разрешение (право) на осуществление лицензируемого указанного вида деятельности при обязательном соблюдении лицензионных требований и условий, выданное лицензирующим органом юридическому лицу или индивидуальному предпринимателю | *Федеральный закон от 25.09.98 № 158-ФЗ в редакции от 12.05.2000 № 69-ФЗ* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Лицензия [в области связи] | Документ, устанавливающий полномочия физических и юридических лиц в соответствии с Федеральным законом «О связи» и иными правовыми актами для осуществления деятельности в области связи | *Федеральный закон от 16.02.95 № 15-ФЗ «О связи», ст. 2* |
| Лицензия [в сфере предоставления услуг связи] | Документ, дающий право на предоставление услуг связи, выданный Министерством связи РФ в установленном порядке в соответствии со статьей 15 Федерального закона «О связи» | *Правила присоединения ведомственных и выделенных сетей, электросвязи к сети электросвязи общего пользования, утвержденные постановлением Правительства РФ от 19.10.96 № 1254, ст. 2* |
| Лицензия [в области зашиты государственной тайны и информации] | Лицензия является официальным документом, который разрешает осуществление на определенных условиях конкретного вида деятельности в течение установленного срока | *Положение о лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны, утвержденное постановлением РФ от 15.04.95 №333, п. 1* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Массовая информация | Предназначенные для неограниченного круга лиц печатные, аудио-, аудиовизуальные и иные сообщения и материалы | *Закон РФ от 27.12.91 №2124-1 «О средствах массовой информации», ст. 2; Федеральный закон от 01.12.95 № 191-ФЗ «О государственной поддержке средств массовой информации и книгоиздания Российской Федерации», ст. 1; Федеральный закон от 04.07.96 № 8 5-ФЗ «Об участии в международном информационном обмене», ст. 2* |
| Матрица доступа | Таблица, отображающая правила разграничения доступа | *Сборник руководящих документов по защите информации от несанкционированного доступа Государственной технической комиссии при Президенте РФ, 1998 г.* |
| Межведомственная комиссия по защите государственной тайны | Коллегиальный орган, координирующий деятельность органов государственной власти по защите государственной тайны в интересах разработки и выполнения государственных программ, нормативных и методических документов, обеспечивающих реализацию законодательства РФ о государственной тайне | *Закон РФ от 21.07.93 №5485-1 «О государственной тайне» в ред. Федерального закона от 06.10.97 № 131-ФЗ, ст. 20* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Международная почтовая связь | Обмен почтовыми отправлениями между организациями почтовой связи, находящимися под юрисдикцией разных государств | *Федеральный закон от 17.07.99 №176-ФЗ «О почтовой связи», ст. 2* |
| Международный информационный обмен | Передача и получение информационных продуктов, а также оказание информационных услуг через Государственную границу РФ | *Федеральный закон от 04.07.96 №85-ФЗ «Об участии в международном информационном обмене», ст. 2* |
| Мероприятие по защите информации | Совокупность действий по разработке и (или) практическому применению способов и средств защиты информации | *ГОСТ Р 50922-96. Защита информации. Основные термины и определения* |
| Мероприятие по контролю эффективности защиты информации | Совокупность действий по разработке и (или) практическому применению методов (способов) и средств контроля эффективности защиты информации | *ГОСТ Р 50922-96. Защита информации. Основные термины и определения* |
| Метка конфиденциальности | Элемент информации, который характеризует конфиденциальность информации, содержащейся в объекте | *Сборник руководящих документов по защите информации от несанкционированного доступа Государственной технической комиссии при Президенте РФ, 1998 г.* |
| Метод (способ) контроля эффективности защиты информации | Порядок и правила применения определенных принципов и средств контроля эффективности защиты информации | *ГОСТ Р 50922-96. Защита информации. Основные термины и определения* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Многоуровневая защита | Защита, обеспечивающая разграничение доступа субъектов с различными правами доступа к объектам различных уровней конфиденциальности | *Сборник руководящих документов по защите информации от несанкционированного доступа Государственной технической комиссии при Президенте РФ, 1998 г.* |
| Модель защиты | Абстрактное (формализованное или неформализованное) описание комплекса программно-технических средств и (или) организационных мер защиты от несанкционированного доступа | *Сборник руководящих документов по защите информации от несанкционированного доступа Государственной технической комиссии при Президенте РФ, 1998 г.* |
| Модификация (переработка) программы для ЭВМ или базы данных | Это любые их изменения, не являющиеся адаптацией | *Закон РФ от 23.09.92 №3523-1 «О правовой охране программ для электронных вычислительных машин и баз данных», ст. 1* |
| Нарушение правил обязательной сертификации | Реализация сертифицированной продукции, не отвечающей требованиям нормативных документов, на соответствие которым она сертифицирована, либо реализация сертифицированной продукции без сертификата соответствия, или без знака соответствия, или без указания в сопроводительной технической документации сведений о сертификации или о нормативных документах, которым должна соответствовать указанная про- | *Кодекс РСФСР об административных правонарушениях от 20.06.84, ст. 170 (в ред. Федерального закона от 19.06.95 № 89-ФЗ, ст. 1)* |

м-да, свежо :(

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| | дукция либо недоведение этих сведений до потребителя (покупателя, заказчика), а равно представление недостоверных результатов испытаний продукции или необоснованная выдача сертификата соответствия на продукцию, подлежащую обязательной сертификации | |
| Национальная безопасность РФ | Безопасность ее многонационального народа как носителя суверенитета и единственного источника власти в РФ | *Указ Президента РФ от 17.12.97 № 1300 (вред. Указа Президента РФ от 10.01.2000 №24 «О концепции национальной безопасности»)* |
| Национальное центральное бюро Интерпола | Подразделение криминальной милиции, входящее в состав центрального аппарата Министерства внутренних дел РФ, имеющее статус главного управления, является органом по сотрудничеству правоохранительных и иных государственных органов РФ с правоохранительными органами иностранных государств-членов Международной организации уголовной полиции - Интерпола (далее именуется - Интерпол) и Генеральным секретариатом Интерпола | *Положение, утвержденное постановлением Правительства РФ от 14.10.96 №1190, п. 1* |
| Национальные интересы России | Совокупность сбалансированных интересов личности, общества и государства в экономической, внутриполитической, социальной, международной, информационной, военной, пограничной, экологической и других сферах. Они носят долгосрочный характер и определяют основные цели, стратегические и текущие задачи | *Указ Президента РФ от 17.12.97 № 1300 (вред. Указа Президента РФ от 10.01.2000 №24 «О концепции национальной безопасности»)* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| | внутренней и внешней политики государства. Национальные интересы обеспечиваются институтами государственной власти, осуществляющими свои функции в том числе во взаимодействии с действующими на основе Конституции РФ и законодательства РФ общественными организациями | |
| Национальные интересы РФ в информационной сфере | Заключаются в соблюдении конституционных прав и свобод граждан в области получения информации и пользования ею, в развитии современных телекоммуникационных технологий, в защите государственных информационных ресурсов от несанкционированного доступа | *Указ Президента РФ от 17.12.97 № 1300 (вред. Указа Президента РФ от 10.01.2000 №24 «О концепции национальной безопасности»)* |
| Национальные интересы РФ в информационной сфере: | ... Соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.<br>... Информационное обеспечение государственной политики Российской Федерация, связанное с доведением до российской и международной общественности достоверной информации о государственной политике РФ, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам.<br>... Развитие современных инфор- | *Доктрина информационной безопасности РФ, 2000 г.* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| | мационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов.<br>... Защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России. | |
| Национальный библиотечно-информационный фонд РФ | Собрание всех видов обязательного экземпляра, комплектуемое на основе обязательного бесплатного экземпляра, распределяемое между книжными палатами, библиотеками, органами научно-технической информации, предназначенное для постоянного хранения и общественного использования | *Федеральный закон от 29.12.94 № 77-ФЗ «Об обязательном экземпляре документов», ст. I* |
| Негосударственная часть Архивного фонда РФ | Архивные фонды и архивные документы, находящиеся в собственности общественных объединений и организаций, а также с момента отделения церкви от государства - в собственности религиозных объединений и организаций, действующих на территории РФ, или в частной собственности и представляющие собой историческую, научную, социальную, экономическую, политическую или культурную ценность | *Основы законодательства РФ об Архивном фонде РФ и архивах от 07.07.93 № 5341-1, ст. 6* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Ненадлежащая реклама | Недобросовестная, недостоверная, неэтичная, заведомо ложная и иная реклама, в которой допущены нарушения требований к ее содержанию, времени, месту и способу распространения, установленных законодательство РФ | *Федеральный закон от 18.07.95 № 108-ФЗ «О рекламе», ст. 2* |
| Несанкционированный доступ к информации | Доступ к информации, нарушающий установленные правила ее получения | *ГОСТ Р 50922-96. Защита информации. Основные термины и определения* |
| Нормы эффективности защиты информации | Значения показателей эффективности защиты информации, установленные нормативными документами | *ГОСТ Р 50922-96. Защита информации. Основные термины и определения* |
| Носитель информации | Физическое лицо, или материальный объектов том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов | *ГОСТ Р 50922-96. Защита информации. Основные термины и определения. (Прил. А)* |
| Носитель сведений, составляющих государственную тайну | Материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов. *Примечание.* Реквизиты носителей сведений, составляющих государственную тайну, включают следующие данные: о степени секретности содержащихся в носителе сведений со ссылкой на соответствующий пункт действующего в данном органе государственной власти, на данном предприятии, в данных учреждении и организации перечня сведений, подлежащих засекречиванию; об органе государственной власти, о предприятии, об учреж- | *Закон РФ от 21.07.93 №5-185-1 «О государственной тайне» в ред. Федерального закона от 06.10.97 № 131-ФЗ, ст. 2, 12* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| | дении, организации, осуществивших засекречивание носителя; о регистрационном номере; о дате или условий рассекречивания сведений либо о событии, после наступления которого сведения будут рассекречены | |
| Обеспечение безопасности | Проведение единой государственной политики в области обеспечения безопасности, применение системы мер экономического, политического, организационного и иного характера, адекватных угрозам жизненно важным интересам личности, общества и государства | *Закон РФ от 05.03.92 №2446-1 «О безопасности», ст. 4* |
| Обеспечение информационной безопасности РФ | Важнейшими задачами обеспечения информационной безопасности РФ являются: реализация конституционных прав и свобод граждан РФ в сфере информационной деятельности; совершенствование и защита отечественной информационной инфраструктуры, интеграция России в мировое информационное пространство; противодействие угрозе развязывания противоборства в информационной сфере. | *Указ Президента РФ от 10 января 2000 г. №24 «О концепции национальной безопасности»* |
| Обнародование произведения | Осуществленное с согласия автора действие, которое впервые делает произведение доступным для всеобщего сведения путем его опубликования, публичного показа, публичного исполнения, передачи в эфире или иным способом | *Закон РФ от 09.07.93 №5331-1 «Об авторском праве и смежных правах», ст. 4* |
| Общедоступная библиотека | Библиотека, которая предоставляет возможность пользования ее фондом и услугами юридическим лицам независимо от их организационно-правовых форм и форм собственности и гражданам без ограничений по уровню образования, специальности, отношению к религии | *Федеральный закон от 29.12.94 № 78-ФЗ «О библиотечном деле», ст. 1* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Общедоступная информация на рынке ценных бумаг | Информация, не требующая привилегий для доступа к ней или подлежащая раскрытию в соответствии с настоящим Федеральным законом | *Федеральный закон от 22.04.96 № 39-ФЗ «О рынке ценных бумаг», ст. 30* |
| Объект доступа | Единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа | *Сборник руководящих документов по защите информации от несанкционированного доступа Государственной технической комиссии при Президенте РФ, 1998 г.* |
| Объект защиты | Информация или носитель информации или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации | *ГОСТ Р 50922-96. Защита информации. Основные термины и определения* |
| Объект почтовой связи | Обособленные подразделения организаций почтовой связи (почтамты, прижелезнодорожные почтамты; отделения перевозки почты при железнодорожных станциях и аэропортах, узлы почтовой связи), а также их структурные подразделения (почтовые обменные пункты, отделения почтовой связи, пункты почтовой связи и другие) | *Федеральный закон от 09.08.9S № 129-ФЗ «О почтовой связи», ст. 1* |
| Объективная форма произведений | Письменная (рукопись, машинопись, нотная запись и так далее); устная (публичное произнесение, публичное исполнение и так далее); звуко- или видеозапись (механическая, магнитная, цифровая, оптическая и так далее); изображение (рисунок, эскиз, картина, план, чертеж, кино-, теле-, видео- или фотокадр и так далее); объемно-пространственная (скульптура, модель, макету сооружение и так далее); другие формы | *Закон РФ от 09.07.93 №5351-1 «Об авторском праве и смежных правах», ст. 6* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Обязательный бесплатный местный экземпляр [документов] | Экземпляры различных видов изготовленных на территории города, района документов, которые подлежат безвозмездной передаче их производителями в соответствующие учреждения и организации в порядке и количестве, установленных настоящим Федеральным законом | *Федеральный закон от 29.12.94 № 77-ФЗ «Об обязательном экземпляре документов», ст. 1* |
| Обязательный бесплатный федеральный экземпляр [документов] | Экземпляры различных видов документов, изготовленных на территории РФ, за ее пределами по заказу предприятий, учреждений, организаций и отдельных лиц, находящихся в ведении РФ, а также документов, импортируемых для общественного распространения на территории РФ, которые подлежат безвозмездной передаче их производителями в соответствующие учреждения и организации в порядке и количестве, установленных настоящим Федеральным законом | *Федеральный закон от 29.12.94 № 77-ФЗ «Об обязательном экземпляре документов», ст. 1* |
| Обязательный бесплатный экземпляр [документов] | Экземпляры различных видов документов, подлежащие безвозмездной передаче их производителями в соответствующие учреждения и организации в порядке и количестве, установленных настоящим Федеральным законом | *Федеральный закон от 29.12.94 № 77-ФЗ «Об обязательном экземпляре документов», ст. 1* |
| Обязательный платный экземпляр [документов] | Экземпляры различных видов документов, подлежащие передаче за плату их производителями в соответствующие учреждения и организации в порядке и количестве, установленных настоящим федеральным законом | *Федеральный закон от 29.12.94 № 77-ФЗ «Об обязательном экземпляре документов», ст. 1* |
| Обязательный экземпляр документов | Экземпляры различных видов тиражированных документов, подлежащие передаче производителями в соответствующие учреждения и организации в порядке и количестве, установленных настоящим Федеральным законом | *Федеральный закон от 29.12.94 № 77-ФЗ «Об обязательном экземпляре документов», ст. 1* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Обязательный экземпляр субъекта РФ [при формировании обязательного экземпляра документов] | Экземпляры различных видов изготовленных на территориях субъектов РФ документов, которые подлежат передаче их производителями в соответствующие учреждения и организации в порядке и количестве, установленных настоящим Федеральным законом | *Федеральный закон от 29.12.94 № 77-ФЗ «Об обязательном экземпляре документов», ст. 1* |
| Ограничения прав должностного лица или гражданина, допущенных или ранее допускавшихся к государственной тайне, могут касаться: | Права выезда за границу на срок, оговоренный в трудовом договоре (контракте) при оформлении допуска гражданина к государственной тайне; права на распространение сведений, составляющих государственную тайну, и на использование открытий и изобретений, содержащих такие сведения; права на неприкосновенность частной жизни при проведении проверочных мероприятий в период оформления допуска к государственной тайне | *Закон РФ от 21.07.93 №5485-1 «О государственной тайне», ст. 24* |
| Оперативно-розыскные мероприятия | Контроль почтовых отправлений, телеграфных и иных сообщений. Прослушивание телефонных переговоров. Снятие информации с технических каналов связи. *Примечание.* Оперативно-розыскные мероприятия, связанные с контролем почтовых отправлений, телеграфных и иных сообщений, прослушиванием телефонных переговоров с подключением к станционной аппаратуре предприятий, учреждений и организаций независимо от форм собственности, физических и юридических лиц, предоставляющих услуги и средства связи, со снятием информации с технических каналов связи, проводятся с использовани- | *Федеральный закон от 12.08.95 № 144-ФЗ «Об оперативно-розыскной деятельности», ст. 9, 10, 11 (в редакции федеральных законов от 18.07.97 № 101-ФЗ, 21.07.98 №117-ФЗ, 105.01.99 №6-ФЗ, 30.12.99 №22 5-ФЗ)* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| | ем оперативно-технических сил и средств органов федеральной службы безопасности и органов внутренних дел и в пределах своих полномочий, федеральных органов налоговой полиции в порядке определенном межведомственными нормативными актами или соглашениями между органами, осуществляющими оперативно-розыскную деятельность. Проведение оперативно-розыскных мероприятий, которые ограничивают конституционные права человека и гражданина на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, передаваемых по сетям электрической и почтовой связи, а также право на неприкосновенность жилища, допускается на основании судебного решения и при наличии информации: о признаках подготавливаемого, совершаемого или совершенного противоправного деяния, по которому производство предварительного следствия обязательно; о лицах, подготавливающих, совершающих или совершивших противоправное деяние, по которому производство предварительного следствия обязательно; о событиях или действиях, создающих угрозу государственной, военной, экономической или экологической безопасности РФ | |
| Оператор связи [электрической или почтовой] | Физическое или юридическое лицо, имеющее право на предоставление услуг электрической или почтовой связи | *Федеральный закон от 16.02.95 № 15-ФЗ «О связи», ст. 2* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Опубликование (выпуск в свет) | Выпуск в обращение экземпляров произведения, фонограммы с согласия автора произведения, производителя фонограммы в количестве, достаточном для удовлетворения разумных потребностей публики исходя из характера произведения, фонограммы | *Закон РФ от 09.07.93 №5351-1 «Об авторском праве и смежных правах», ст. 4* |
| Орган защиты информации | Административный орган, осуществляющий организацию защиты информации. | *ГОСТ Р 50922-96. Защита информации. Основные термины и определения. (Прил. А)* |
| Организации почтовой связи | Юридические лица независимо от их организационно-правовых форм, оказывающие услуги почтовой связи в качестве основного вида деятельности | *Федеральный закон от 17.07.99 №176-ФЗ «О почтовой связи», ст. 2* |
| Организации теле-, радиовещания (телерадиовещательная компания - ТМС) | Организация, осуществляющая производство, монтаж, расстановку во времени и распространение с использованием электромагнитных волн (по эфирным, кабельным, проводным и иным электромагнитным системам) звуковой (радиовещание), визуальной и аудиовизуальной (телевещание) массовой информации и данных, предназначенных для получения непосредственно телезрителями и радиослушателями | *Федеральный закон от 01.12.95 № 191-ФЗ «О государственной поддержке средств массовой информации и книгоиздания Российской Федерации», ст. I* |
| Организационный контроль эффективности защиты информации | Проверка полноты и обоснованности мероприятий по защите информации требованиям нормативных документов по защите информации | *ГОСТ Р 50922-96. Защита информации. Основные термины и определения* |
| Организация защиты информации | Содержание и порядок действий по обеспечению защиты информации | *ГОСТ Р 50922-96. Защита информации. Основные термины и определения* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Органы внешней разведки РФ... | 6) Организуют и обеспечивают в пределах своей компетенции защиту государственной тайны в учреждениях РФ, находящихся за пределами территории РФ, включая определение порядка осуществления физической и инженерно-технической защиты указанных учреждений, мероприятия по предотвращению утечки по техническим каналам сведений, составляющих государственную тайну...<br>8) обеспечивают безопасность командированных за пределы РФ граждан РФ, имеющих по роду своей деятельности допуск к сведениям, составляющим государственную тайну, и находящихся с ними членов их семей...<br>11) обеспечивают собственную безопасность, т. е. защиту своих сил, средств и информации от противоправных действий и угроз. | *Федеральный закон от 10.01.96 № 5-ФЗ «О внешней разведке», ст. 6* |
| Органы защиты государственной тайны | Межведомственная комиссия по защите государственной тайны; органы федеральной исполнительной власти (Федеральная служба безопасности РФ, Министерство обороны РФ, Федеральное агентство правительственной связи и информации при Президенте РФ), Служба внешней разведки РФ, Государственная техническая комиссия при Президенте РФ и их органы на местах; органы государственной власти, предприятия, учреждения и организации и их структурные подразделения по защите государственной тайны | *Закон РФ от 21.07.93 №5485-1 «О государственной тайн» в ред, от 06.10.97№ 131-ФЗ, ст. 20* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Органы правоохранительные | Государственные органы, основной функцией которых является охрана законности и правопорядка, борьбы с преступностью: суд, прокуратура, органы внутренних дел, контрразведки, таможенного контроля, налоговой полиции, юстиции, арбитража. В широком смысле данное понятие включает также государственно-общественные (субсидируемые государством) органы самодеятельности населения. | *Федеральная программа, утвержденная Указом Президента РФ от 24.05.91 № 1016* |
| Органы федеральной службы безопасности | к) Участвовать в разработке и реализации мер по защите сведений, составляющих государственную тайну; осуществлять контроль за обеспечением сохранности сведений, составляющих государственную тайну, в государственных органах, воинских формированиях, на предприятиях, в учреждениях и организациях независимо от форм собственности; в установленном порядке осуществлять меры, связанные с допуском граждан к сведениям, составляющим государственную тайну | *Федеральный закон от 03.01.95 № 40-ФЗ «Об органах Федеральной службы безопасности в Российский Федерации», ст. 12* |
| Оригинальная топология | Топология, созданная в результате творческой деятельности автора. Топология признается оригинальной до тех пор, пока не доказано обратное | *Закон РФ от 23.09.92 №3526-1 «О правовой охране топологии интегральных микросхем», ст. 3* |
| Основания для отказа должностному лицу или гражданину в допуске к государственной тайне | Признание его судом недееспособным, ограниченно дееспособным или рецидивистом, нахождение его под судом или следствием за государственные и иные тяжкие преступления, наличие у него неснятой судимости за эти преступления; наличие у него медицинских противопоказаний для рабо- | *Закон РФ от 21.07.93 №5485-1 «О государственной тайне» в ред, от 06.10.97 № 131-ФЗ. ст. 22* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| | ты с использованием сведений, составляющих государственную тайну, согласно перечню, утверждаемому Министерством здравоохранения РФ; постоянное проживание его самого и (или) его близких родственников за границей и (или) оформление указанными лицами документов для выезда на постоянное жительство в другие государства, выявление в результате проверочных мероприятий действий оформляемого лица, создающих угрозу безопасности РФ; уклонение его от проверочных мероприятий и (или) сообщение им заведомо ложных анкетных данных | |
| Основной субъект обеспечения безопасности | Государство, осуществляющее функции в этой области через органы законодательной, исполнительной и судебной властей | *Закон РФ от 05.03.92 №2446-1 «О безопасности»* |
| Основные объекты безопасности | Личность - ее права и свободы; общество - его материальные и духовные ценности; государство - его конституционный строй, суверенитет и территориальная целостность | *Закон РФ от 05.03.92 №2446-1 «О безопасности», ст. 1* |
| Открытый ключ электронной цифровой подписи | Уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе | *Федеральный закон РФ от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи»* |
| Отнесение сведений к государственной тайне и их засекречивание | Введение в предусмотренном настоящим Законом порядке для сведений, составляющих государственную тайну, ограничений на | *Закон РФ от 21.07.93 №5485-1 «О государственной тайне» вред.* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| | их распространение и на доступ к их носителям.<br>Обоснованность отнесения сведений к государственной тайне и их засекречивания - установление путем экспертной оценки целесообразности засекречивания конкретных сведений, вероятных экономических и иных последствий этого акта исходя из баланса жизненно важных интересов государства, общества и граждан.<br>Своевременность отнесения сведений к государственной тайне и их засекречивания - установление ограничений на распространение этих сведений с момента их получения (разработки) или заблаговременно | *Федерального закона от 06.10.97 № 131-ФЗ, ст. 6* |
| Пароль | Идентификатор субъекта доступа, который является его (субъекта) секретом | *Сборник руководящих документов по защите информации от несанкционированного доступа Государственной технической комиссии при Президенте РФ, 1998 г.* |
| Передача в эфир | Сообщение произведений, фонограмм, исполнений, постановок, передач организаций эфирного или кабельного вещания для всеобщего сведения (включая показ или исполнение) посредством их передачи по радио или телевидению (за исключением кабельного телевидения). При передаче произведений, фонограмм, исполнений, постановок, передач организаций эфирного или кабельного вещания в эфир через спутник под | *Закон РФ от 09.07.93 №5351-1 «Об авторском праве и смежных правах», ст. 4* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| | передачей в эфир понимается прием сигналов с наземной станции на спутники передача сигналов со спутника, посредством которых произведения, фонограммы, исполнения, постановки, передачи организаций эфирного или кабельного вещания могут быть доведены до всеобщего, сведения независимо от фактического приема их публикой | |
| Передача организации эфирного или кабельного вещания | Передача, созданная самой организацией эфирного или кабельного вещания, а также по ее заказу за счет ее средств другой организацией | *Закон РФ от 09.07.93 №5351-1 «Об авторском праве и смежных правах, ст. 4* |
| Передающий центр (ПЦ) | Радиотелевизионные передающие центры (РТПЦ), радиоцентры (РЦ) и иные организации электросвязи, предоставляющие в том числе услуги по распространению теле- и (или) радиопрограмм, подготовленных организациями теле-, радиовещания | *Федеральный законом 01.12.95 № 191-ФЗ «О государственной поддержке средств массовой информации и книгоиздания Российской Федерации», ст. I* |
| Периодическое печатное издание | Газета, журнал, альманах, бюллетень иное издание, имеющее постоянное название, текущий номер и выходящее в свет не реже одного раза в год | *Закон РФ от 27.12.91 №2124-1 «О средствах массовой информации», ст. 2; Федеральный закон от 01.12.95 № 191-ФЗ «О государственной поддержке средств массовой информации и книгоиздания Российской Федерации», ст. 1* |
| Персональные данные | Информация о гражданах (персональные данные) | |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Письменная корреспонденция | Простые и регистрируемые письма, почтовые карточки, секограммы, бандероли и мелкие пакеты | *Федеральный закон от /7.07.99 №176-ФЗ«0 почтовой связи», ст. 2* |
| Подтверждение подлинности электронной цифровой подписи в электронном документе | Положительный результат проверки соответствующим сертифицированным средством электронной подписи с использованием сертификата ключа подписи принадлежности электронной цифровой подписи в электронном документе владельцу сертификата ключа подписи и отсутствия искажений в подписанном данной электронной цифровой подписью электронном документе | *Федеральный закон РФ от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи»* |
| Показ произведения | Демонстрация оригинала или экземпляра произведения непосредственно или на экране с помощью пленки, диапозитива, телевизионного кадра или иных технических средств, а также демонстрация отдельных кадров аудиовизуального произведения без соблюдения их последовательности | *Закон РФ от 09.07.93 №5351-1 «Об авторском правей смежных правах», ст. 4* |
| Показ фильма | Публичная демонстрация фильма, осуществляемая в кинозале, по эфирному, кабельному, спутниковому телевидению и другими техническими способами | *Федеральный закон от 22.08.9б №126-ФЗ «О государственной поддержке кинематографии Российской Федерации», ст. 3* |
| Получатель документов | Юридическое лицо, наделенное правом получения, хранения и общественного использования обязательного экземпляра на безвозмездной или возмездной основе | *Федеральный закон от 29.12.94 № 77-ФЗ «Об обязательном экземпляре документов», ст. 1* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Пользователь сертификата ключа подписи | Физическое лицо, использующее полученные в удостоверяющем центре сведения о сертификате ключа подписи для проверки принадлежности электронной цифровой подписи владельцу сертификата ключа подписи; информационная система общего пользования - информационная система, которая открыта для использования всеми физическими и юридическими лицами и в услугах которой этим лицам не может быть отказано | *Федеральный закон РФ от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи»* |
| Пользователь библиотеки | Физическое или юридическое лицо, пользующееся услугами библиотеки | *Федеральный закон от 29.12.94 № 78-ФЗ «О библиотечном деле», ст. 1* |
| Пользователь (потребитель) информации | Субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением | *ГОСТ Р 50922-96. Защита информации. Основные термины и определения. (Прил. А)* |
| Пользователь (потребитель) информации | Субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею | *Федеральный закон от 20.02.95 №24-ФЗ «Об информации, информатизации и защите информации», ст. 2* |
| Пользователь (потребитель) информации, средств международного информационного обмена | Субъект, обращающийся к собственнику или владельцу за «получением необходимых ему информационных продуктов или возможности использования средств международного информационного обмена и пользующийся ими | *Федеральный закон от 04.07.96 № 85-ФЗ «Об участии в международном информационном обмене», ст. 2* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Пользователь связи | Физические и юридические лица, являющиеся потребителями услуг связи | *Федеральный закон от 16.02.95 № 15-ФЗ «О связи», ст. 2* |
| Последующая передача в эфир | Последующая передача в эфир ранее переданных в эфир произведений, фонограмм, исполнений, постановок, передач организаций эфирного или кабельного вещания | *Закон РФ от 09.07.93 №5351-1 «Об авторском праве и смежных правах», ст. 4* |
| Потребитель услуг телеграфной связи | Учреждения, организации и предприятия, независимо от формы собственности, их объединения и физические лица, которым была предоставлена услуга телеграфной связи, а также которые обратились или имеют намерение обратиться с целью получить услугу телеграфной связи | *Правила, утвержденные постановлением Правительства РФ от 23.04.94 №374. п. 3 (утр. силу от 28.08.97 №1108)* |
| Почтовая связь | Прием, обработка, перевозка и доставка почтовых отправлений, а также перевод денежных средств | *Федеральный закон от 16.02.95 № 15-ФЗ «О связи», ст. 2* |
| Почтовая связь | Прием, обработка, перевозка и доставка почтовых отправлений, а также почтовых и телеграфных переводов денежных средств | *Федеральный закон от 17.07.99 №176-ФЗ«0 почтовой связи», ст. 2 (утр. силу)* |
| Почтовая связь | Вид связи, представляющий собой единый производственно-технологический комплекс технических и транспортных средств, обеспечивающий прием, обработку, перевозку, доставку (вручение) почтовых отправлений, а также осуществление почтовых переводов денежных средств | *Федеральный закон от 17.07.99 №176-ФЗ«0 почтовой связи», ст. 2* |
| Почтовая связь общего пользования | Составная часть единой почтовой связи РФ, которая открыта для пользования всем гражданам (физическим лицам) и юридическим лицам и в услугах которой этим лицам не может быть отказано | *Федеральный закон от 0908.95 № 129-ФЗ «О почтовой связи», ст. 1. (Утр. силу от 17.07.99 №176-ФЗ«0 почтовой связи»)* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Почтовые отправления | Адресованные письменная корреспонденция, прямые почтовые контейнеры | *Федеральный закон от 16.02.95 № 15-ФЗ «О связи», ст. 1* |
| Почтовые отправления | Местные и иногородние письма и почтовые карточки, бандероли и мелкие пакеты, посылки, почтовые контейнеры, печатные издания в соответствующей упаковке | *Федеральный закон от 09.08.95 №129-ФЗ«0 почтовой связи», ст. 1.(Утр. силу от 17.07.99 №176-ФЗ«0 почтовой связи»)* |
| Правила доступа к информации | Совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям | *ГОСТ Р 50922-96. Защита информации. Основные термины и определения. (Прил. А)* |
| Правила разграничения доступа | Совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа | *Сборник руководящих документов по защите информации от несанкционированного доступа Государственной технической комиссии при Президенте РФ, 1998 г.* |
| Право доступа к информации | Совокупность правил доступа к информации, установленных правовыми документами или собственником, владельцем информации | *ГОСТ Р 50922-96. Защита информации. Основные термины и определения. (Прил. А)* |
| Предприятия, учреждения и организации связи | Юридические лица независимо от форм собственности, предоставляющие услуги электрической или почтовой связи физическим и юридическим лицам в качестве основного лица деятельности | *Федеральный закон от 16.02.95 № 15-ФЗ «О связи», ст. 2* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Пресс-конференция, интервью [при ведении предвыборной агитации] | Не являющиеся политической рекламой обращения кандидата (кандидатов), их доверенных лиц, представителя (представителей) избирательных объединений к избирателям с изложением собственной предвыборной программы (платформы), сообщения, сделанные в ходе встречи с журналистом (журналистами). | *Положение, утвержденное Указом Президента РФ от 29.10.93 №1792. Н. 2* |
| Принципы обеспечения безопасности | Законность; соблюдение баланса жизненно важных интересов личности, общества и государства; взаимная ответственность личности, общества и государства по обеспечению безопасности; интеграция с международными системами безопасности | *Закон РФ от 05.03.92 №2446-1 «О безопасности», ст. 5* |
| Программа для ЭВМ | Объективная форма представления совокупности данных и команд, предназначенных для функционирования электронных вычислительных машин (ЭВМ) и других компьютерных устройств с целью получения определенного результата. Под программой Для ЭВМ подразумеваются также подготовительные материалы, полученные в ходе ее разработки, и порождаемые ею аудиовизуальные отображения | *Закон РФ от 23.09.92 №3523-1 «О правовой охране программ для электронных вычислительных машин и баз данных», ст. 1* |
| Программа для ЭВМ | Объективная фирма представления совокупности данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств с целью получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения | *Закон РФ от 09.07.93 №5351-1 «Об авторском праве и смежных правах», ст. 4* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Программа интерактивного типа («мультимедиа») для ЭВМ | Программа для всех видов персональных ЭВМ (в том числе для телевизионных игровых компьютерных приставок), основанная на диалоговом (интерактивном) взаимодействии пользователя с ЭВМ | *Прил. № 1 к постановлению Правительства РФ от 17.05.96 № 614. п. 2* |
| Производитель документов | Юридическое лицо независимо от его организационно-правовой формы и формы собственности, производящее, публикующее и распространяющее различные виды обязательных экземпляров | *Федеральный закон от 29.12.94 № 77-ФЗ «Об обязательном экземпляре документов», ст. 1* |
| Пропускной режим [на охраняемых объектах] | Порядок прохода лиц, проезда транспортных средств, проноса и провоза вещей на охраняемые объекты, устанавливаемый, соответствующими лицами, замещающими государственные должности в федеральных органах государственной власти, совместно с федеральными органами государственной охраны | *Федеральный закон от 27.05.96 № 57-ФЗ «О государственной охране», ст. 1* |
| Публичный показ, публичное исполнение или сообщение для всеобщего сведения | Любые показ, исполнение или сообщение произведений, фонограмм, исполнении, постановок, передач организаций эфирного или кабельного вещания непосредственно либо с помощью технических средств в месте, открытом для свободного посещения, или в месте, где присутствует значительное число лиц, не принадлежащих к обычному кругу семьи, независимо от того, воспринимаются ли произведения, фонограммы, исполнения, постановки, передачи организаций эфирного или кабельного вещания в месте их сообщения или в другом месте одновременно с сообщением произведений, фонограмм, исполнений, постановок, передач организаций эфирного или кабельного вещания | *Закон РФ от 09.07.93 №5351-1 «Об авторском праве и смежных правах», ст. 4* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Радио-, теле-, видео-, кинохроникальная программа | Совокупность периодических аудио-, аудиовизуальных сообщений и материалов (передач), имеющая постоянное название и выходящая в свет (эфир) не реже одного раза в год | *Закон РФ от 27.12.91 №2124-1 «О средствах массовой информации», ст. 2; Федеральный закон от 01.12.95 № 191-ФЗ «О государственной поддержке средств массовой информации и книгоиздания Российской Федерации», ст. 1* |
| Радиоэлектронные средства | Технические средства, состоящие из одного или нескольких радиопередающих или радиоприемных устройств или их комбинации и вспомогательного оборудования, предназначенные для передачи и приема радиоволн | *Кодекс РСФСР об административных правонарушениях от 20.06.84, ст. 137 (вред. Федерального закона от 06.08.96 № 108-ФЗ «О рекламе», ст. 1); Особые условия утвержденные постановлением Правительства РФ от 17.07.96 №832, п. 2* |
| Радиоэлектронные средства | Радиостанции, радиотелефоны, системы радионавигации, радиоопределения, системы кабельного телевидения и другие устройства, при работе которых используются электромагнитные колебания с частотами выше 9 кГц | *Особые условия приобретения радиоэлектронных средств и высококачественных устройств, утвержденные постановлением Правительства РФ от 17.07.96 № 832, п. 2* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Разведывательная деятельность | Деятельность, которая осуществляется органами внешней разведки РФ посредством добывания и обработки информации о затрагивающих жизненно важные интересы РФ реальных и потенциальных возможностях, действиях, планах и намерениях иностранных государств, организаций и лиц, а также оказание содействия в реализаций мер, осуществляемых государством в интересах обеспечения безопасности РФ | *Федеральный законом 10.01.96 № 5-ФЗ «О внегиней разведке», ст. 2* |
| Разведывательная информация | Информация о затрагивающих жизненно важные интересы РФ реальных и потенциальных возможностях, действиях, планах и намерениях иностранных государств, организаций и лиц | *Федеральный закон от 10.01.96 № 5-ФЗ «О внешней разведке», п. 1 см. 2* |
| Разглашение государственной тайны | Разглашение сведений, составляющих государственную тайну, лицом, которому она была доверена или стала известна по служб» или работе, если эти сведения стали достоянием других лиц, при отсутствии признаке] государственной измены | *Уголовный кодекс РФ от 13.06.96 № 63-ФЗ, ст. 283* |
| Распространение программы для ЭВМ или базы данных | Предоставление доступа к воспроизведенной в любой материальной форме программе для ЭВМ или базе данных, в том числе сетевыми и иными способами, а также путем продажи, проката, сдачи внаем, Предоставления взаймы, включая импорт для любой из этих целей | *Закон РФ от 23:09.92 №3523-1 «О правовой охране Программ для электронных вычислительных машин и баз данных», ст. 1* |
| Распространение продукции средства массовой информации | Продажа (подписка, доставка, раздача) периодических печатных изданий, аудио- или видеозаписей программ, трансляция радио-, телепрограмм (вещание), демонстрация кинохроникальных программ | *Закон РФ от 27.1291 №212-1-1 «О средствах массовой информации», ст. 2. Федеральный закон от 01.12.95* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| | | *№ 191-ФЗ «О государственной поддержке средств массовой информации и книгоиздания Российской Федерации», ст. 1* |
| Распространитель [средств массовой информации] | Лицо, осуществляющее распространение продукции средства массовой информации по договору с редакцией, издателем или на иных законных основаниях | *Закон РФ от 27.12.91 №2124-1 «О средствах массовой информации», ст. 2* |
| Распространитель периодических печатных изданий по подписке | Юридическое лицо или индивидуальный предприниматель, оказывающее по договору с редакцией, издателем или на иных законных основаниях услуги по доставке (раздаче) комплектов периодических печатных изданий в течение определенного договором периода времени | *Правила, утвержденные постановлением Правительства РФ от 14.03.95 №250, п. 4 (утр. силу с 01.01.98)* |
| Рассекречивание сведений и их носителей | Снятие ранее введенных в предусмотренном настоящим Законом порядке ограничений на распространение сведений, составляющих государственную тайну, и на доступ к их носителям | *Закон РФ от 21.07.93 №5485-1 «О государственной тайне» в ред. Федерального закона от 06.10.97 № 131-ФЗ, ст. 13* |
| Редакция средства массовой информации | Организация, учреждение, предприятие либо гражданин, объединение граждан, осуществляющие производство и выпуск средства массовой информации | *Закон РФ от 27.12.91 №2124-1 «О средствах массовой информации», ст. 2* |
| Редакция средства массовой информации | Организация (независимо от формы собственности), осуществляющая производство и выпуск средства массовой информации | *Федеральный закон от 01.12.95 № 191-ФЗ «О государственной поддержке средств массовой информации и книгоиздания Российской Федерации», ст. 1* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Реклама | Распространяемая в любой форме, с помощью любых средств информация о физическом или юридическом лице, товарах, идеях и начинаниях (рекламная информация), которая предназначена для неопределенного круга лиц и призвана формировать или поддерживать интерес к этим физическому, юридическому лицу, товарам, идеям и начинаниям и способствовать реализации товаров, идей и начинаний | *Федеральный законом 18.07.95 № 108-ФЗ «О рекламе», ст. 2* |
| Репродуцирование (репрографическое воспроизведение) | Факсимильное воспроизведение в любых размере и форме одного или более экземпляров оригиналов или копий письменных и других графических произведений путем фотокопирования или с помощью других технических средств, иных, чем издание; репрографическое воспроизведение не включает в себя хранение или воспроизведение указанных копий в электронной (включая цифровую), оптической или иной машиночитаемой форме | *Закон РФ от 09.07.93 №5351-1 «Об авторском праве и смежных правах», ст. 4* |
| Сведения, не подлежащие отнесению к государственной тайне и засекречиванию: | О чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях;<br>о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;<br>о привилегиях, компенсациях и льготах, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям; | *Закон РФ от 21.07.93 №5485-1 «О государственной тайне» вред. Федерального закона от 06.10,97 № 131-ФЗ, ст. 7* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| | о фактах нарушения прав и свобод человека и гражданина;<br>о размерах золотого запаса и государственных валютных резервах РФ, о состоянии здоровья высших должностных лиц РФ;<br>о фактах нарушения законности органами государственной власти и их должностными лицами. | |
| Сведения, относящиеся к государственной тайне; перечень сведений, составляющих государственную тайну | Совокупность категорий сведений, в соответствии с которыми Сведения относятся к государственной тайне и засекречиваются на основаниях и в порядке, установленных Федеральным законодательством.<br>*Примечание.* Государственную тайну составляют:<br>1) сведения в военной области:<br>о содержании стратегических и оперативных планов, документов боевого управления по подготовке и проведению операций, стратегическому, оперативному и мобилизационному развертыванию Вооруженных Сил РФ, других войск, воинских формирований и органов, предусмотренных Федеральным законом «Об обороне», об их боевой и мобилизационной готовности, о создании и об использовании мобилизационных ресурсов, о планах строительства Вооруженных Сил РФ, других войск РФ, о направлениях развития вооружения и военной техники, о содержании и результатах выполнения целевых программ, научно-исследовательских и опытно-конструкторских работ по созданию и модернизации образцов вооружения и военной техники;<br>о разработке, технологии, произ- | *Закон РФ от 21.07.93 №5485-1 «О государственной тайне» в ред. Федерального закона от 06.10.97 М131-ФЗ, ст. 2, 5* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| | водстве, об объемах производства, о хранении, об утилизации ядерных боеприпасов, Их составных частей, делящихся ядерных материалов, используемых в ядерных боеприпасах, о технических средствах и (или) методах защиты ядерных боеприпасов от несанкционированного применения, а также о ядерных энергетических и специальных физических установках оборонного значения; о тактико-технических характеристиках и возможностях боевого применения образцов вооружения и военной техники, о свойствах, рецептурах или технологиях производства новых видов ракетного топлива или взрывчатых веществ военного назначения; о дислокации, назначении, степени готовности, защищенности режимных и особо важных объектов, об их проектировании, строительстве и эксплуатации, а также об отводе земель, недр и акваторий для этих объектов; о дислокации, действие тельных наименованиях, об организационной структуре, о вооружении, численности Войск и состоянии их боевого обеспечения, а также о военно-политической и (или) оперативной обстановке; 2) сведения в области экономики, науки и техники: о содержании планов подготовки РФ и ее отдельных регионов к возможным военным действиям, о мобилизационных мощностях промышленности по изготовлению и ремонту вооружения и военной техники, об объемах производства, поставок, о запасах стратегических видов сырья и материалов, а также о раз- | |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| | мещении, фактических размерах и об использовании государственных материальных резервов;<br>об использовании инфраструктуры РФ в целях обеспечения обороноспособности и безопасности государства,; о силах и средствах гражданской обороны, о дислокации, предназначении и степени защищенности объектов административного управления, о степени обеспечения безопасности населения, о функционировании транспорта и связи в РФ в целях обеспечения безопасности государства; об объемах, о планах (заданиях) государственного оборонного заказа, о выпуске и поставках (в денежном или натуральном выражении) вооружения, военной техники и другой оборонной продукции, 0 наличии и наращивании мощностей по их выпуску, о связях предприятий по кооперации, о разработчиках или об изготовителях указанных вооружения, военной техники и другой оборонной продукции;<br>о достижениях науки и техники, о научно-исследовательских, об опытно-конструкторских, о проектных работах и технологиях, имеющих важное оборонное или экономическое значение, влияющих на безопасность государства; об объемах запасов, добычи, передачи и потребления платины, металлов платиновой группы, природных алмазов, а также об объемах других стратегических видов полезных ископаемых РФ (по списку, определяемому Правительством РФ); | |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| | 3) сведения в области внешней политики и экономики: о внешнеполитической, внешнеэкономической деятельности РФ, преждевременное распространение которых может нанести ущерб безопасности государства; о финансовой политике в отношении иностранных государств (за исключением обобщенных показателей по внешней задолженности), а также о финансовой или денежно-кредитной деятельности, преждевременное распространение которых может нанести ущерб безопасности государства;<br>4) сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности: о силах, средствах, об источниках, о методах, планах и результатах разведывательной, контрразведывательной и оперативно-розыскной деятельности, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения; о лицах, сотрудничающих или сотрудничавших на конфиденциальной основе с органами, осуществляющими разведывательную, контрразведывательную и оперативно-розыскную деятельность; об организации, о силах, средствах и методах обеспечения безопасности объектов государственной охраны, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения;<br>о системе президентской, правительственной, шифрованной, в том числе кодированной и засекреченной связи, о шифрах, о раз- | |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| | работке, об изготовлении шифров и обеспечении ими, о методах и средствах анализа шифровальных средств и средств специальной защиты, об информационно-аналитических системах специального назначения; о методах и средствах защиты секретной информации; об организации и о фактическом состоянии защиты государственной тайны; о защите Государственной границы РФ, исключительной экономической зоны и континентального шельфа РФ; о расходах федерального бюджета, связанных с обеспечением обороны, безопасности государства и правоохранительной деятельности в РФ; о подготовке кадров, раскрывающие мероприятия, проводимые в целях обеспечения безопасности государства | |
| Сдавать в прокат (внаем) (в области авторского права) | Предоставлять экземпляр произведения или фонограммы во временное пользование в целях извлечения прямой или косвенной коммерческой выгод | *Закон РФ от 09.07.93 №5331-1 «Об авторском праве и смежных правах», ст. 4* |
| Сертификат [в сфере оказания услуг связи] | Документ, подтверждающий, что надлежащим образом идентифицированные оборудование или услуга связи соответствуют требованиям нормативных документов | *Федеральный закон от 16.02.95 № 15-ФЗ «О связи», ст. 2* |
| Сертификат соответствия | Документ, выданный по правилам системы сертификации для подтверждения соответствия сертифицированной продукции установленным требованиям | *Закон РФ от 10.06.93 №5151-1 «О сертификации продукции и услуг», ст. 6* |
| Сертификат средств электронной цифровой подписи | Документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной цифровой подписи установленным требова- | *Федеральный закон РФ от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи»* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| | ниям; закрытый ключ электронной цифровой подписи - уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи | |
| Сертификат ключа подписи | Документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и которые выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи | *Федеральный закон РФ от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи»* |
| Сеть почтовой связи | Совокупность объектов почтовой связи и почтовых маршрутов | *Федеральный закон от 17.07.99 №176-ФЗ «О почтовой связи», ст. 2* |
| Сеть связи общего пользования | Составная часть взаимоувязанной сети связи РФ, открытая для пользования всем физическим и юридическим лицам, в услугах которой этим лицам не может быть отказано | *Федеральный закон от 16.02.95 № 15-ФЗ «О связи», ст. 2* |
| Сеть электросвязи | Технологические системы, обеспечивающие один или несколько видов передач: телефонную, телеграфную, факсимильную, передачу данных и других видов документальных сообщений, включая обмен информацией между ЭВМ, телевизионное, звуковое и иные виды радио- проводного вещания | *Федеральный закон от 16.02.95 № 15-ФЗ «О связи», ст. 2* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Силы обеспечения безопасности | Вооруженные Силы, федеральные органы безопасности, органы внутренних дел, внешней разведки, обеспечения безопасности органов законодательной, исполнительной, судебной властей и их высших должностных лиц, налоговой службы, службы ликвидации последствий чрезвычайных ситуаций, формирования гражданской обороны, пограничные войска, внутренние войска; органы, обеспечивающие безопасное ведение работ в промышленности, энергетике, на транспорте и в сельском хозяйстве; службы обеспечения безопасности средств связи и информации, таможни, природоохранные органы, органы охраны здоровья населения и другие государственные органы обеспечения безопасности | *Закон РФ от 05.03.92 №2446-1 «О безопасности», ст. 12* |
| Система безопасности | Органы законодательной, исполнительной и судебной властей, государственные, общественные и иные организации и объединения, граждане, принимающие участие в обеспечении безопасности в соответствии с законом, а также законодательство, регламентирующее отношения в сфере безопасности | *Федеральный закон от 05.03.92 №2446-1 «О безопасности», ст. 8* |
| Система защиты государственной тайны | Совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях | *Закон РФ от 21.07.93 №5485-1 «О государственной тайне» в ред. Федерального закона от 06.10.97 № 131-ФЗ, ст. 2* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Система защиты информации | Совокупность органов и (или) исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации | *ГОСТ Р 30922-96. «Защита информации. Основные термины и определения»* |
| Система обеспечения информационной безопасности РФ | Часть системы обеспечения национальной безопасности страны. Основными элементами организационной основы системы обеспечения информационной безопасности РФ являются: Президент РФ, Совет Федерации Федерального Собрания РФ, Государственная Дума Федерального Собрания РФ, Правительство РФ, Совет Безопасности РФ, федеральные органы исполнительной власти, межведомственные и государственные комиссии, создаваемые Президентом РФ и Правительством РФ, органы исполнительной власти субъектов РФ, органы местного самоуправления, органы судебной власти, общественные объединения, граждане, принимающие в соответствии с законодательством РФ участие в решении задач обеспечения информационной безопасности РФ. Президент РФ - руководит ... органами и силами по обеспечению информационной безопасности РФ; санкционирует действия по обеспечению информационной безопасности РФ; ... формирует, реорганизует и упраздняет подчиненные ему органы и силы по обеспечению информационной | *Доктрина информационной безопасности РФ, 2000 г.* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| | безопасности РФ; определяет в своих ежегодных посланиях Федеральному Собранию приоритетные направления государственной политики в области обеспечения информационной безопасности РФ, а также меры по реализации настоящей Доктрины<br>Палаты Федерального Собрания РФ - ...формируют законодательную базу в области обеспечения информационной безопасности РФ.<br>Правительство РФ - ... координирует деятельность федеральных Органов исполнительной власти и органов исполнительной власти субъектов РФ, а также при формировании... проектов федерального бюджета на соответствующие годы предусматривает выделение средств, необходимых для реализации федеральных программ в этой области.<br>Совет Безопасности РФ - проводит работу по выявлению и оценке угроз информационной безопасности РФ, оперативно подготавливает проекты решений Президента РФ по предотвращению таких угроз, разрабатывает предложения в области обеспечения информационной безопасности РФ, а также предложения по уточнению отдельных положений настоящей Доктрины, координирует деятельность органов и сил по обеспечению информационной безопасности РФ, контролирует реализацию федеральными органами исполнительной власти и органами исполнительной власти субъектов РФ решений Президента РФ в этой области. | |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| | Федеральные органы исполнительной власти - обеспечивают исполнение законодательства РФ, решений Президента РФ и Правительства РФ в области обеспечения информационной безопасности РФ; ... разрабатывают нормативные правовые акты в этой области ...<br>Межведомственные и государственные комиссии Федерации - решают ... задачи обеспечения информационной безопасности РФ.<br>Органы исполнительной власти субъектов РФ - взаимодействуют с федеральными органами исполнительной власти по вопросам исполнения законодательства РФ, решений Президента РФ и Правительства РФ в области обеспечения информационной безопасности РФ, а также по вопросам реализации федеральных программ в этой области; совместно с органами местного самоуправления осуществляют мероприятия по привлечению граждан, организаций и общественных объединений к оказанию содействия в решении проблем обеспечения информационной безопасности РФ; вносят в федеральные органы исполнительной власти предложения по совершенствованию системы обеспечения информационной безопасности РФ.<br>Органы местного самоуправления - обеспечивают соблюдение законодательства РФ в области обеспечения информационной безопасности РФ.<br>Органы судебной власти - осуществляют правосудие по делам о преступлениях, связанных с посяя- | |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| | гательствами на законные интересы личности, общества и государства в информационной сфере, и обеспечивают судебную защиту граждан и общественных объединений, чьи права были нарушены в связи с деятельностью по обеспечению информационной безопасности РФ | |
| Система обеспечения национальной безопасности РФ | Органы, силы и средства обеспечения национальной безопасности, осуществляющие меры политического, правового, организационного, экономического, военного и иного характера, направленные на обеспечение безопасности личности, общества и государства | *Указ Президента РФ от 10 января 2000 г. №24 «О концепции национальной безопасности»* |
| Система обязательного экземпляра | Совокупность видов обязательных экземпляров, а также установленный порядок их собирания, распределения и использования | *Федеральный закон от 29.12.94 № 77-ФЗ «Об обязательном экземпляре документов», ст. 1* |
| Система разграничения доступа | Совокупность реализуемых правил разграничения доступа в средствах вычислительной техники или автоматизированных системах | *Сборник руководящих документов по защите информации от несанкционированного доступа Государственной технической комиссии при Президенте РФ, 1998 г.* |
| Система сертификации средств защиты информации | Совокупность участников сертификации, осуществляющих ее на основании требований государственных стандартов, нормативных документов, утверждаемых Правительством РФ и федеральными органами по сертификации в пределах их компетенции | *Постановление Правительства РФ от 26.06.95 №608* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Служба внешней разведки РФ | Орган внешней разведки, который может при собственных лицензировании и сертификации приобретать, разрабатывать (за исключением криптографических средств защиты), создавать, эксплуатировать информационные системы, системы связи и системы передачи данных, а также средства защиты информации от утечки по техническим каналам. Служба внешней разведки РФ в пределах своих полномочий осуществляет разведывательную деятельность в политической, экономической, военно-стратегической, научно-технической и экологической сферах, а также в сфере обеспечения безопасности учреждений РФ, граждан РФ, имеющих по роду своей деятельности допуск к сведениям, составляющим государственную тайну | *Федеральный закон от 10.01.96 № 5-ФЗ «О внешней разведке», п. 12, ст. 6 и п. 1 ст. 11* |
| Служебная информация | Любая не являющаяся общедоступной информация об эмитенте и выпущенных им эмиссионных ценных бумагах, которая ставит лиц, обладающих в силу своего служебного положения, трудовых обязанностей или договора, заключенного с эмитентом, такой информацией, в преимущественное положение по сравнению с другими субъектами рынка ценных бумаг | *Федеральный заколот 22.04.96 № 39-ФЗ «О рынке ценных бумаг», ст. 31* |
| Служебная информация ограниченного распространения | Несекретная информация, касающаяся деятельности организаций, ограничения на распространение которой диктуются служебной необходимостью. | *Постановление Правительства РФ от 03.11.94 № 1233* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Служебная или коммерческая тайна | Информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании и обладатель информации принимает меры, к охране ее конфиденциальности. Сведения, которые не могут составлять служебную или коммерческую тайну, определяются законом и иными правовыми актами | *Гражданский кодекс РФ от 3.11.94 №31-ФЗ «Гражданский кодекс Российской Федерации», ст. 139* |
| Служебное произведение | Произведение, созданное в порядке выполнения служебных обязанностей или служебного задания | *Закон РФ от 09.07.93 №5351-1 «Об авторском праве и смежных правах», ст. 14* |
| Служебный подлог | Внесение должностным лицом, а также государственным служащим или служащим органа местного самоуправления, не являющимся должностным лицом, в официальные документы заведомо ложных сведений, а равно внесение в указанные документы исправлений, искажающих их действительное содержание, если эти деяния совершены из корыстной или иной личной заинтересованности | *Уголовный кодекс РФ от 13.06.96 М63-ФЗ, ст. 32* |
| Смежные права | [совокупность правовых норм], регулирующих отношение, возникающие в связи с созданием и использованием фонограмм, исполнений, постановок, передач, организации эфирного или кабельного вещания (смежные права) | *Федеральный закон от 09.07.93 № 535 ]-1 (в ред, от 19.07.95 №110-ФЗ)* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Собственник документированной информации, информационных ресурсов, информационных продуктов и(или) средств международного информационного обмена | Субъект, реализующий полномочия владения, пользования, распоряжения указанными объектами в объеме, устанавливаемом законом | *Федеральный закон от 04.07.96 №85-ФЗ «Об участии в международном информационном обмене», ст. 2* |
| Собственник информации | Субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами | *ГОСТ Р 50922-96. Защита информации. Основные термины и определения. (Прил. А)* |
| Собственник информационных ресурсов, информационных систем, технологий и средств их обеспечения | Субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения указанными объектами | *Федеральный закон от 20.02.95 N9 24-03 «Об информации, информатизации и защите информации», ст. 2* |
| Совет Безопасности РФ | Конституционный орган, осуществляющий подготовку решений Президента РФ в области обеспечения безопасности, рассматривающий вопросы внутренней и внешней политики РФ в области обеспечения безопасности, стратегические проблемы государственной, экономической, общественной, оборонной, информационной, экологической и иных видов безопасности, охраны здоровья населения, прогнозирования, предотвращения чрезвычайных ситуаций и преодоления их последствий, обеспечения стабильности и правопорядка | *Закон РФ от 05.03.92 №2-146-1 «О безопасности», ст. 13* |
| Совет Безопасности РФ | Проводит работу по упреждающему выявлению и оценке угроз национальной безопасности РФ, оперативно готовит для Президента РФ проекты решений по их | *Указ Президента РФ от 10 января 2000 г. №24 «О концепции национальной безопас-* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| | предотвращению, разрабатывает предложения в области обеспечения национальной безопасности РФ, а также предложения по уточнению отдельных положений Концепции национальной безопасности РФ, координирует деятельность сил и останов обеспечения национальной безопасности, контролирует реализацию федеральными органами исполнительной власти и органами исполнительной власти субъектов РФ решений в этой области | *ности»* |
| Совет Безопасности РФ | Конституционный орган, осуществляющий подготовку решений Президента РФ по вопросам обеспечения защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, проведения единой государственной политики в области обеспечения безопасности | *Положение, утвержденное Указом Президента РФ от 10.07.96 № 1024, п. 4* |
| Сообщать [в области авторского права и смежных прав] | Показывать, исполнять, передавать в эфир или совершать иное действие (за исключением распространения экземпляров произведения или фонограммы), посредством которого произведения, фонограммы, исполнения, постановки, передачи организации эфирного или кабельного вещания становятся доступными для слухового и(или) зрительного восприятия, независимо от их фактического восприятия публикой | *Закон РФ от 09:07.93 №5351-1 «Об авторском праве и смежных правах», ст. 4* |
| Сообщать для всеобщего сведения по кабелю [в области авторского права и смежных прав] | Сообщать произведения, фонограммы, исполнения, постановки, передачи организаций эфирного или кабельного вещания для всеобщего сведения посредством кабеля, провода, оптического волокна или с помощью аналогичных средств | *Закон РФ от 09.07.93 №5351-1 «Об авторском праве и смежных правах», ст. 4* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Составитель (в области авторского права) | Автор сборника и других составных произведений; составительство - подбор или расположение материалов, представляющие результат творческого труда | *Закон РФ от 09.07.93 №5351-1 «Об авторском праве и смежных правах», ст. 11* |
| Специализированное средство массовой информации | Такое средство массовой информации, для регистрации или распространения продукции которого настоящим Законом установлены специальные правила | *Закон РФ от 27.12.91 №2124-1 «О средствах массовой информации», ст. 2* |
| Специальная информация | Материалы внешней разведывательной деятельности, информация по поддержанию управления народным хозяйством в особый период, военное время и при чрезвычайных ситуациях, экономическая информация мобилизационного назначения, информация социально-экономического мониторинга, необходимые для принятия решений в области безопасности, обороны, экономики, науки и техники, международных отношений, экологии, а также мобилизационной готовности | *Закон РФ от 19.02.93 №-1524-1 «О Федеральных органах правительственной связи и информации», ст. 3* |
| Специальная и защищенная база данных | База данных, содержащая сведения, отнесенные в установленном порядке к государственной тайне | *Временное положение, утвержденное постановлением Правительства РФ от 28.02.96 №226, п. 5.1* |
| Способ защиты информации | Порядок и правила применения определенных принципов и, средств защиты информации | *ГОСТ Р 50922-96. Защита информации. Основные термины и определения* |
| Средства электронной цифровой подписи | Аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций - создание электронной цифровой подписи в электронном документе с исполь- | *Федеральный закон РФ от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи»* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| | зованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей | |
| Средства защиты информации | Технические, криптографические, программные и другие средства, предназначенные для защиты сведений, «составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации | *Закон РФ от 21.07.93 №5485-1 «О государственной тайне» вред. Федерального закона от 06.10.97 № 131-ФЗ, ст. 2* |
| Средство защиты информации | Техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации | *ГОСТ Р 50922-96. Защита информации. Основные термины и определения* |
| Средства контроля эффективности защиты информации | Техническое, программное средство, вещество и/или материал, предназначенные или используемые для контроля эффективности защиты информации | *ГОСТ Р 50922-96. Защита информации. Основные термины и определения* |
| Средства массовой информации | Периодическое печатное издание, радио-, теле-, видеопрограмма, кинохроникальная программа, иная форма периодического распространения массовой информации | *Закон РФ от 27.12.91 №2124-1 «О средствах массовой информации», ст. 2; Федеральный закон от 01.12.93 №191-ФЗ «О государственной поддержке средств массовой информации и книгоиздания Российской Федерации», ст. 1* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Средства массовой информации рекламного характера | Средство массовой информации, в котором реклама превышает 40 процентов объема отдельного номера периодического издания, а в теле-, радиопрограммах - 25 процентов объема вещания | *Федеральный закон от 01.12.95 № 191-ФЗ «О государственной поддержке средств массовой информации и книгоиздания Российской Федерации», ст. 1* |
| Средства массовой информации эротического характера | Периодическое печатное издание или теле-, радиопрограмма, которые в целом и систематически эксплуатируют интерес к сексу | *Федеральный закон от 01.12.95 № 191-ФЗ «О государственной поддержке средств массовой информации и книгоиздания Российской Федерации», ст. 1* |
| Средства международного информационного обмена | Информационные системы, сети и сети связи, используемые при международном информационном обмене | *Федеральный закон от 04.07.96 №85-ФЗ «Об участии в международном информационном обмене», ст. 2* |
| 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 | *Федеральный закон от 20.02.95 № 24-ФЗ «Об информации, информатизации и защите информации», ст. 2* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Средства почтовой связи | Здания, сооружения, нежилые помещения, оборудование и почтовый транспорт, почтовые конверты и почтовая тара, используемые для оказания услуг почтовой связи | *Федеральный закон от 17.07.99 №176-ФЗ «О почтовой связи», ст. 2* |
| Средства связи | Технические средства, используемые для формирования, обработки, передачи или приема сообщений электросвязи либо почтовых отправлений | *Федеральный закон от 16.02.95 № 15-ФЗ «О связи», ст. 2* |
| Срок засекречивания сведений, составляющих государственную тайну | Не должен превышать 30 лет. В исключительных случаях этот срок может быть продлен по заключению межведомственной комиссии по защите государственной тайны | *Закон РФ от 21.07.93 №5485-1 «О государственной тайне» вред. Федерального закона от 06.10.97 № 131-ФЗ, ст. 13* |
| Стандарт | Государственный стандарт, санитарные нормы и правила, строительные нормы и правила и другие документы, которые в соответствии с законом устанавливают обязательные требования к качеству товаров (работ, услуг) | *Закон РФ от 0702.92 №2300-1 «О защите прав потребителей», (в рад. Федерального закона от 09.01.96 №2-ФЗ, преамбула)* |
| Стандартизация | Деятельность по установлению норм, правил и характеристик... в целях обеспечения: безопасности продукции, работ и услуг для окружающей среды, жизни, здоровья и имущества; технической и информационной совместимости, а также взаимозаменяемости продукции; качества продукции, работ и услуг в соответствии с уровнем развития науки, техники и технологии, единства измерений; экономии всех видов ресурсов; безопасности хозяйственных субъектов с учетом риска возникновения природных и техногенных катастроф и других чрезвычайных ситуаций; обороноспособности и мобилизационной готовности страны | *Закон Российского Федерации от 10.06.93 №515-1-1 «О стандартизации», ст. 1* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Степень секретности сведений, составляющих государственную тайну | Должна соответствовать степени тяжести ущерба, который может быть нанесен безопасности РФ вследствие распространения указанных сведений. Устанавливаются три степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведений: «особой важности», «совершенно секретно» и «секретно» | *Закон РФ от 21.07.93 №5485-1 «О государственной тайне» вред. Федерального закона от 06.10.97 № 131-ФЗ, ст. 8* |
| Страховой фонд документации | Создание и сохранение страхового фонда документации на вооружение и военную технику, важнейшую гражданскую продукцию, объекты повышенного риска, системы жизнеобеспечения населения и объекты, являющиеся национальным достоянием, входит в содержание мобилизационной подготовки и мобилизации в РФ | *Федеральный закон от 26.02.97 № 31-ФЗ «О мобилизационной подготовке и мобилизации в Российской Федерации», ст. 1* |
| Субъект доступа (к информации) | Субъект доступа: участник правоотношение в информационных процессах | *ГОСТ Р 50922-96. Защита информации. Основные термины и определения. (Прил. А)* |
| Субъект доступа | Лицо или процесс, действие которого регламентируется правилами разграничения доступа | *Сборник руководящих документов по защите информации от несанкционированного доступа Государственной технической комиссии при Президенте РФ, 1998 г.* |
| Субъекты безопасности | Граждане, общественные организации и объединения, обладающие правами и обязанностями по участию в обеспечении безопасности | *Закон РФ от 05.03.92 №2-146-1 «О безопасности»* |

| *Термин* | *Определение* | *Источнык* |
|---|---|---|
| Субъекты смежных прав | Исполнители, производители фонограмм, организации эфирного или кабельного вещания | *Закон РФ от 09.07.93 №5351-1 «Об авторском праве и смежных правах», ст. 36* |
| Тайна (почтовой) связи | Тайна переписки, почтовых, телеграфных и иных сообщений, входящих в сферу деятельности операторов почтовой связи, не подлежащая разглашению без согласия пользователя услуг почтовой связи.<br>Информация об адресных данных пользователей услуг почтовой связи, о почтовых отправлениях, почтовых переводах денежных средств, телеграфных и иных сообщениях, входящих в сферу деятельности операторов почтовой связи, а также сами эти почтовые Отправления, переводимые денежные средства, телеграфные и иные сообщения являются тайной связи и могут выдаваться только отправителям (адресатам) или их представителям | *Федеральный закон от 17.07.99 №176-ФЗ «О почтовой связи», ст. 2, 15* |
| Тайна связи | Тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, входящих в сферу деятельности операторов почтовой связи, не подлежащая разглашению без согласия пользователя услуг почтовой связи | *Федеральный акон от 17.07.99 № 176-ФЗ«0 почтовой связи», ст. 1* |
| Тайна связи | Тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электрической и почтовой связи, охраняется Конституцией РФ.<br>*Примечание.* Ограничения тайны связи: Прослушивание телефонных переговоров, ознакомление с сообщениями электросвязи, за- | *Федеральный закон от 16.02.95 №15-ФЗ «О связи», ст. 32* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| | держка, осмотр и выемка почтовых отправлений и документальной корреспонденции, получение сведений о них, допускаются только на основании судебного решения и др. | |
| Тайный архив | Архив, о котором не заявлено публично | *Основы законодательства РФ об Архивном фонде РФ и архивах от 07.07.93 М 5341-1 ст. 1* |
| Телерадиокомпания, осуществляющая вещание на территорию избирательного округа | Телерадиокомпания, зона уверенного приема теле-, радиопрограмм которой находится в пределах соответствующего избирательного округа либо примерно совпадает с его границами | *Положение, утвержденное Указом Президента РФ от.29. 10. 93 Ns 1792, п. 2* |
| Терроризм | Совершение взрыва, поджога или иных действий, создающих опасность» гибели людей, причинения значительного имущественного ущерба либо наступления иных общественно опасных последствий, если эти действия совершены в целях нарушения общественной безопасности, устрашения населения либо оказания воздействия на принятие решений органами власти, а также угроза совершения указанных действий в тех же целях | *Уголовный кодекс Российский Федерации от 13.06.96 № 63-ФЗ, ст. 203* |
| Техника защиты информации | Средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные дда обеспечения, защиты информации | *ГОСТ Р 50922-96: Защити информации- Основные термины и определения.* |
| Технический контроль эффективности защиты информации | Контроль эффективности защиты информации, проводимой с использованием средств контроля | *ГОСТ Р 50922-96 Защита информацыи. Основные термины и определения* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Топология интегральной микросхемы | Зафиксированное на материальном носителе пространственно-геометрическое расположение совокупности элементов интегральной микросхемы и связей между ними | *Закон РФ от 23.09.92 № 3526-1 «О правовой охране топологии интегральных микросхем», ст. 1* |
| Трафик | Совокупность сообщений, передаваемых по сети электросвязи | *Правила, утвержденные постановлением Правительства РФ от 19.10.96 № 1254, ст. 2* |
| Третейский информационный суд [при проведении избирательной кампании 1993 г.] | Состоит из 9 членов, назначаемых Президентом РФ из числа специалистов, не являющихся членами какого-либо избирательного объединения, кандидатами в депутаты Государственной думы или Совета Федерации либо их доверенными лицами | *Положение об информа ционных гарантиях предвыборной агитации, утвержденное Указом Президента РФ от 29.10.93 №1792, п. 9* |
| Угрозы безопасности | Совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства | *Закон РФ от 05.03.92 №2-146-1 «О безопасности», ст. 3* |
| Угрозы информационной безопасности Российской Федерации (виды) | Угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России; угрозы информационному обеспечению государственной политики РФ; угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности | *Доктрина информационной безопасности РФ, 2000 г.* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| | и эффективного использования отечественных информационных ресурсов; угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России | |
| Угрозы национальной безопасности РФ в информационной сфере | Стремление ряда стран к доминированию в мировом информационном пространстве, вытеснению России с внешнего и внутреннего информационного рынка; разработка рядом государств концепции информационных войн, предусматривающей создание средств опасного воздействия на информационные сферы других стран мира; нарушение нормального функционирования информационных и телекоммуникационных систем, а также сохранности информационных ресурсов, получение несанкционированного доступа к ним | *Указ Президента РФ от 10 января 2000 г. №2-1 «О концепции национальной безопасности»* |
| Услуги почтовой связи | Действия или деятельность по приему, обработке, перевозке, доставке (вручению) почтовых отправлений, а также по осуществлению почтовых переводов денежных средств | *Федеральный закон от 17. 07.99 №176-ФЗ«0 почтовой связи», ст. 2* |
| Услуги связи | Продукт деятельности по приему, обработке, передаче и доставке почтовых отправлений или сообщений электросвязи | *Федеральный законом 16.02.95 № 15-ФЗ «О связи», ст. 2* |
| Услуги телеграфной связи | Результат деятельности хозяйствующего субъекта в сфере оказания услуг телеграфной связи | *Правила, утвержденные по становлением Правительства РФ от 23.04.94 №374, п. 3 (утр. силу 28.08.97 №1108)* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Утечка информации | Неконтролируемое распространение защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации разведкой | *ГОСТ Р 30922-96. Защита информации. Основные термины и определения* |
| Учреждения связи | См.: Предприятия, учреждения и организации связи | |
| Федеральное агентство правительственной связи и информации при Президенте РФ (ФАПСИ) | Центральный орган федеральной исполнительной мести, ведающий вопросами организации и обеспечения правительственной связи, иных видов специальной связи для государственных органов, организации и обеспечения криптографической и инженерно-технической безопасности шифрованной связи, организации и ведения разведывательной деятельности в сфере шифрованной, засекреченной и иных видов специальной связи, специального информационного обеспечения высших органов государственной власти РФ, центральных органов федеральной исполнительной власти | *Закон РФ от J 9.02.93 №4524-1 «О федеральных органах правительственной связи и информации», ст. 6* |
| Федеральные органы правительственной связи и информации | Составная часть сил обеспечения безопасности РФ, обеспечивающая государственные органы, организации, предприятия, учреждения специальными видами связи и информации, а также организующая деятельность центральных органов федеральной исполнительной власти, организаций, предприятий, учреждений по обеспечению криптографической и инженерно-технической безопасности шифрованной связи в РФ и ее учреждениях за рубежом, осуществляющая государственный контроль за этой деятельностью | *Закон РФ от 19.02.93 №4524-1 «О федеральных органах правительственной связи и информации». ст.1* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Фонограмма | Любая исключительно звуковая запись исполнений или иных звуков | *Закон РФ от 09.07.93 №5351-1 «Об авторском праве и смежных правах», ст. 4* |
| Целостность информации | Способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и (или) преднамеренного искажения (разрушения) | *Сборник руководящих документов по защите информации от несанкционированного доступа Государст венной технической комиссии при Президенте РФ, 1998 г.* |
| Цель защиты информации | Желаемый результат защиты информации. *Примечание.* Целью защиты информации может быть предотвращение ущерба собственнику, владельцу, пользователю информации в результате возможной утечки информации и (или) несанкционированного и непреднамеренного воздействия на информацию | *ГОСТ Р 50922-96. Защита информации. Основные термины и определения* |
| Цензура массовой информации | Требование от редакции средства массовой информации со стороны должностных лиц, государственных органов, организаций, учреждений или общественных объединений предварительно согласовывать сообщения и материалы (кроме случаев, когда должностное лицо является автором или интервьюируемым), а равно наложение запрета на распространение сообщений и материалов, их отдельных частей | *Закон РФ от 27.12.91 №2124-1 «О средствах массовой информации», ст. 3* |
| Централизованная библиотечная система | Добровольное объединение библиотек в структурно-целостное образование | *Федеральный закон от 29.12.94 № 78-ФЗ «О библиотечном деле», ст. 1* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Чрезвычайная ситуация | Это обстановка на определенной территории, сложившаяся в результате аварии, опасного природного явления, катастрофы, стихийного или иного бедствия, которые могут повлечь или повлекли за собой человечески жертвы, ущерб здоровью людей или окружающей природной среде значительные материальные потери и нарушение условий жизнедеятельности людей | *Федеральный закон от 21.12.94 № 68-ФЗ «О защите населения и территории от чрезвычайных ситуации природного и техногенного характера», ст. I; Типовое соглашение о сотрудничестве в области предупреждения и ликвидации чрезвычайных ситуаций, одобренное постановлением Правительства РФ от 30.04.97 №516, ст. I* |
| Чрезвычайное положение, вводимое на всей либо на части территории РСФСР | Особый правовой режим деятельности органов государственной власти и управления, предприятий, учреждений и организаций, допускающий установленные настоящим Законом ограничения прав и свобод граждан и прав юридических лиц, а также возложение на них дополнительных обязанностей. Чрезвычайное положение является временной мерой и может вводиться исключительно в интересах обеспечения безопасности граждан и охраны конституционного строя республики | *Закон РСФСР от 17.05.91 №1253-1 «О чрезвычайном положении», ст. 1* |
| Экземпляр произведения | Копия произведения, изготовленная в любой материальной форме | *Закон РФ от 09.07.93 №5351-1 «Об авторском праве и смежных правах», ст. 4* |

| *Термин* | *Определение* | *Источник* |
|---|---|---|
| Экземпляр фонограммы | Копия фонограммы на любом материальном носителе, изготовленная непосредственно или косвенно с фонограммы и включающая все звуки или часть звуков, зафиксированных в этой фонограмме | *Закон РФ от 09.07.93 №5351-1 «Об авторском праве и смежных правах», ст. 4* |
| Электронный документ | Документ, в котором информация представлена в электронно-цифровой форме | *Федеральный закон РФ от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи»* |
| Электронная цифровая подпись | Реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе | *Федеральный закон РФ от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи»* |
| Эффективность защиты информации | Степень соответствия результатов защиты информации поставленной цели | *ГОСТ Р 0922-96. Защита информации. Основные термины и определения* |

# Приложение 11

# ТЕРМИНЫ ПО ЗАЩИТЕ ИНФОРМАЦИИ

Термины расположены в алфавитном порядке по первому слову. Прямым шрифтом в круглых скобках приведены факультативные элементы терминов, в квадратных скобках - синонимические варианты предшествующего элемента или группы элементов; *adj* - прилагательное или причастие, v - глагол.

| | |
|---|---|
| Access control | Контроль доступа, управление доступом |
| Access method | Метод доступа |
| Access mode | Режим доступа |
| Access right | Право доступа |
| Access scan | Поиск с перебором |
| Adversary | См.: attacker |
| Amplification | Расширение прав |
| Asymmetric encryption | Асимметрическое шифрование |
| Asynchronous attack | Шифрование типа «асинхронная атака» |
| Attack | Попытка раскрытия (криптосистемы), криптоанализ |
| Attacker | Нарушитель, противник |
| Audit log | Журнал ревизии |
| Authenti(fi)cation | 1. Аутентификация, опознавание.<br>2. Подтверждение права на доступ.<br>3. Проверка подлинности |
| Authenti(fi)cation code | Код аутентификации |
| Authenti(fi)cation of message | Аутентификация сообщения |
| Authenti(fi)cation of user | Аутентификация пользователя |
| Authentication problem | Проблема проверки на достоверность |
| Authorization | 1. Разрешение, предоставление права на доступ.<br>2. Проверка полномочий.<br>3. Авторизация |
| Authorized access | Санкционированный доступ |
| Authorized user | 1. Зарегистрированный пользователь.<br>2. Привилегированный пользователь |
| Auxiliary key | Вторичный ключ |

| | |
|---|---|
| Birthday attack | Криптоанализ на основе парадокса дней рождения |
| Block chaining | Сцепление блоков |
| Block encryption | Блочное шифрование |
| Candidate key | Возможный ключ |
| Capabilities list | Список полномочий (мандатов) |
| Capability | Полномочия, мандат |
| Capability-based addressing | Адресация по полномочиям |
| Certification | Освидетельствование |
| Central keying authority | Центр распределения [распространения, управления] ключей, ЦРК |
| Chained key | Сцепленный ключ (в базах данных) |
| Challenge and response procedure | Процедура запроса и подтверждения |
| Cheating | Обман |
| Cipher I | Шифр, код |
| Cipher II, v | Шифровать, кодировать |
| Cipherer | Шифратор, кодирующее устройство |
| Ciphertext | Шифротекст |
| CKA | См.: central keying authority |
| Classical cipher | Классический шифр |
| Clear text | Исходный текст |
| Code | Код (метод преобразования открытого текста в криптограмму путем использования кодовых таблиц) |
| Common system area | Общая системная область защиты |
| Computational compexity | Вычислительная сложность |
| Computer security | Защита [защищенность] ЭВМ от несанкционированного доступа |
| Concatenated key | См.: chained key |
| Conceptual integrity | Концептуальная целостность [последовательность, согласованность] |
| Confinement | Изоляция |
| Consistency | Целостность, непротиворечивость |
| Control Program Facility | Управляющая программа |
| CPF | См.: Control Program Facility |
| Cryptanalysis | Криптоанализ, анализ шифра (метод раскрытия кода или шифра) |
| Cryptanalyst | Дешифровальщик |

| | |
|---|---|
| Criptography | Криптография |
| Crypto logy | Криптология (сочетание криптографии и криптоанализа) |
| Cryptosystem | Криптографическая система |
| CSA | См.: common system area |
| DAM | См.: direct access method |
| Data corruption | Нарушение целостности данных |
| Data Encryption Standard | Стандарт на шифрование данных |
| Data integrity | Целостность [сохранность, неискаженность, подлинность] данных |
| Data protection | Защита данных |
| Data security | Защита [защищенность] информации [данных] (от несанкционированного доступа) |
| Data set | Набор данных |
| Decipher, v | Расшифровывать; декодировать |
| Decryption | Расшифрование, дешифрование, декодирование |
| Decryption key | Ключ расшифрования |
| Denial-of-access external security | Внешняя безопасность на основе лишения доступа |
| DES | См.: Data Encryption Standard |
| Detection mechanism | Система [устройства] обнаружения |
| Digital signature | Цифровая подпись |
| Direct access method | Прямой метод доступа |
| Division of responsibilities | Разделение обязанностей |
| Eavesdropper | Пассивный нарушитель, перехватчик |
| Encipherer | Шифратор, кодирующее устройство |
| Enciphering key | Ключ шифрования |
| Encode, v | Шифровать, кодировать |
| Encoder | 1. Кодер, кодирующее устройство.<br>2. Кодировщик, шифровальщик |
| Encription | (За)шифрование |
| Encription key | Ключ шифрования |
| Endorsment | Аттестация |
| End-to-end | Сквозное шифрование |
| Essential undecidability | Существенная неразрешимость |
| Exposure | Незащищенность (данных), подверженность (данных постороннему воздействию) |

| | |
|---|---|
| External security | Внешняя защита |
| Extra key | Дополнительный ключ (поиска) |
| Forger | Фальсификатор, подделыватель (подписи, документа и т. д.) |
| Forgery | 1. Подделка, подлог.<br>2. Фальшивый документ.<br>3. Подложная подпись |
| Geeric key | Общий ключ; общая часть ключа |
| Geeric operation | Типовая операция |
| Geeric system functional flaw | Типовой функциональный дефект |
| Hardware security | Аппаратная защита |
| Identification | 1. Идентификация (процесс отождествления объекта с одним из известных системе объектов; опознавание выдавшего запрос пользователя, канала или процесса).<br>2. Метка, идентифицирующая объект |
| Identify, v | 1. Идентифицировать, распознавать, опознавать.<br>2. Обозначать, именовать |
| Implementation standard | Стандарт реализации |
| Inconsistency | Нарушение целостности, противоречивость |
| Infinite random key | Неопределенный рандомизированный ключ (шифра) |
| Insecure channel | Незащищенный канал |
| Insider | Пользователь (системы, в системе) |
| Intended receiver | Санкционированный получатель |
| Integrity | Целостность, сохранность (данных) |
| Interface standard | Стандарт взаимодействия |
| Internal security | Внутренняя безопасность [защита] |
| Interoperability | Функциональная совместимость, стандарт на функциональную совместимость |
| Intruder | Нарушитель, злоумышленник (пользователь или программа, пытающиеся получить несанкционированный доступ к данным); см. также attacker |
| KDC | См.: key distribution cente |
| Key | Ключ |
| Key distribution | Распределение [распространение, доставка, передача] ключей, ЦРК |
| Key field | Поле ключа |

| | |
|---|---|
| Key management | Управление ключами |
| Key notarization | Нотаризация нотариальное засвидетельствование] ключа |
| Key protection | Защита по ключу |
| Key-sequenced data set | Набор данных, упорядоченный по поступлению ключей записей |
| Key-verify | Контролировать (данные) повторным набором на клавиатуре |
| Knapsack cryptosystem | Ранцевая криптосистема |
| Legality checking | Проверка законности |
| Legitimate user | Законный пользователь |
| Link encryption | Шифрование передач по линиям (каналам) связи |
| Lost object problem | Проблема утери объектов |
| Major key | Главный (первичный] ключ |
| Model validation | Обоснование модели |
| Monitoring | Проверка, контроль |
| Multiple-key retrieval | Выборка [поиск] по нескольким ключам |
| Operating system penetration | Преодоление защиты операционной системы |
| Operator spoof | Обман оператора |
| Pass key | Ключ (для) доступа |
| Password sutentication | Идентификация по паролю |
| Password protection | Защита паролями |
| Penetration entrapment | Ловушка для злоумышленников [нарушителей] |
| Penetration work factor | Объем работы по преодолению защиты |
| Physical security | Физическая защита [защищенность] |
| Piggyback | Паразитирование |
| Plaintext | Открытый текст, исходный текст |
| Primary key | Первичный [главный] ключ |
| Privacy | Секретность, конфиденциальность |
| Privacy problem | Проблема сохранения тайны |
| Privacy key | Секретный ключ |
| Privacy key encryption | Шифрование по закрытым ключам в криптосистеме с открытыми ключами |
| Privilege violation | Нарушение полномочий |
| Problem of dispute | Проблема подтверждения отправителя |
| Protection against disasters | Защита от бедствий |

| | |
|---|---|
| Protection against intruders | Защита от злоумышленников |
| Protection domain | Область защиты |
| Protection key | Ключ защиты (памяти) |
| Private, adj | Секретный |
| Private exponent | Секретный показатель степени |
| Public key | Открытый ключ |
| Public key encryption | Шифрование с открытыми ключами |
| Public, adj | Открытый |
| Public exponent | Открытый показатель степени |
| Public key system | Криптосистема с открытым ключом |
| Recursive unsolvability | Рекурсивная неразрешимость |
| Revocation of capability | Отмена полномочий |
| Receiver | Получатель |
| Risk management | Управление риском |
| Satisfiability | Выполнимость (требований) |
| Secondary key | Вторичный ключ |
| Secrecy | Секретность |
| Secure data storage | Надежное хранение данных |
| Security | Безопасность, защита, защищенность, стойкость |
| Security suditing | Проверка защиты, проверка на стойкость |
| Security requirement | Требование по безопасности [защите] |
| Security standard | Стандарт по защите от несанкционированного доступа |
| Sensitive, adj | Конфиденциальный (об информации) |
| Sign I | 1. Признак.<br>2. Обозначение.<br>3. Знак (при числе).<br>4. Заверение (документа или данных) |
| Sign II, v | 1. Подписывать(ся).<br>2. Заверять |
| Signature | Сигнатура, подпись |
| Sound protocol | Надежный протокол |
| Space object | Объект памяти |
| Storage key | 1. Ключ хранения (в базах данных).<br>2. Ключ защиты памяти |
| Storage protection | Защита памяти |
| Storage protection key | Ключ защиты памяти |

| | |
|---|---|
| Stream encryption | Поточное шифрование |
| Strong cryptoalgoritm | Стойкий криптоалгоритм |
| Substitution cipher | Шифр подстановки |
| Surveillance | Надзор (наблюдение за работой системы), ревизия, идентификация (подтверждение права доступа) |
| Surveilance program | Программы контроля |
| Survivable system | Живучая система |
| Symmetric encryption | Симметричное шифрование |
| System pointer | Системный указатель [ссылка] |
| Threat monitoring | Профилактический контроль |
| Transparent multiprocessing | Прозрачная мультипроцессорная обработка |
| Transposition cipher | Перестановочный шифр |
| Trap | Ловушка, тайный ход |
| Trap door | Лазейка (слабое место, напр. в системе защиты), тайный ход |
| Trapping | Организация ловушек (в системе) |
| «Trojan Horse» | «Троянский конь» |
| Undecipherable | Не поддающийся расшифровке |
| Unauthorized, adj | 1. Несанкционированный (о действии, предпринятом пользователем или программой без соответствующих полномочий).<br>2. Непривилегированный (о пользователе или программе; не имеющих определенных прав) |
| Unauthorized access | Несанкционированный доступ |
| Undecidability | Неразрешимость |
| Unsolvability | Неразрешимость |
| User | Пользователь |
| User suthentification | Идентификация пользователя |
| User-defined key | Ключ пользователя; клавиша, программируемая пользователем |
| User interface security | Безопасность [защита] интерфейса с пользователем [пользовательского интерфейса] |
| User requirement | Требование пользователя (устанавливаемое пользователем) |
| User identification | См.: user authentification |
| User interface security | Безопасность интерфейса пользователя |
| Validation | Проверка правильности |
| Weak cryptoalgorithm | Нестойкий криптоалгоритм |

# ОГЛАВЛЕНИЕ

Е. Б. Белов, В. П. Лось,
Р. В. Мещеряков, А. А. Шелупанов

# Основы информационной безопасности

Изложены вопросы теории и практики обеспечения информационной безопасности личности, общества и государства. Большое внимание уделено проблеме безопасности автоматизированных систем, включая вопросы определения модели нарушителя и требований к защите информации. Анализируются современные способы и средства защиты информации и архитектура систем защиты информации.

В приложениях приведен справочный материал по ряду нормативных правовых документов и вариант рабочей программы по дисциплине «Основы информационной бе



ISBN 5-93517-292-5
9 785935 172923