Котухов М.М., Марков А.С.

ЗАКОНОДАТЕЛЬНО-ПРАВОВОЕ И ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

1998 г.

УДК [681.322.067+681.324](075.8)

КОТУХОВ Михаил Михайлович
МАРКОВ Алексей Сергеевич

ЗАКОНОДАТЕЛЬНО-ПРАВОВОЕ И ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Котухов М.М., Марков А.С. Законодательно-правовое и организационно-техническое обеспечение информационной безопасности автоматизированных систем. - 1998.- 158 с.

В книге изложены важнейшие современные направления законодательно-правового и организационно-технического обеспечения информационной безопасности автоматизированных систем. Освещены основные широко применяемые на практике законодательные и нормативные акты в области охраны государственной, служебной, коммерческой и других видов тайны. Рассмотрены вопросы лицензирования деятельности в области защиты информации и сертификации средств защиты, а также основанные на действующем законодательстве современные и перспективные организационно-технические методы и средства защиты информации в автоматизированных системах.

Предназначено для руководителей службы информационной безопасности организации, аналитиков и администраторов безопасности автоматизированных систем, а также студентам, изучающих курсы “Защита информации в вычислительных системах и информационно-телекоммуникационных сетях” и “Законодательство в области защиты информации”.

С О Д Е Р Ж А Н И Е

В В Е Д Е Н И Е

Проблема защиты информации от постороннего доступа и нежелательных воздействий на нее возникла практически на заре человечества. С развитием общественных отношений, появлением частной собственности, государственного строя, борьбой за власть и дальнейшим расширением масштабов человеческой деятельности информация приобретает все большую ценность. Наиболее ценной становится та информация, единоличное обладание которой позволяет ее владельцу получить какой-либо материальный, политический, военный и т.п. выигрыш [27, 70].

С переходом на использование технических средств связи информация подвергается воздействию неблагоприятных случайных процессов: неисправностей и сбоев аппаратуры, ошибок операторов и т.п., которые могут привести к ее разрушению, изменениям, потере, а также создать предпосылки для доступа к ней посторонних лиц.

С появлением автоматизированных систем и информационно-вычислительных сетей проблема защиты информации приобретает еще большее значение. Этому способствовали:

- повышение важности и общественной значимости информации, усиление ее влияния на все без исключения стороны общественной жизни;
- увеличение объемов информации, накапливаемой, хранимой и обрабатываемой с помощью ЭВМ и других средств вычислительной техники;
- сосредоточение в единых банках и базах данных информации различного назначения и принадлежности;
- расширение круга пользователей, имеющих доступ к ресурсам вычислительной системы и находящимся в ней массивам данных;
- усложнение режимов функционирования технических средств, широкое внедрение многопрограммного режима, режима разделения времени и реального времени;
- автоматизация межмашинного обмена информацией, в том числе и на большие расстояния;
- увеличение количества связей в автоматизированных и системах и сетях;
- появление персональных ЭВМ, расширяющих возможности не только пользователя, но и нарушителя.

В 1983 году Министерство обороны США выпустило книгу в оранжевой обложке с названием “Критерии оценки надежных компьютерных систем” (Trusted Computer Systems Evaluation Criteria, TCSEC) [76], положив тем самым начало систематическому распространению знаний об информационной безопасности за пределами правительственных ведомств. Во второй половине 1980-х годов аналогичные по назначению документы были изданы в ряде европейских стран.

В 1992 году в России Государственная техническая комиссия при Президенте РФ издала серию руководящих документов, посвященных проблеме защиты информации от несанкционированного доступа, средств вычислительной техники и автоматизированных систем [51-54], которые явились практически первыми в нашей стране открытыми изданиями, посвященными этой проблеме.

К настоящему времени и в самом человеческом обществе, и в технологии обработки данных произошли большие изменения, которые повлияли на саму суть проблемы защиты информации. Индустрия переработки информации достигла невиданного ранее масштаба.

Появилась возможность достаточно свободного выхода в глобальную информационно-вычислительную сеть с домашнего компьютера. Развитие системы “электронных денег” (кредитных карточек) создало предпосылки для хищений крупных сумм денег. Возникло целое направление специальных компьютерных злоумышленников “хэкеров” (hacker) - компьютерных хулиганов, получающие удовольствие от проникновения в чужой компьютер, и крэкеров (cracker) - похитителей информации, выкачивающих целые информационные банки данных. Широко распространились разнообразные программы-вирусы.

В печати регулярно сообщается о все новых и новых компьютерных преступлениях в нашей стране и за рубежом. Так, в частности, В.Левин в 1994 году из Санкт-Петербурга проник в компьютерную систему Ситибанка США и незаконно перевел 2.8 млн. долларов на счета своих сообщников в США, Швейцарии, Нидерландах и Израиле. Служба безопасности филиала Инкомбанка России в 1995 году пресекла попытку бухгалтера этого филиала незаконно перевести крупную сумму в валюте на счета своих сообщников. По сообщениям МВД и ФСБ России, в 1993 году была совершена попытка хищения свыше 68 млн. руб. путем манипулирования с данными Центрального банка России [10, 11].

Сегодня в России наблюдается всплеск интереса к информационной безопасности, который объясняется в первую очередь развитием банковского и страхового бизнеса, ростом и развитием крупных коммерческих структур, выходом их на международный уровень, а также повышением уровня криминогенной обстановки в стране. Поэтому проблема защиты информации в ЭВМ и обеспечения безопасности автоматизированных систем и информационно-вычислительных сетей находится в центре внимания не только специалистов по разработке и эксплуатации этих систем, но и широкого круга пользователей.

Следует отметить, что в настоящее время в проблеме защиты информации существует два направления, отличающихся по существу общественных отношений и формой организации. Это защита государственного информационного ресурса и защита информации независимого сектора экономики [17-21]. Очевидно, что защитные мероприятия призваны обеспечить конфиденциальность, целостность и доступность информации, однако если для режимных государственных организаций на первом месте стоит конфиденциальность, а целостность понимается исключительно как неизменность информации, то для коммерческих структур, вероятно, важнее всего целостность (актуальность) и доступность данных и услуг по их обработке. По сравнению с государственными, коммерческие организации более открыты и динамичны, поэтому вероятные угрозы для них отличаются и количественно, и качественно.

ЧАСТЬ 1. ОСНОВНЫЕ ПОЛОЖЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. ОСНОВНЫЕ ПОНЯТИЯ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Проведенный анализ терминологических источников по информационной безопасности, в том числе законодательных актов Российской Федерации, руководящих документов Государственной технической комиссии при Президенте Российской Федерации (Гостехкомиссии России), отечественных и зарубежных стандартов, показал, что в этой области пока не существует терминологического единства.

Понятие информационной безопасности, на наш взгляд, непосредственно связано с понятием информатизации общества.

Под **информационной безопасностью в широком смысле** будем понимать такое свойство процесса информатизации и всей жизнедеятельности общества, которое гарантирует устранение всех негативных последствий информатизации, либо сводит их до такого минимума, который обеспечивает выживание и дальнейшее развитие человечества, его превращение в развитую, гуманную информационную цивилизацию [6].

Только в случае обеспечения информационной безопасности информатизация общества окажется процессом всеобщей интеллектуально-гуманистической перестройки жизнедеятельности человечества на основе наиболее полного использования информации как ресурса его развития.

Проблема информационной безопасности в своем системно-обобщенном плане в настоящее время только начинает разрабатываться в рамках нового научного направления, именуемого социальной информатикой и претендующего на изучение закономерностей взаимодействия общества и информатики, прежде всего процесса информатизации общества и становления информационной цивилизации [1, 5, 6, 62].

Информационная безопасность в узком смысле (Information security) - это совокупность свойств информации, связанная с обеспечением запрещения неавторизованного доступа (получения, ознакомления с содержанием, передачи, хранения и обработки), модификации или уничтожения, а также любых других несанкционированных действий с личной, конфиденциальной или секретной информацией, представленной в любом физическом виде.

По своему содержанию информационная безопасность включает:

- компьютерную безопасность;

- безопасность информационных систем и процессов в обществе (в том числе и еще не охваченных процессом информатизации);

- создание необходимой социальной среды для гуманистической ориентации информационных процессов.

Таким образом, в отличие от трактовки зарубежных специалистов [74] *информационная безопасность не сводится только к компьютерной безопасности*, так же как информатизация не тождественна компьютеризации общества. Поэтому понятие информационной безопасности, включая в себя компьютерную безопасность в качестве неотъемлемой составной части, должно распространяться на все информационные процессы в обществе и другие социальные процессы, в той или иной степени влияющие на информацию и средства информатики.

Компьютерная безопасность (Computer security) - раздел информационной безопасности, связанный с ее обеспечением при создании и эксплуатации различных систем электронной обработки данных и автоматизированных сетей связи, в первую очередь вычислительных (компьютерных) систем.

Она определяется степенью защищенности (охраны) информации, технических и программных средств вычислительной техники от нанесения им ущерба в результате сознательных либо случайных противоправных действий или стихийных бедствий.

Безопасность вычислительных (информационных, компьютерных) систем (Security of Information (Computer) Systems)- совокупность свойств, связанная с достижением компьютерной безопасности при эксплуатации вычислительных (информационных, компьютерных) систем.

Безопасность данных (Data security) - совокупность свойств данных, связанная с достижением информационной безопасности и определяемая защищенностью данных от случайного или преднамеренного доступа к ним лиц, не имеющих на это право, от неавторизованной модификации данных или от их уничтожения.

Защита (Protection; Lock out) **информации при эксплуатации вычислительных (компьютерных) систем** - система мер, направленных на ограничение доступа ко всей или части информации, а также недопущения ее несанкционированного использования при эксплуатации вычислительных (компьютерных) систем.

Защита информации в широком смысле согласно Указа Президента Российской Федерации от 5 января 1992 года “ создании Государственной технической комиссии при Президенте Российской Федерации” является неразрывной частью процесса информатизации и отождествляется с безопасностью информационного ресурса, включающего в себя важнейшую и ценнейшую информацию и средства, способы ее обработки и хранения - информационные технологии.

Защита данных (Data protection) - система организационных, методических, правовых, информационных, программных и технических мероприятий, методов и средств, направленных на ограничение или исключение несанкционированного доступа к данным, их использования или изменения на любой стадии процесса сбора, обработки, хранения, передачи и уничтожения.

Под **каналом утечки информации** будем понимать способ, позволяющий нарушителю получить несанкционированный доступ к обрабатываемой или хранящейся в системе информации.

Основные термины и определения, из документов Гостехкомиссии России “Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Термины и определения” [54] и “Руководящий документ. Средства

вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации” [55] приведены в Приложении 1.

2. ВИДЫ НАРУШЕНИЙ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

2.1. Сущность проблемы обеспечения информационной безопасности

Сущность проблемы обеспечения информационной безопасности в вычислительных (компьютерных) системах и инфомационно-телекоммуникационных сетях в общем случае сводится к тому, что широкое распространение и повсеместное применение вычислительной техники, в первую очередь компьютерных сетевых технологий и персональных ЭВМ, резко повысило уязвимость собираемой, накапливаемой, хранимой и обрабатываемой в них информации [70].

2.2. Потенциальные угрозы безопасности информации

При анализе общей проблемы безопасности информации выделяются те направления, в которых преднамеренная или непреднамеренная деятельность человека, а также неисправности технических средств, ошибки программного обеспечения или стихийные бедствия могут привести к разглашению, утечке, несанкционированному доступу, модификации или уничтожению информации.

По-видимому, целесообразно в общем плане различать угрозы безопасности собственно вычислительной системы (информационно-вычислительной или телекоммуникационной сети) и угрозы безопасности находящейся, циркулирующей и обрабатываемой в ней информации.

Под **угрозой безопасности** вычислительной системы понимаются воздействия на систему, которые прямо или косвенно могут нанести ущерб ее безопасности. Разработчики требований безопасности и средств защиты выделяют три вида угроз [13]:

- угрозы нарушения конфиденциальности обрабатываемой информации;
- угрозы нарушения целостности обрабатываемой информации;
- угрозы нарушения работоспособности системы (отказа в обслуживании).

Угрозы конфиденциальности направлены на разглашение секретной или конфиденциальной информации, т.е. информация становится известной лицу, которое не должно иметь к ней доступ. Иногда для обозначения этого явления используется термин **“несанкционированный доступ” (НСД)**, особенно популярный в отечественных литературных источниках, под которым понимается доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых средств вычислительной техники (СВТ) или автоматизированных систем (АС). При этом, под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения СВТ или АС.

Традиционно противостоянию угрозам этого типа уделяется максимальное внимание, и фактически подавляющее большинство исследований и разработок было сосредоточено в этой области, так как она непосредственно относится к защите государственной тайны.

Угрозы целостности представляют собой любое искажение или изменение неуполномоченным на это действие лицом хранящейся в вычислительной системе или передаваемой информации. Целостность информации может быть нарушена как злоумышленником,

так и в результате объективных (неумышленных) воздействий со стороны среды эксплуатации системы. Наиболее актуальна эта угроза для систем передачи информации - компьютерных сетей и систем телекоммуникаций.

Угрозы нарушения работоспособности (отказ в обслуживании) направлены на создание ситуаций, когда в результате преднамеренных или непреднамеренных действий снижается работоспособность вычислительной системы, либо ее ресурсы становятся недоступными.

Цель защиты систем обработки информации заключается в противодействии угрозам безопасности. Поэтому систему можно считать безопасной или защищенной, когда она способна успешно и эффективно противостоять угрозам безопасности.

С точки зрения безопасности информации в настоящее время четко обозначились *три аспекта ее уязвимости*:

- опасность несанкционированного (случайного или злоумышленного) получения и использования информации лицом, которому она не предназначалась;
- возможность несанкционированной (случайной или злоумышленной) модификации;
- подверженность физическому уничтожению или искажению.

Появилась новая отрасль компьютерной преступности - *разработка и внедрение компьютерных вирусов*, число типов и видов которых, по оценке отечественных и зарубежных экспертов, приближается к нескольким тысячам. Имеются сведения о том, что рядом государственных и военных научных центров зарубежных государств разрабатываются так называемые “боевые вирусы”, предназначенные для поражения систем управления оружием, войсками и систем связи [86].

Наиболее широкое распространение получили случаи несанкционированного злоумышленного получения (хищения) информации с использованием различных каналов ее утечки.

Все возможные каналы утечки информации в вычислительных системах и сетях можно классифицировать исходя из типа средства, являющегося основным при получении информации по этим каналам. Различают три типа таких средств: человек, аппаратура, программа. Соответственно, возможные каналы утечки также разбиваются на три группы.

Группу возможных каналов утечки информации, в которых основным средством является человек, составляют:

- хищения носителей информации (магнитных и оптических дисков, магнитных лент, дискет, карт и т.п.);
- чтение информации с экрана посторонними лицами (во время отображения информации на экране законным пользователем или при отсутствии законного пользователя на рабочем месте);
- чтение информации из оставленных без присмотра распечаток и других твердых копий.

В группе возможных каналов утечки информации, в которых основным средством является аппаратура, можно выделить:

- подключения специальных технических средств к устройствам ЭВМ или средствам передачи информации;
- использование специальных технических средств для перехвата электромагнитных излучений.

К группе возможных каналов утечки информации, в которых основным средством является программа, можно отнести:

- несанкционированный доступ программы к данным;
- расшифровку программой зашифрованной информации;
- копирование программой информации с носителей.

2.3. Компьютерные преступления

Для подавляющего большинства компьютерных преступлений характерны корыстные мотивы. Однако представляет интерес наметившаяся в последнее время тенденция к совершению таких преступлений специалистами - профессиональными электронщиками или программистами. Люди, работающие в этой области, обычно весьма любознательны и обладают острым умом, а также склонностью к озорству. Они нередко воспринимают меры по обеспечению безопасности вычислительных (компьютерных) систем как вызов своему профессионализму и стараются найти технические пути, которые доказывали бы их личное превосходство. Постепенно они не только набирают опыт, но и приобретают вкус к этой деятельности. В конце концов, им приходит в голову мысль, что если уж заниматься такого рода “игрой”, то лучше одновременно получать и какую-то выгоду. Программисты рассчитывают поднять свой престиж, похвастaвшись перед знакомыми или коллегами умением найти слабости в компьютерной системе, а иногда и просто продемонстрировать, как эти слабости можно использовать.

Объекты атак, относимых к компьютерным преступлениям, можно разделить на три категории:

- сами компьютеры;
- объекты, которые могут быть атакованы с помощью компьютера как инструмента;
- объекты, для которых компьютер является орудием преступления.

2.3.1. Основные виды компьютерных преступлений

Рассмотрим основные виды компьютерных преступлений [1, 2, 5, 8, 9, 11, 43, 56 и др.], связанных со злоумышленным нарушением безопасности информации, в том числе так называемыми “хэкерами” (hacker) - лицами, проникающими в информационные сети, или “крэкерами” (cracker) - похитителями информации.

I. Перехват информации

A. Непосредственный перехват. Перехват данных осуществляется либо непосредственно через телефонный канал системы, либо подключением к линии принтера.

B. Электромагнитный перехват. Не требует непосредственного подключения к системе и производится улавливанием с помощью довольно несложной техники излучения, производимого центральным процессором, дисплеем, телефоном, принтером.

C. “Жучок”. Установка микрофона в компьютере с целью перехвата разговоров работающего на ЭВМ персонала.

D. Откачивание данных. Сбор информации, требующейся для получения основных материалов. Часто при этом исследуется не само содержание информации, а схемы ее движения.

E. “Уборка мусора”.
   1. Физический вариант. Сбор использованных листингов, выброшенных служебных бумаг и т.д.
   2. Электронный вариант. Исследование данных, оставленных в памяти вычислительной машины.

II. Несанкционированный доступ

A. “За дураком”.
   1. Физический вариант. Проникновение в помещения, где установлены компьютеры, следом за законным пользователем.
   2. Электронный вариант. Подключение терминала незаконного пользователя к линии связи законного пользователя в начале или при прерывании активного режима.

B. “За хвост”. Перехват сигнала, обозначающего конец работы законного пользователя с последующим осуществлением доступа к системе.

C. “Абордаж”. Хэкеры часто проникают в чужие информационные системы, подбирая номера на удачу, угадывая коды и т.п.

D. “Неспешный выбор”. Несанкционированный доступ к файлам законного пользователя осуществляется нахождением слабых мест в защите системы. Однажды обнаружив их, нарушитель может не спеша исследовать содержащуюся в системе информацию, копировать ее, возвращаться к ней многократно.

E. “Брешь”. В отличии от “неспешного выбора”, где ищутся слабости в защите системы, при данном способе производится поиск брешей, обусловленных ошибками или неудачной логикой построения программы.

F. “Люк”. “Люк” - это развитие приема “брешь”. В найденной бреши программа “развивается”, и туда дополнительно вставляют одну или несколько команд. Люк “открывается” по мере необходимости, а встроенные команды автоматически осуществляют свою задачу.

G. “Системные ротозеи”. Расчет на адекватную проверку полномочий пользователя (имена, коды, шифр-ключи и т. п.). Несанкционированный доступ по существу осуществляется нахождением бреши в программе входа в систему.

H. “Маскарад”.
   1. Физический вариант. Для получения информации злоумышленники выдают себя за других лиц, чаще всего за журналистов.
   2. Электронный вариант. Проникновение в компьютерную систему по кодам и другим идентификационным шифрам законных пользователей.

I. “Мистификация”. Иногда случается, как например с ошибочным телефонными звонками, что пользователь удаленного терминала подключается к чьей-то системе, будучи абсолютно уверенным, что работает с той системой , с какой и намеревался. Владелец системы, к которой произошло фактическое подключение, формируя правдоподобные отклики, может поддерживать это заблуждение в течение определенного времени и получать некоторую информацию, в частности, коды доступа к данным.

J. Аварийный доступ. Используется тот факт, что в любом компьютерном комплексе имеется особая программа, применяемая как системный инструмент в случае возникновения сбоев или других отклонений в работе ЭВМ, своеобразный аналог приспособлений, помещаемых в транспорте под надписью “Разбить стекло в случае аварии”. Такая программа - мощный и опасный инструмент в руках злоумышленника.

K. “Склад без стен”. Несанкционированный доступ осуществляется в результате системной поломки. Например, если некоторые файлы пользователя остаются открытыми, он может получить доступ к не принадлежащим ему частям банка данных. Все происходит так, словно клиент банка, войдя в выделенную ему в хранилище комнату, замечает, что у нее нет одной стены.

3. Манипулирование данными

A. Подмена данных. Изменение или введение ложных данных осуществляется, как правило, при вводе в ЭВМ или выводе истинных данных.

B. Подмена кода. Вариантом подмены данных является изменение кода программы.

C. “Троянский конь”. Тайное введение в чужую программу таких команд, которые позволяют осуществить новые, не планировавшиеся владельцем программы функции, но одновременно сохранять и прежнюю работоспособность. По существу, это “люк”, который открывается не “вручную”, а автоматически, без дальнейшего участия злоумышленника. С помощью “троянского коня” преступники обычно отчисляют на свой счет определенную сумму денег с каждой банковской операции.

D. “Троянский конь в цепях”. В отличии от программных “троянских коней”, которые представляют собой совокупность команд, речь идет о “троянских конях” в электронных цепях компьютеров. Это очень редкий способ, потому что если в предыдущих поколениях компьютеров, где использовались схемные соединения и печатные платы, еще можно было применять этот прием, то сейчас внести какие-либо изменения можно, пожалуй, только на уровне конструирования и заводского производства печатных плат.

E. “Троянская матрешка”. Еще одна разновидность “троянского коня”. Ее особенность состоит в том, что в кусок программы вставляются не команды, выполняющие “грязную” работу, а команды, формирующие эти команды и после их выполнения уничтожающие их. В этом случае программисту, пытающемуся найти “троянского коня”, необходимо искать не его самого, а формирующие его команды. Развивая эту идею, можно представить себе команды, которые создают другие команды сколь угодно большое число раз, которые создают “троянского коня”.

F. “Компьютерные вирусы”. “Троянские кони” типа “сотри все данные этой программы, перейди в следующую и сделай тоже самое”. Современные вирусы обладают свойством переходить в компьютерных сетях из одной вычислительной системы в другую, распространяясь как вирусное заболевание.

G. “Салями”. Тактика использования “троянского коня”, основанная на том, что отчисляемые суммы малы и их потери практически незаметны (например по 1 коп. с операции), а накопление осуществляется за счет большого количества операций. Это один из простейших и безопасных способов, особенно если отчисляются

дробные (стоимостью меньшей, чем самая малая денежная единица, - например 1 коп.) денежные суммы, поскольку в этих случаях все равно делается округление.

H. “Логическая бомба”. Тайное встраивание в программу команд, которые должны сработать один раз или срабатывать многократно при определенных условиях.

I. “Временная бомба”. Разновидность “логической бомбы”, которая срабатывает по достижении определенного момента времени.

J. “Асинхронная атака”. Сложный способ, требующий хорошего знания операционной системы. Используя асинхронную природу функционирования операционной системы, ее заставляют работать при ложных условиях, из-за чего управление обработкой информации частично или полностью нарушается. Если лицо, совершающее “асинхронную атаку”, достаточно искусно, оно может использовать ситуацию, чтобы внести изменения в операционную систему или направить ее на выполнение своих целей, причем вне системы эти изменения не будут заметны.

K. Моделирование.

1. Реверсивная модель. Создается модель конкретной системы. В нее вводятся реальные исходные данные и учитываются планируемые действия. Затем исходя из полученных правильных результатов, подбираются правдоподобные желаемые результаты. После этого модель возвращается назад, к исходной точке, и становится ясно, какие манипуляции с входными данными нужно проводить. В принципе “прокручивание” модели “вперед-назад” может происходить не один раз, чтобы через несколько итераций добиться желаемого результата. После этого остается только осуществить задуманное действие.
2. “Воздушный змей”. В простейшем случае требуется открыть в двух банках по небольшому счету. Далее деньги переводятся из одного банка в другой и обратно с постепенно повышающимися суммами. Хитрость заключается в том, чтобы до того, как в банке обнаружится, что поручение о переводе не обеспечено необходимой суммой, приходило бы извещение о переводе в этот банк, так чтобы общая сумма соответствовала требованию о первом переводе. Этот цикл повторяется большое число раз (“воздушный змей” поднимается все выше и выше) до тех пор, пока на счете не оказывается достаточно большая сумма (фактически она постоянно “перескакивает” с одного счета на другой, увеличивая свои размеры). Тогда деньги быстро снимаются и владелец счетов исчезает. Этот способ требует очень точного расчета, но для двух банков его можно сделать и без компьютера. На практике в такую игру включают большое число банков, так что сумма накапливается быстрее и число поручений о переводе не достигает подозрительной частоты. Но управлять этим процессом можно только с помощью компьютера.
3. “Ловушка на живца”. Создание особой программы, удачно разрекламированной и потому якобы представляющей интерес для специалистов (“живец”). На самом деле программа работает некоторое время, затем имитирует системную поломку и записывает коды доступа в систему всех пользователей, осуществляющих работу с программой. Полученные данные используются для других компьютерных злоупотреблений.

Перечисленные компьютерные преступления чаще всего представляют собой:

- хищение денег (подделку счетов и платежных ведомостей, приписки сверхурочных часов работы, фальсификация платежных документов, вторичное получение уже произведенных выплат, перечисление денег на подставные счета и т.д.);
- хищение вещей (совершение покупок с фиктивной оплатой, добывание запасных частей и редких материалов);
- хищение машинной информации;
- внесение изменений в машинную информацию;
- несанкционированная эксплуатация системы;
- несанкционированное использование ресурсов ЭВМ или сети (например, хищение машинного времени);
- подделка документов (полученных фальшивых дипломов, фиктивное продвижение по службе);
- саботаж;
- шпионаж (политический, военный и промышленный).

Особым видом компьютерного преступления является вандализм, который обычно принимает форму физического разрушения вычислительных (компьютерных) систем или их компонентов. Часто этим занимаются уволенные сотрудники из чувства мести, люди, страдающие компьютерными фобиями. Они поджигают компьютеры, закладывают в них взрывчатку, заливают краской и т. п.

2.3.2. Удаленное несанкционированное проникновение в систему

2.3.2.1. Развитие информационных сетей

Теорией показано, а практикой подтверждено, что эффективное решение интеллектуальных и аналитических задач самого разнообразного характера и любого уровня возможно только путем широкого и оперативного обмена информацией между руководителями и исполнителями, включая в обязательном порядке и по параллельным связям. Поэтому стержнем любой информационной системы и всего процесса информатизации и организации управления является создание распределенных архитектур (сетей) и их последующая модернизация и расширение.

Конечно, оборудование рабочих мест изолированными средствами вычислительной техники также позволило значительно повысить эффективность труда каждого отдельно взятого пользователя и исполнителя и работы в этом направлении продолжаются. Однако такая замкнутая система ограничена в дальнейшем развитии огромными затратами на создание информационных услуг для каждого рабочего места. Данную ситуацию можно сравнить, например, с организацией производства, когда один, максимум два, крупных металлургических комбината обеспечивают своей продукцией сотни и тысячи предприятий самого разнообразного профиля. Конечно, для каждого предприятия можно было бы создать свой металлургический комбинат, но это, разумеется, нецелесообразно.

Развитие распределенных архитектур (сетей) позволяет с наибольшей эффективностью применять технологию гипертекста: в автоматическом режиме создавать аналитические документы даже по вопросам стратегического характера. Технология цифровой передачи графической информации открывает широкие перспективы для организации опера-

тивного удаленного обмена документами любого характера, например, картами и различными схемами.

Говоря о больших преимуществах сетей по сравнению с изолированными средствами вычислительной техники необходимо особо подчеркнуть, что на современном этапе развития информационной сферы даже создание отдельных сетей не позволяет в полной мере использовать возможности автоматизированной обработки информации. В первую очередь это касается таких сфер деятельности, как государственное или военное управление, в которой для поддержания баланса сил и средств, не говоря уже о достижении превосходства, требуется обеспечить максимально оперативную и автоматическую обработку и передачу информации через все уровни управления как по командной линии в обоих направлениях, так и по параллельным связям между отдельными ее потребителями. В качестве примера можно привести циркулярную передачу оповещения о воздушном нападении или о ядерной угрозе, запрос артиллерийской или авиационной поддержки, вызов противотанкового резерва или спасательной команды.

Для решения этой сложной и крупномасштабной задачи уже недостаточно применения отдельных автоматизированных сетей, а требуется решать проблему межсетевого обмена информацией. Идеальным решением могло быть создание глобальной, гетерогенной, сквозной системы, обеспечивающей передачу информации, представленной в любой форме, по всем направлениям в национальном или даже мировом масштабе в реальном масштабе времени.

Суммируя все эти доводы можно с уверенностью сказать, что развитие сетей и, следовательно, средств удаленного доступа к информационным ресурсам будет прогрессировать и эта тенденция сохранится на отдаленную перспективу.

Наряду с рядом несомненно положительных сторон развитие распределенных архитектур в то же время создает и широкие возможности для проведения акций по удаленному и автономному проникновению в информационные ресурсы неуполномоченными на то лицами с разведывательными или диверсионными целями. На первоначальном этапе появления вычислительных сетей этими возможностями пользовались лишь частные лица, сначала для развлечения, затем с целью наживы. В дальнейшем удаленным несанкционированным доступом стали пользоваться и спецслужбы для решения стратегических разведывательных задач.

Несанкционированное проникновение в информационные системы приобрело такой широкий размах, что появившийся на заре развития вычислительной техники термин “хэкеризм” прочно вошел без перевода почти во все языки мира.

2.3.2.2. Оценка и анализ явления “хэкеризм”

Деятельность по удаленному несанкционированному проникновению в информационные системы с целью хищения, уничтожения или изменения содержащейся в них информации исходно получило название “хэкеризм” [58]. В настоящее время эта деятельность стала эффективным и часто применяемым средством противоборства в информационной сфере.

Считается, что из безобидного спортивного увлечения, каковым хэкеризм был первоначально, он окончательно превратился в опасную деятельность в конце 80-х годов. Так, в 1987 году осведомитель контрразведки ФРГ (das Bundesamt fuer Verfassungsschutz), внед-

ренный в компьютерный клуб “Chaos Computer Club” (CCC) сообщил, что группе членов клуба удалось ввести в автоматизированную сеть НАСА SPANet диверсионную программу типа “троянский конь”. В результате этой акции под контролем этой группы оказалось более 130 компьютеров космического агентства США. Уже тогда контрразведка ФРГ активно включилась в расследование, поскольку в Федеральной криминальной полиции (das Bundeskriminalamt) полагали, что имеют дело с фактом шпионажа, однако, этого в конечном итоге доказать не удалось.

Начало этого вида деятельности как средства борьбы специалисты также относят к концу 80-х годов и считается, что впервые целенаправленно, планомерно и в широком масштабе оно было применено советскими разведывательными службами. В частности, в марте 1989 года Федеральная криминальная полиция ФРГ во взаимодействии с контрразведкой страны выявила группу западногерманских специалистов, занимавшихся хищением секретной информации в пользу СССР из автоматизированных информационных систем в США, ФРГ и во Франции методом удаленного доступа.

На этом случае стоит остановиться более подробно, поскольку он является в некотором смысле классическим и его уроки полезны для изучения обеим сторонам. Это была организованная группа во главе с руководителем, в которой обязанности распределялись в соответствии с возможностями каждого члена. Её успешная деятельно на протяжении трех лет с 1986 по 1989 год (как было установлено) стала возможной благодаря правильному и продуманному сочетанию агентурных способов организации и управления и технических методов добывания.

Как всегда в таких случаях, факт незаконной деятельности был выявлен органами безопасности благодаря совершенно незначительной детали. Все началось с того, что при сведении балансов оплаты по счетам за пользование информационными услугами вычислительного центра лаборатории имени Лоуренса в Беркли (США) управляющий компьютерными системами Клиффорд Столл (Clifford Stoll) обнаружил недостачу в 75 центов. В дальнейшем из Национального центра компьютерной безопасности, относящегося к ведению АНБ, пришла информация о том, что кто-то из лаборатории в Беркли пытается проникнуть в один из многочисленных компьютеров этого агентства. После этого Столл при поддержке ФБР начал серьезно заниматься расследованием. Он установил, что незаконный пользователь применяет для поиска информации такие ключевые слова как атомная энергия, вооружения, системы оружия, СОИ и тому подобные, что, конечно, сразу же наталкивало на мысль о шпионаже. Используя эту информацию нарушителю устроили ловушку: подставили объемный фальшивый файл с материалами якобы по СОИ и пока он копировал этот файл удалось проследить его сетевой адрес в Бремене.

В то же время хэкеры действовали аккуратно и всю извлеченную информацию переписывали первоначально в центральный компьютер университета Бремена, а затем по частям пересылали в домашние компьютеры в Ганновере. Это, во-первых, значительно усложняло расследование, а во-вторых, мешало выдвинуть законные обвинения.

Окончательно раскрыть эту группу и привлечь к ответственности удалось лишь только потому, что двое соучастников добровольно пришли в полицию и сознались в содеянном.

2.3.2.3. Оценка возможностей по удаленному проникновению

Несмотря на ряд случаев успешного несанкционированного проникновения в информационные системы, в том числе и военные, деятельность эта связана со многими трудностями и опасностями. Привлекаться к ней могут только высокоподготовленные и квалифицированные специалисты и при этом исключительно под руководством и контролем оперативных работников, имеющих хорошую подготовку по вопросам информатики и вычислительной техники. С каждым годом работа по получению несанкционированного удаленного доступа становится более сложной и опасной, что связано, в первую очередь, с совершенствованием систем защиты и безопасности. Это особенно наглядно видно при подробном рассмотрении общей картины развития систем обеспечения информационной безопасности.

В начале 1980-х годов резко возросла потребность в создании и развитии связей между информационными системами, а также каналов доступа к ним потребителей информации. Однако в тот период еще не было специальных национальных и международных телекоммуникационных сетей и для доступа к центральному компьютеру (host computer) использовались обычные телефонные линии.

Большая часть программных средств, которыми были оснащены информационные системы для обеспечения удаленного доступа к ним, позволяла осуществлять автоматический набор пароля с терминала. Входными параметрами для получения доступа к центральному компьютеру в тот период были лишь имя пользователя и пароль, причем длина слова пароля редко превышала четыре символа. Администрация информационных систем не имела опыта в вопросах безопасности и в целом отсутствовал единый комплексный подход к решению этой задачи.

В этих условиях получение удаленного несанкционированного доступа к информационным системам не представляло труда даже для начинающего. Так, например, подбор пароля можно было выполнять в автоматическом режиме, циклически с помощью простой самодельной программы. Таким образом, злоумышленник имел в своем распоряжении неограниченное количество попыток и при относительно небольших расходах за пользование телефонной линией шансы на успешный подбор пароля были достаточно высоки. При этом для злоумышленника практически отсутствовал риск быть пойманным.

В конце 1980-х годов после многочисленных случае несанкционированного доступа к информационным ресурсам ситуация резко изменилась. В большинстве систем были введены жесткие нормы безопасности, доступ к ним стал возможен только через специальные телекоммуникационные линии и службы с контролем и регистрацией сведений о пользователях в специальных узлах, что позволяет в случае необходимости найти нарушителя. Была исключена возможность циклического запроса паролей: после нескольких попыток выбранный вход в систему блокируется. В большинстве стандартов минимальная длина пароля была определена в восемь символов.

Все эти жесткие меры защиты стали применяться в подавляющем большинстве современных информационных систем и, в первую очередь, это касается военных, правительственных и банковских информационных систем. Тем не менее существуют возможности по получению удаленного несанкционированного доступа в эти системы без агентурного проникновения на сами объекты, связанные с конкретными недостатками архитектур и ошибками в их эксплуатации. Наиболее характерными являются следующие:

- использование заводского пароля, введенного в систему на предприятии изготовителе при её поставке заказчику;
- обход идентификации конечного пользователя, то есть создание условий, когда запрос допуска исходит от какого-то промежуточного и при этом уполномоченного звена (информационной системы, телекоммуникационного узла), которым манипулирует нарушитель;
- использование информации “электронных досок объявлений” (electronic bill board).

Наглядным примером использования заводского пароля является случай проникновения в Федеральное ведомство здравоохранения (ФВЗ) Швейцарии в 1989 году. При этом двум специалистам-хэкерам удалось получить удаленный несанкционированный доступ в два регистра с наивысшей степенью секретности автоматизированной информационной системы ФВЗ: список лиц с положительной реакцией на HIV-вирус и учет сотрудников атомных объектов страны, получивших те или иные дозы радиации. Примечательным в этой истории является то, что самым сложным для нарушителей оказалось найти сетевой адрес информационной системы ФВЗ, для чего они через домашний компьютер с модемом организовали в автоматическом режиме циклический просмотр-запрос возможных адресов. Доступ же к секретным регистрам им удалось получить с помощью пароля (field/digital), который был введен в систему на предприятии-изготовителе при её поставке заказчику. Несмотря на инструкции и предписания этот пароль не был изъят из системы и при этом он имел высшую степень приоритета, что позволяло нарушителям выполнять в системе любые операции, вплоть до полного уничтожения всей информации.

Поразительным является беспечность администрации системы, не обнаружившей никаких нарушений на протяжении недели, хотя нарушители несколько раз оставляли заметные следы о своих визитах. Детали этого происшествия стали известны благодаря тому что, хэкеры пригласили корреспондента одной из национальных газет и дали подробное интервью, которое и было затем опубликовано.

Для демонстрации метода обхода идентификации конечного пользователя можно привести факт незаконного использования доступа в центральный компьютер Высшей технической школы (ВТШ) города Цюриха (die Eidgenoessische Technische Hochschule Zuerich - ETH) для бесплатного пользования телекоммуникационными услугами. Это стало возможным благодаря тому, что для доступа в информационную систему ВТШ “Kometh” с домашнего компьютера через модем по телефонной сети не требуется предоставлять пароль. Сама же сеть “Kometh” имеет выход на территорию США через национальную информационную сеть “Telepac” и подводный кабель между Европой и Северной Америкой. При этом система контроля паролей в компьютерных центрах телефонных компаний США оказалась весьма слабой и легко раскрываемой. Подобрав несколько паролей, швейцарские хэкеры в течение длительного времени бесплатно пользовались линиями связи для доступа в “электронные почтовые ящики” как в США так и на территории Швейцарии через американские коммуникационные системы.

Этот факт был вскрыт примерно через полгода, когда несколько телекоммуникационных компаний США предъявили ВТШ счета на общую сумму в несколько тысяч долларов. Руководство школы вынуждено было оплатить счета, но ни одного нарушителя найдено не было.

Использование информации “электронных досок объявлений” заключается в регулярном изучении и анализе информации, помещаемой на этих “досках”. Наряду с массой мелких и малозначимых сведений их хозяева помещают также пароли различных информационных систем, которые им удалось или самим подобрать или они их знают как бывшие сотрудники каких-либо учреждений. Имели место случаи, когда хэкеры через электронные доски предлагали пароли военных и государственных информационных систем в обмен на регистрационные параметры каких либо фирм или банков [71].

В настоящее время наилучшим (наиболее дешевым и быстрым) способом получения доступа в информационные системы считается *агентурное внедрение на объект* с тем, чтобы либо непосредственно приобрести (купить) копию требуемого информационного массива, либо получить через агентуру необходимые регистрационные данные (пароль идентификационный номер) для удаленного доступа в соответствующую базу данных. Сам удаленный доступ также целесообразно осуществлять с помощью агентуры [37, 56].

2.3.2.4. Возможные направления применения “хэкеризма”

Наряду с добывание чисто военно-технических сведений большие возможности открывает хэкеризм по сбору коммерческой, страховой и тому подобной информации. Так, интересным представляется, например, анализ коммерческой деятельности цементно-бетонных предприятий (данная информация как правило не является секретной), выполняющих заказы по строительству шахтных пусковых установок (ШПУ), аэродромов и командных пунктов. Проникновение в информационные системы социальных служб и органов страхования дает оперативную информацию в интересах проверки и поиска перспективных лиц.

Одним из направлений деятельности в области хэкеризма считается систематический сбор паролей и прочих атрибутов допуска в информационные системы с целью планомерной подготовки их массированного вывода из строя в какое-то определенное время, например, путем внедрения в эти системы компьютерных вирусов.

2.3.3. Перехват компрометирующих излучений

Изучение вопросов перехвата компрометирующих излучений уделяется значительное внимание в большинстве индустриально развитых стран, особенно в США и Западной Европе. Так, по оценкам специалистов, только в ФРГ разработкой аппаратуры перехвата компрометирующего излучения занято более 100 частных компаний. Огромным преимуществом добывания информации с помощью данного метода является то, что эта деятельность не оставляет за собой следов и её почти невозможно пресекать используя нормы закона. Это и обуславливает повышенный интерес к ней со стороны многих разведывательных и специальных служб, а также разработчиков этой аппаратуры.

Еще в начале исследовательских работ по регистрации компрометирующего излучения было установлено, что самым сильным его источником являются мониторы на основе катодного кинескопа. Это связано с конкретными особенностями устройства таких мониторов, у которых при работе системы развертки и управления электронным лучом возникает достаточно сильное высокочастотное излучение. Данное излучение, в основном, совпадает с обычным телевизионным сигналом за тем основным исключением, что оно не содержит

синхронизирующих импульсов [73]. Было также установлено, что это излучение может распространяться как через атмосферу на частоте телевизионного диапазона III, так и по проводящим линиям (кабелям электропроводки, трубопроводам водоснабжения и канализации и так далее) в телевизионном диапазоне I. Последняя особенность делает возможным эффективный перехват компрометирующего излучения без применения антенных систем, если аппаратуру перехвата удается расположить в том же помещении, где находится источник излучения. Наиболее опасными (и в то же время удобными для перехвата) с точки зрения компрометирующего излучения являются мониторы старой конструкции, в которых практически без изменения реализован телевизионный принцип развертки и управления электронным лучом.

Практические эксперименты показали, что для удовлетворительного воспроизведения информации, отображенной на экране монитора-излучателя, с расстояния до 40 метров достаточно иметь обычный телевизионный приемник доработав его следующим образом:

- имеется блок ввода и регулировки синхронизирующих сигналов, а телевизионный приемник имеет вход для его подключения;
- расширен диапазон рабочих частот (супер)гетеродина;
- установлен предварительный антенный усилитель;
- приемник оснащен устройством оптимизации работы декодера.

Такой “любительский” комплект позволяет снимать читаемую информацию с экранов находящихся неподалеку мониторов. Недостатком работы этой упрощенной аппаратуры является то, что на экране телевизионного приемника по ряду технических причин не воспроизводятся горизонтальные линии, в результате чего затруднено чтение некоторых букв таких как E, F, L, T. Однако нет никаких принципиальных препятствий для разработки высокочувствительной профессиональной аппаратуры, в которой бы были устранены указанные недостатки и которая позволяла бы одновременно в автоматическом режиме записывать на носитель (например на видеокассету) перехватываемую информацию.

2.4. Компьютерные вирусы

Менее 15 лет тому назад компьютерные вирусы были еще мало известны [8], а интерес к ним проявлялся лишь в научных кругах. Сегодня они представляют из себя серьезную угрозу для всех аспектов обработки данных с применением автоматизированных вычислительных средств. Всему миру уже известна способность компьютерных вирусов уничтожать или изменять массивы информации и программные средства. Однако в принципе вирусы могут выводить из строя некоторые узлы компьютеров, например, прецизионные механические системы дисководов, вводя их в резонанс.

В наибольшей опасности находятся пользователи операционной системы MS-DOS/Windows и ее разновидностей как наиболее часто употребляемой и широко распространенной, однако, в последние несколько лет наметилась отчетливая тенденция к расширению “сферы влияния” компьютерных вирусов [34]. Так, в некоторых странах НАТО отмечались случаи полной или частичной потери работоспособности боевых ракет вследствие неправильного функционирования средств программного обеспечения в системах пуска и наведения.

Было, например, точно установлено, что отказ системы автоматического пуска ракет “Пэтриот” (Patriot), размещенных в ходе конфликта в Персидском заливе в 1991 году в Тур-

ции, был обусловлен ошибкой в одной из программ компьютера пусковой установки, попавшей сюда, как полагают, уже в процессе эксплуатации. После тщательного анализа эксперты США пришли к выводу, что именно эта же ошибка стала причиной и самопроизвольного пуска одной ракеты “Пэтриот” в Турции в районе города Инсирлик.

Кроме того, в ходе учебных пусков французских противокорабельных ракет (ПКР) “Экзосет” (Exocet) в том же году было зарегистрировано несколько случаев полного отказа системы наведения ракет на цель. В ходе тщательного анализа французские специалисты установили, что эти отказы вызваны компьютерным вирусом, попавшим в бортовую систему наведения ракеты, наиболее вероятно, на этапе производства и сборки. Среди прочих версий попадания вируса в программное обеспечение не исключают также возможность его намеренного ввода фирмой-производителем для получения в последующем дополнительных прибылей за счет выполнения дорогостоящего ремонта.

Были зарегистрированы также и другие случаи попадания компьютерных вирусов и программных ошибок в боевые системы с более легкими последствиями.

Анализ всех этих фактов свидетельствует о достаточно реальных возможностях преднамеренного ввода программных ошибок и компьютерных вирусов в программное обеспечение средств управления пуском и бортовых систем наведения ракет, а также другой боевой техники как на этапе сборки и отладки, так и в процессе эксплуатации. При этом можно заранее предусмотреть желаемое нарушение в работе аппаратных средств за счет ввода вируса, а сам вирус можно замаскировать под обычную непреднамеренную ошибку программирования.

Таким образом проблема компьютерных вирусов чрезвычайно актуальна и перспективна. Для ее исследования создаются новые и расширяются действующие научно-исследовательские органы; возникли сотни частных компаний, специализирующихся на изучении компьютерных вирусов и разработке средств борьбы с ними.

Технология компьютерных вирусов предоставляет возможность осуществления почти анонимных диверсий. Например, если бы Роберт Моррис не признался в содеянном в знаменитом случае внедрения “червя” в сеть Internet [42], вряд ли бы его удалось привлечь к ответственности в соответствии с законодательством. Правда, здесь необходимо сделать оговорку в отношении анонимности. Данное утверждение верно, если злоумышленник (злоумышленники) не оставляет за собой следа, например не использует вирусы для получения денег по именному документу. Так, например остались анонимными большинство разработчиков компьютерных вирусов, не преследующих цели наживы, а большинство искателей наживы были так или иначе изобличены.

2.4.1. Основные положения

Прежде, чем перейти к освещению данной темы следует дать определение компьютерному вирусу. Задача эта не такая простая, если учесть буквально огромное количество известных компьютерных вирусов, разнообразие механизмов их функционирования и производимых ими эффектов.

По определению Йоахима Шнайдера (Joachim Schneider), руководителя исследовательского центра проблем компьютерных вирусов в Мюнхене, под этим термином понимается скрытная и разрушительная программа, обладающая способностью изменять другие

программы таким образом, что в них после определенных операций внедряется копия машинного кода вируса (без ведома пользователя). Поскольку измененные программы после инфицированная приобретают свойство вируса к самокопированию, то инфекция продолжает распространяться. К этому следует добавить, что в принципе можно разработать вирус, способный в ходе размножения “развиваться”, то есть изменяться и даже приспосабливаться к обстановке. В какой-то степени этим свойством обладает так называемый “китовый” вирус, способный в разных средах приобретать различные формы.

Данное определение, по всей видимости, наиболее точно отражает существо дела, однако следует отметить, что существуют довольно опасные компьютерные программы, получившие название “троянский конь”, которые не способны размножаться. Замаскированные обычно под полезные сервисные программы они выполняют свою разрушительную функцию чаще всего уже при запуске компьютера. В связи с отсутствием способности к распространению эти программы не могут называться вирусами в том смысле, какой придается данному термину, однако их нельзя отбрасывать из рассмотрения, поскольку они также могут весьма эффективно использоваться для борьбы в информационной сфере.

Все вирусы по их целевому результату действия делятся на две категории: “вирусы публичного эффекта” (public domain viruses), которые для простоты называют обычными вирусами, и специальные диверсионные программы. Большинство из известных на сегодняшний день вирусов относятся к первой категории, то есть они рассчитаны скорее на шумный эффект, а не на решение какой-то целесообразной задачи. Для них не определена конкретная цель. Эти вирусы наименее опасны для компьютерных систем и информационных массивов, по крайней мере в настоящее время [23, 29], когда хорошо отработаны методы борьбы с ними. В то же время, учитывая исторический опыт, нельзя исключать того, что будет изобретено что-либо качественно новое, и поэтому следует в любом случае соблюдать все меры предосторожности, позволяющие до минимума свести ущерб, если такое и случится.

Вторая категория представляет из себя тщательно составленные целенаправленные программы-диверсанты, предназначенные для выполнения одной четко определенной функции, например для получения денег по ложному счету. На сегодняшний день уже имеется значительное количество примеров успешных и провалившихся попыток получения денег с помощью подобных вирусов.

Разница между “диверсионными программами” и обычными вирусами заключается, во-первых в уровне профессионализма, на котором они созданы. Для того, чтобы составить диверсионную программу требуется, как правило, группы программистов самой высокой квалификации, обладающих фундаментальными общими познаниями в области информатики и вычислительной техники и глубокими специальными знаниями конкретной системы, в которую осуществляется проникновение. Весьма показателен в этом случае вышеупомянутый пример с Робертом Моррисом, которому не хватило квалификации для реализации своего “гениального” замысла.

В свое время, когда появились первые компьютерные вирусы, некоторые аналитики высказывали опасения по поводу того, что это могло быть целенаправленной акцией разработчиков программного обеспечения. Такое предположение выглядит вполне естественным, учитывая, что компании занимавшиеся в тот период созданием антивирусных программ оказались на подъеме, однако, не было отмечено ни одного случая, подтверждающего эту гипотезу.

Во-вторых, обычные вирусы создаются отдельными личностями из честолюбивых побуждений как реакция индивидуума на непризнание его обществом для достижения шумного публичного эффекта. Их поступки напоминают “подвиг” Герострата, который в древней Греции поджег храм богини Артемиды только лишь для того, чтобы прославиться. В то же время диверсионные программы предназначены для решения четко определенной задачи в интересах достижения какой-то ощутимой, материальной выгоды. При этом создатели таких программ стремятся, по возможности, исключить проявление их воздействия.

В-третьих, создание и внедрение обычных вирусов носит случайный спорадический характер и вызывается такими факторами как обида, социальная неудовлетворенность и т.п. Применение же диверсионных программ представляет из себя лишь часть комплекса мероприятий, проводимых по единому плану, под единым руководством, и согласованных по месту, времени и цели.

Таким образом. “компьютерный вирус”, или “программа-вирус”, - это программа, которая способна размножать себя в компьютере, а также передаваться другим средствам вычислительной техники по каналам связи или через внешние магнитные носители. При этом особую опасность представляют вирусы, обладающие способностью искажать (уничтожать) записанные информацию и программы, увеличивать время реакции системы на запросы пользователей и исполнения программ, нарушать правильную работу компьютера, вызывая осыпания (выпадения) букв (слов) в текстах, отображаемых на экране дисплея, и т.п.

Компьютерные вирусы могут быть написаны в принципе любым программистом, распространяться в любой вычислительной среде, однако наибольшую опасность они представляют для персональных компьютеров (ПЭВМ). Это объясняется, во-первых, относительной простотой программных структур для них и, во-вторых, широким применением ПЭВМ, и почти неконтролируемым распространением их программного обеспечения. Кроме того, это связано с включением ПЭВМ в вычислительные сети, которые позволяют обмениваться информацией и программами по каналам связи.

Полный жизненный цикл компьютерного вируса имеет следующие этапы: внедрение, инкубационный период, репродуцирование (саморазмножение) и деструкция, т.е. этап, когда “вирус” осуществляет разрушительную функцию. В память ПЭВМ вирус может быть занесен вместе с некоторой программой, в теле которой он размещается злоумышленником-программистом. При этом запуск прикладной программы приводит к запуску вируса. Моменту активизации программы-вируса может предшествовать инкубационный период, который продолжается от нескольких дней до нескольких месяцев. Это позволяет скрыть источник проникновения вируса в компьютер. После окончания инкубационного периода вирус активизируется, осуществляет репродуцирование себя на другие, доступные места в памяти. При этом вирус может сцепляться другими программами или внедряться в них.

Находясь в активном состоянии программа-вирус, содержащая деструктивную функцию, может реализовать ее.

2.4.2. Классификация компьютерных вирусов

К настоящему времени в мире информатики уже насчитывается достаточное количество фактов, позволяющих провести определенный анализ и классификацию.

Настоящие вирусы (к которым не относятся программы типа “троянский конь”) состоят, по крайней мере, из двух функционально разделенных компонентов. Один из них отвечает за размножение, а второй выполняет задачу по нанесению ущерба. Компонент, ответственный за размножение, включает в себя все те функции, которые необходимы для распространения вируса, в частности поиск неинфицированных программ, внесение в них изменений, внедрение в оперативную память и, наконец, выполнение маскировочных мероприятий.

Компонент, выполняющий задачу по нанесению ущерба, вступает в действие как правило после завершения работы той части вируса, которая отвечает за размножение. Почти всегда для этого компонента четко определяются условия начала его работы (пуска) и предусматривается их проверка при каждой активизации вируса. Если эти условия не соблюдены, то работы данного компонента прекращается и не происходит ничего, чтобы могло бы броситься в глаза. Это объясняет почему вирусные инфекции очень часто могут оставаться незамеченными на протяжение длительного времени. Вирус “спит” пока не наступит определенный момент.

Если же указанные условия соблюдаются, то вступает в действие компонент, выполняющий разрушительную функцию. Последствия при этом могут быть разными: от невинных эффектов на экране, необъяснимых нарушений работы портов и до полной потери всех данных на жестких дисках или на дискетах. Довольно часто происходит весьма сложное искажение данных так, что ущерб в полной мере можно обнаружить только по истечению значительного времени.

В принципе, все вирусы с технической точки зрения делятся на две большие группы, отличающиеся друг от друга по объекту внедрения: файловые и системные.

2.4.2.1. Файловые вирусы

Файловые вирусы составляют наиболее многочисленную группу и в свою очередь разделяются по способу воздействия на две подгруппы: вирусы необратимой модификации (ueberschreibende Viren) и вирусы гибкой модификации (nicht ueberschreibende Viren). Вирусы необратимой модификации разрушают программы (файлы) благодаря своему механизму размножения, в результате чего начало программы сразу же заменяется машинным кодом вируса. Измененные программы становятся неработоспособными непосредственно после воздействия на них и поэтому данный тип вирусов быстро обнаруживается и его возможности по распространению и нанесению ущерба ограничен.

Вирусы гибкой модификации, называемые также прикрепляющимися вирусами (link-viruses), более опасны, поскольку их присутствие в системе обнаружить не легко. Такие вирусы “повисают” на программах и, несмотря на произведенные изменения, они способны восстановить прежний вид этих программ непосредственно перед их пуском. Обычно заражение вирусом можно обнаружить только путем сравнения размеров файла с оригиналом.

По способу использования оперативной памяти файловые вирусы бывают резидентные (размещаемые в памяти резидентно) и нерезидентные (удаляются из памяти вместе с выгружаемой инфицированной программой. В специальной терминологии резидентные называются вирусами непрямого действия (indirect action viruses), а нерезидентные - вирусами прямого действия (direct action viruses).

Большинство файловых вирусов (но не все) при вызове зараженных ими программ резидентно инсталлируются в оперативную память, благодаря чему они в той или иной степени могут контролировать систему и, таким образом, эффективно распространяться. Передача инфекции происходит не прямым способом, то есть не в момент загрузки зараженной программы, а в результате последующего функционирования системы, например при последовательной загрузке еще не зараженных программ. Большинство представителей этого подвида заражают программы только при выполнении определенных команд ОС, связанных с загрузкой и запуском программ, в момент обращения к этим командам. Однако некоторые вирусы обладают более сильным и совершенным механизмом, способным распространять инфекцию при выполнении всего перечня файловых команд, осуществляющих открытие, закрытие, копирование и перенос файлов. Поэтому простая проверка программных файлов (путем их открытия для просмотра) на предмет инфекции в этом случае принесет больше вреда, чем пользы.

Другой подвид файловых вирусов (прямого действия) не остается в оперативной памяти резидентно, а только лишь при запуске инфицированной программы такой вирус начинает искать другие программы и пытается их заразить. В этом случае при загрузке неинфицированной программы не происходит ни её заражения, ни дальнейшего распространения инфекции.

2.4.2.2. Системные вирусы

Системные вирусы работают на более глубоком уровне, внедряясь в дисковую структуры ОС, связанную с базовыми функциями запуска компьютера и ввода/вывода информации.

Активизация этого типа вируса, в отличие от других, происходит только при запуске (перезапуске) компьютера с зараженного диска, после чего вирус резидентно инсталлируется в оперативной памяти и начинает манипулировать пусковым сектором (загрузчиком) и другими элементами дисковой структуры. Распространение инфекции происходит при обращении ОС к другим дискам.

Обнаружить такой вирус и освободиться от него весьма трудно. Это связано, в первую очередь, с тем, что он попадает в оперативную память в процессе запуска компьютера, то есть еще до того как сможет заработать какая-либо антивирусная программа. Единственная возможность обнаружить инфекцию заключается в проверке оперативной памяти сразу же после загрузки. При обнаружении вируса компьютер следует немедленно выключить и загрузить с неинфицированного диска.

В зависимости от конечного объекта внедрения различают два подтипа системных вирусов: вирусы пускового сектора и декомпозиционные вирусы. Разница между ними заключается лишь в том, что вирус пускового сектора “оккупирует” пусковой сектор системного драйва (диска), а декомпозиционный вирус проникает в первый (пусковой) сегмент логического несистемного драйва. Поэтому дальнейшее описание будет сосредоточено на вирусе пускового сектора, являющимся наиболее сложным и эффективным.

Вирусы пускового сектора появились совсем недавно. Вообще раньше считалось, что создать такой, более или менее функционирующий, вирус нельзя, поскольку размер пускового сектора ограничен и там почти невозможно разместить какую-либо действующую программу вместе с пусковой записью (boot-strap record). Однако по мере развития техники

программирования был изобретен изощренный механизм, благодаря которому эту задачу удалось решить другим путем.

Детальный механизм работы вируса пускового сектора заключается в том, что сам вирус размещается в первом (пусковом) секторе, замещая пусковую запись своим кодом. Оригинал же пусковой записи он копирует на свободное место на диске. При загрузке ОС загрузчик размещает вирус в оперативной памяти, после чего туда загружается и сам вирус. Данный механизм позволяет создавать вирусы этого типа сложные по структуре и значительно превышающие по размеру пусковой сектор. В этом случае вирус компонуется из двух частей: загрузочной, ограниченной по размеру для размещения в пусковом секторе, и функциональной, размещаемой на свободном дисковом пространстве. После того, как загрузочная часть, попав в оперативную память, берет на себя управление, она находит на диске и загружает в память функциональную часть, затем происходит загрузка пускового записи.

Необходимо особо отметить, что вирус пускового сектора может распространяться не только через системный диск. “Гениальность” описанного выше механизма заключается в том, что пусковой сектор имеется на любом диске единственно, что не все они содержать пусковую запись. Если же пользователь по ошибке пытается запустить компьютер с несистемного (не имеющего пусковую запись) диска, инфицированного вирусом пускового сектора, то компьютер выдаст на экран монитора сообщение об ошибке и попросит сменить диск. Однако считывание пускового сектора происходит в любом случае и, если он содержит вирус, то последний немедленно попадает в оперативную память. После устранения ошибки и смены диска компьютер оказывается зараженным. Существует, правда, простой и надежный способ защиты от попадания вирусов пускового сектора с несистемных дисков: после ошибочной попытки запуска необходимо произвести полную перезагрузку компьютера, то есть очистить оперативную память.

Воздействие системных вирусов чаще всего носит исключительно разрушительный характер. Механизм действия известного всему миру вируса “disk-killer” (разрушитель дисков) основан на последовательном преобразовании двоичных записей дорожек (tracks) с помощью функции XOR, после чего содержание файлов (частей файлов), использующих преобразованные дорожки, превращается в бессмыслицу.

В заключение следует отметить, что в последнее время появились сообщения о достижении существенного прогресса в реализации концепции гибридной диверсионной программы, сочетающей в себе преимущества файлового и системного вирусов. Внешне такая диверсионная программа ведет себя как файловый вирус. Однако после его обнаружения и удаления (повторной инсталляции) зараженных файлов он вновь распространяется по диску, инфицируя файлы из оперативной памяти, куда он попадет с пускового сектора (сегмента).

2.4.3. Механизмы вирусной атаки

Все известные вирусы различаются способом размещения в программном обеспечении, методом распространения в вычислительной среде, способом активизации, характером наносимого ущерба [5, 7, 8, 28, 30, 64 и др.].

Компьютерный вирус может находиться в операционной среде, где он сцепляется с программами, расположенными в системной части накопителя на гибком магнитном диске (НГМД) или на жестком магнитном диске (“винчестере”). Его внутренние поля могут располагаться в структуре файлов типа EXE - в области между таблицей адресов и загрузочным модулем программы или в свободной памяти файла за программой, в библиотеках компиляторов - наиболее эффективном варианте размещения вируса, поскольку он при этом может автоматически внедряться в любую программу, составляемую компилятором, в сетевом драйвере (программном обеспечении работы вычислительной сети), в “плохих” или специальных секторах на диске, в постоянном запоминающем устройстве (ПЗУ) в качестве программно-технической закладки, которую обнаружить весьма трудно.

Рис. 2.1. Классификация компьютерных вирусов

Компьютерный вирус может распространяться транзитно или резидентно. В первом случае, находясь в оперативном запоминающем устройстве (ОЗУ) компьютера, вирус дописывает себя в другие программы, хранимые на диске, во втором случае вирус, введенный в память ЭВМ (в часть, где находятся программы операционной системы (ОС)), при обращениях к ОС “заражает” программы (диски), вызываемые на выполнение.

Активизироваться вирус может: с момента внедрения в средства вычислительной техники, по наступлении определенного события (даты, заданного числа обращений к зараженной программе), случайно (по показанию датчика случайных чисел, содержащегося в вирусе).

Среди вирусов есть такие, которые не создают серьезных помех работе средств вычислительной техники, вызывают нарушения, поддающиеся исправлению, и производят необратимые изменения и разрушения. Наибольшую опасность представляют вирусы, имеющие деструктивную функцию. Эти вирусы наносят следующие виды ущерба вычислительным средствам: изменение данных в файлах данных, изменение назначенного магнитного диска, в результате чего данные записываются на другой диск. Например, данные могут быть направлены на квазидиск в ОС и потеряны после выключения ЭВМ; уничтожение специальных файлов, содержащих выполняемые программы и данные; уничтожение информации форматированием диска или отдельных треков на нем; уничтожение каталога диска; уничтожение (выключение) программ, постоянно находящихся в ОС; нарушение работоспособности ОС, при которой она не воспринимает внешних воздействий и требует полной загрузки.

2.4.4. Дальнейшее развитие “вирусной технологии”

Появление компьютерных вирусов дало сильный толчок процессу разработки методов и развития технологии борьбы с ними, и успехи в этой области очевидны и несомненны. Однако по мере разработки антивирусных средств шли интенсивные изыскания и в направлении совершенствования диверсионных программ. В результате была разработана технология “стелт-вируса” или вируса-невидимки по аналогии с термином стелт-бомбардировщик (stealth-bomber).

Идея заключается в том, чтобы устранить основной признак, выдающий наличие вируса в системе (на диске), - размер файла. ЭТо достигается введением в вирус механизма воздействия на атрибуты файла, а именно на атрибут его размера. Внедрившись в файл и увеличив его размеры, вирус переписывает соответствующий атрибут, считав значение последнего до внедрения, на первоначальную величину. Таким образом, при простой проверке файлов наличие вируса-невидимки обнаружить не удается. Для этого требуется сложная процедура суммирования размеров всех находящихся на диске файлов и файловых структур с фактическим свободным пространством и последующее сравнение полученной величины с объемом диска.

В настоящее время появилась новая разновидность диверсионных программ, предназначенная для поражения компьютеров, работающих в сетях. Это автономная, саморазмножающаяся и медленно распространяющаяся сложная программа, которая по аналогии с крылатой ракетой (cruise missile) получила экзотическое название “круизный вирус” (cruise virus).

Первой важнейшей отличительной особенностью данной диверсионной программы является то, что она попадает в компьютеры через сети. С точки зрения концепций создания диверсионных программ такой подход считается самым перспективным, поскольку развитие информационных технологий идет в направлении объединения СВТ в сети. В ближайшем будущем отдельно работающие компьютеры будут редким исключением. Что же касается, например, даже простых задач управления, то для их решения уже на нынешнем этапе

необходимо в обязательном порядке создавать распределенные информационно-вычислительные архитектуры.

Во-вторых, “круизный вирус” предназначен для осуществления диверсий не вообще в информационной системе, а только в конкретном, четко выбранном компьютере. При этом его даже не обязательно непосредственно внедрять в сеть, к которой подключен компьютер-цель. Подобные диверсионные программы проектируются таким образом, что они могут существовать незамеченными сколько угодно времени до тех пор, пока не достигнут своей цели. Это означает, что “круизному вирусу” необходимо лишь дать возможность попасть в информационное сообщество, например во время общественного форума, “прикрепленным” к сервисной программе, распространяемой на встрече пользователей какой-либо системы.

Мир компьютерных специалистов отличается чрезвычайно тесными контактами и самым активным обменом информацией и программным обеспечением. Здесь совершенно естественным считается использование служебных средств вычислительной техники для копирования игровых программ или печатания личных писем. Более того, в некоторых странах на фирмах и в учреждениях разрешается работать со служебной информацией дома на личном персональном компьютере. Так, старшим офицерам Главного штаба Вооруженных сил Швейцарии в ряде случаев даже разрешается работать дома с секретной информацией.

Все это, несомненно, повышает вероятность того, что “выпущенный на волю” вирус в конце концов достигнет своей цели, даже если он первоначально и не попадет в выбранное для проникновения учреждение или ведомство.

2.4.5. Оценка состояния работ по разработке вирусов

Приведенный выше анализ свидетельствует о широких возможностях по применению компьютерных вирусов для противодействия в информационной сфере, в том числе и в военных целях. Есть основания полагать, что в ряде стран ведутся серьезные изыскательские работы в этом направлении. Так, например, в США в 1990 году Центром по радиоэлектронному противодействию сухопутных войск (US Army Center for Signals Warfare, Warrenton, Virginia) был проведен отбор опытных специалистов по компьютерным вирусам, а также хорошо знающих системы защиты автоматизированных информационных систем и методы их преодоления. Кроме того, Центр организовал конкурс среди компьютерных фирм США на проведение научно-исследовательских работ по изучению возможностей вывода из строя систем управления оружием противника путем внедрения в них диверсионных компьютерных программ (вирусов).

По взглядам экспертов министерства обороны США существует принципиальная возможность внедрения компьютерных вирусов в системы управления противником путем передачи их машинного кода через радиосигналы. Особенно привлекателен такой метод для внедрения диверсионных программ в автоматизированные комплексы обеспечения работы средств ПВО и систем управления боем. При этом также исследуется возможность создания вируса-камикадзе, который бы мог самоуничтожаться после осуществления диверсионного акта. Это позволило бы, во-первых, провести реальные испытания таких диверсионных программ в условиях мирного времени, а во-вторых, исключить попадание в руки противника содержания этих программ.

Наряду с такими экстраординарным методом внедрения прорабатываются и другие, более традиционные направления, и в первую очередь использование для этих целей агентурного проникновения. Учитывая характер и перспективность всех этих работ предпринимаются меры по сохранению в тайне масштабов исследований и их результатов.

3. НАПРАВЛЕНИЯ, МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1. Основные направления обеспечения информационной безопасности

К основным аспектам проблемы обеспечения информационной безопасности относятся [63]:

- защита государственной тайны, т.е. секретной и другой конфиденциальной информации, являющейся собственностью государства, от всех видов несанкционированного доступа, манипулирования и уничтожения;
- защита прав граждан на владение, распоряжение и управление принадлежащей им информацией;
- защита прав предпринимателей при осуществлении ими коммерческой деятельности;
- защита конституционных прав граждан на тайну переписки, переговоров, личную тайну;
- защита технических и программных средств информатики от ошибочных действий персонала и техногенных воздействий, а также стихийных бедствий и иных форс-мажорных обстоятельств с целью сохранения возможности управления процессом обработки.

В настоящее время в проблеме защиты информационного ресурса существует два направления, отличающихся по существу общественных отношений и формой организации. Это защита государственного информационного ресурса и защита информации независимого сектора экономики.

Функционально государственная система защиты информации должна в полной мере обеспечивать решение таких задач, как:

- разработка общей технической политики и концепций обеспечения безопасности информации;
- разработка законодательно-правового обеспечения проблемы, участие в подготовке законодательных актов в смежных областях;
- координация деятельности органов государственного управления по отдельным направлениям защиты информации;
- разработка нормативно-технических и организационно-распорядительных документов;
- сертификация технических и программных средств по требованиям безопасности;
- лицензирование деятельности по оказанию услуг в сфере безопасности информации;
- надзор (контроль);
- подготовка кадров;
- финансирование важнейших научно-исследовательских и опытно-конструкторских работ;
- страхование;
- информационное обеспечение.

Формирование облика системы защиты информации является сложной системной задачей. В разных странах она сильно различается по содержанию и зависит от таких факторов, как научный потенциал страны, степень внедрения средств информатизации в жизнь общества и экономику, развитие производственной базы, ориентация потребителя и, в первую очередь, армии и государственных структур на приобретение отечественных

средств вычислительной техники или на закупку их по импорту, общей культуры общества и, наконец, традиций и норм поведения субъектов правоотношений.

Рис. 3.1. Основные направления деятельности по защите информации

Основными направлениями деятельности по защите информации в организациях являются (рис. 3.1):

1. Законодательно-правовое обеспечение, представляющее собой взаимоувязанный комплекс законодательных и иных правовых актов, устанавливающих правовой статус субъектов правоотношений, субъектов и объектов защиты, методы, формы и способы защиты и их правовой статус.

Следует особо отметить необходимость законодательно-правового обеспечения таких важных аспектов деятельности системы защиты, как сертификация и лицензирование.

Система законодательных актов и разработанных на их базе нормативных и организационно-распорядительных документов должна обеспечивать организацию эффективного надзора за их исполнением со стороны правоохранительных органов и реализацию мер судебной защиты.

2. Организационно-техническое обеспечение, которое представляет собой комплекс взаимокоординируемых мероприятий и технических мер, реализующих практические механизмы защиты. Условно эти мероприятия подразделяются на системообразующие и

надзорные (контрольные). Особенностью надзорных мероприятий является необходимость создания независимого, внеотраслевого надзора за защитой и уровнем безопасности информации.

3. Страховое обеспечение предназначено для защиты собственника информации или средств информатизации как от традиционных угроз (краж, стихийных бедствий), так и от угроз, возникающих в ходе информатизации общества. К ним относятся утечки информации, хищения, модификации, уничтожение, отказы в обслуживании и др.

Весьма остро стоит вопрос защиты от военного и промышленного шпионажа и страхование риска.

Система защиты информации должна отвечать следующим требованиям:

1. Обеспечивать безопасность информации, средств информатизации, защиту интересов участников информационных отношений. Решение этой задачи достигается комплексной реализацией законодательной, организационно-технической и страховой форм защиты.
2. Система в целом, методы и способы защиты должны быть по возможности “прозрачными” для пользователя, не создавать ему дополнительных неудобств, связанных с процедурами проверки полномочий и контроля доступа к информации.
3. Система должна реализовывать методы как директивного, так и функционального управления.

3.2. Классификация методов и средств защиты информации

Все мероприятия по защите информации в общем плане должны обеспечить достижение следующих целей:

- предупреждение появления угроз информации;
- выявление возможных направлений и степени нарастания опасности нарушения безопасности информации;
- обнаружение реальных фактов нарушения безопасности информации;
- пресечение разглашения, утечки и несанкционированного доступа к информации, нарушения ее целостности и потери;
- ликвидацию или снижение уровня ущерба от нарушения безопасности информации и ее использования злоумышленниками.

Рассмотрим основные способы защиты информации (рис. 3.2). Препятствия физически преграждают злоумышленнику путь к защищаемой информации (т.е. на территорию и в помещения с аппаратурой, носителями информации и т.п.).

Управление доступом - способ защиты информации регулированием использования всех ресурсов систем (технических, программ средств, элементов баз данных). Предполагается, что в системе обработки данных установлены четкие и однозначные регламенты работы для пользователей, технического персонала программных средств, элементов баз данных и носителей информации.

В системе обработки данных должны быть регламентированы дни недели и время суток, в которые разрешена работа пользователям и персоналу системы.

В дни работы персонала должен быть определен перечень ресурсов системы, к которым разрешен доступ и порядок доступа к ним.

Необходимо иметь список лиц, которым предоставлено право на использование технических средств, программ и функциональных задач.

Для элементов баз данных указываются список пользователей, имеющих право доступа, и перечень процедур.

Для носителей информации строго определяются место постоянного хранения, список лиц, имеющих право получать их, перечень программ, имеющих право обращения к носителям.

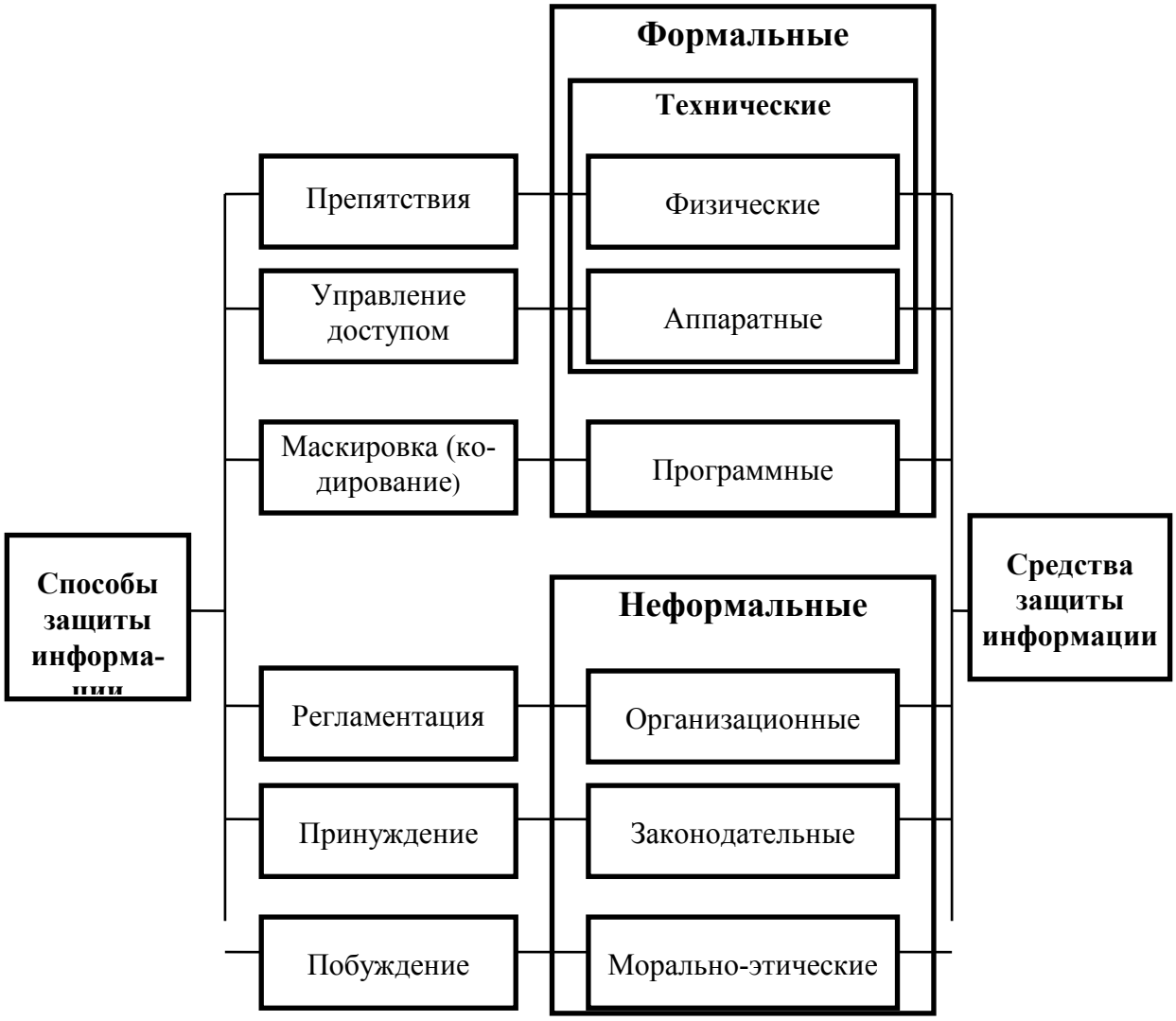

Рис. 3.2. Способы и средства защиты информации

Собственно управление доступом включает следующие функции защиты:

- идентификацию пользователей, персонала и ресурсов системы, причем под идентификацией понимается присвоение каждому названному выше объекту персонального идентификатора (имени, кода, пароля и т.п.) и опознание (установление подлинности) субъекта или объекта по предъявленному им идентификатору;

- проверку полномочий, заключающуюся в проверке соответствия дня недели, времени суток, а также запрашиваемых ресурсов и процедур установленному регламенту;
- разрешение и создание условий работы в пределах (и только в пределах) установленного регламента;
- регистрацию (протоколирование) обращений к защищаемым ресурсам;
- реагирование (задержка работ, отказ, отключение, сигнализация) при попытках несанкционированных действий.

Маскировка - способ защиты информации путем ее криптографического закрытия. Специалисты считают криптографическое закрытие весьма эффективным как с точки зрения собственно защиты, так и с точки зрения наглядности для пользователей. За рубежом этот вид защиты широко применяется как при обработке, так и при хранении информации. При передаче информации по линиям связи большой протяженности криптографическое закрытие является единственным способом надежной ее защиты.

Регламентация как способ защиты заключается в разработке и реализации в процессе функционирования систем обработки данных комплексов мероприятий, создающих такие условия автоматизированной обработки и хранения защищаемой информации, при которых возможности несанкционированного доступа к ней сводились бы к минимуму.

Специалисты утверждают [24, 49, 57], что для эффективной защиты необходимо строго регламентировать структурное построение (архитектура зданий, оборудование помещений, размещение аппаратуры и т.п.), технологические схемы автоматизированной обработки защищаемой информации, организацию и обеспечение работы всего персонала, занятого обработкой информации и т.п.

Принуждение - такой способ защиты, при котором пользователи и персонал систем обмена данными вынуждены соблюдать правила обработки и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.

Рассмотренные способы защиты информации реализуются применением различных средств защиты. Различают технические, программные, организационные, законодательные и морально-этические средства (рис. 3.2).

Техническими называются средства, которые реализуются в виде электрических, электромеханических, электронных устройств. Всю совокупность технических средств принято делить на аппаратные и физические. Под аппаратными техническими средствами защиты понимаются устройства, встраиваемые непосредственно в аппаратуру систем обработки данных, или устройства, которые сопрягаются с аппаратурой по стандартному интерфейсу. Наиболее известные аппаратные средства, используемые на первом этапе - это схемы контроля информации по четности, схемы защиты полей памяти по ключу, специальные регистры (например, регистры границ поля запоминающих устройств) и т.п.

Физическими называются такие средствами, которые реализуются в виде автономных устройств и систем (электронно-механическое оборудование охранной сигнализации и наблюдения, замки на дверях, решетки на окнах и т.п.).

Программные средства защиты образуют программы, специально предназначенные для выполнения функций, связанных с защитой информации.

Организационными средствами защиты называются организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуата-

ции систем для обеспечения защиты информации. Организационные мероприятия охватывают все структурные элементы систем обработки данных на всех этапах их жизненного цикла: строительство помещений, проектирование системы, монтаж и наладка оборудования, испытания и проверки, эксплуатация.

К законодательным средствам защиты относятся законодательные акты, которыми регламентируются правила использования и обработки информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил.

К морально-этическим средствам защиты относятся всевозможные нормы, которые сложились традиционно или складываются по мере распространения вычислительных средств в стране или обществе. Эти нормы большей частью не являются обязательными, как законодательные меры, однако несоблюдение их ведет обычно к потере авторитета, престижа человека или группы лиц (организаций).

Морально-этические нормы бывают как “неписаные” (например, общепринятые нормы честности, патриотизма и т.п.), так и регламентированные в законодательном порядке, т.е. в виде свода правил и предписаний. Наиболее характерным примером таких норм является Кодекс профессионального поведения членов Ассоциации пользователей ЭВМ США [84, 85].

Все рассмотренные средства защиты делятся на формальные и неформальные. К первым относятся средства, выполняющие защитные функции строго по заранее предусмотренной процедуре и без непосредственного участия человека. К неформальным средствам отнесены такие, которые либо определяются целенаправленной деятельностью людей, либо регламентируют (непосредственно или косвенно) эту деятельность.

На первом этапе развития концепций защиты информации преимущественное развитие имели программные средства, второй этап характеризовался интенсивным развитием всех основных классов средств, на третьем этапе все определенней вырисовываются следующие тенденции:

- аппаратная реализация основных функций защиты;
- создание комплексных средств защиты, выполняющих несколько различных функций защиты;
- унификация и стандартизация средств.

ЧАСТЬ 2. ЗАКОНОДАТЕЛЬНО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4. ЗАКОНОДАТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ ПО ВОПРОСАМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1. Основы законодательства России по вопросам защиты информации

Законодательные меры по защите информации предусматривают создание в стране законодательной базы, предусматривающей разработку новых или корректировку существующих законов, положений, постановлений и инструкций, а также создание действенной системы контроля за исполнением указанных документов.

В настоящее время такая законодательная база создается. По состоянию на начало 1998 года она, прежде всего, включает пакет Федеральных законов, Указов Президента РФ, постановлений Правительства РФ, межведомственных руководящих документов и стандартов, перечень которых приведен в Приложении 2.

Указом Президента РФ от 17 декабря 1997 года № 1300 утверждена **“Концепция национальной безопасности Российской Федерации”**, в которой указывается на необходимость защиты государственного информационного ресурса от утечки важной политической, экономической, научно-технической и военной информации.

Важнейшими задачами обеспечения национальной безопасности Российской Федерации в информационной сфере определены:

- установление необходимого баланса между потребностью в свободном обмене информацией и допустимыми ограничениями ее распространения;
- совершенствование информационной структуры, ускорение развития новых информационных технологий и их широкое распространение, унификация средств поиска, сбора, хранения, обработки и анализа информации с учетом вхождения России в глобальную информационную структуру;
- разработка соответствующей нормативно-правовой базы и координация, при ведущей роли Федерального агентства правительственной связи и информации при Президенте Российской Федерации (ФАПСИ), деятельности федеральных органов государственной власти и других органов, решающих задачи обеспечения информационной безопасности;
- развитие отечественной индустрии телекоммуникационных и информационных средств, их приоритетное по сравнению с зарубежными аналогами распространение на внутреннем рынке;
- защита государственного информационного ресурса, прежде всего в федеральных органах государственной власти и на предприятиях оборонного комплекса.

В принятом в 1996 году **Уголовном кодексе Российской Федерации**, как наиболее сильнодействующем законодательном акте по предупреждению преступлений и привлече-

нию преступников и нарушителей к уголовной ответственности, вопросам безопасности информации посвящены следующие главы и статьи:

- Глава 19. Преступления против конституционных прав и свобод человека и гражданина
  - Статья 137. Нарушение неприкосновенности частной жизни
  - Статья 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений
  - Статья 139. Нарушение неприкосновенности жилища
  - Статья 140. Отказ в предоставлении гражданину информации
  - Статья 144. Воспрепятствование законной профессиональной деятельности журналистов
  - Статья 146. Нарушение авторских и смежных прав
  - Статья 147. Нарушение изобретательских и патентных прав
- Глава 23. Преступления против интересов службы в коммерческих и иных организациях
  - Статья 201. Злоупотребление полномочиями
  - Статья 203. Превышение полномочий служащими частных охранных или детективных служб
- Глава 22. Преступления в сфере экономической деятельности
  - Статья 183. Незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну
  - Статья 189. Незаконный экспорт технологий, научно-технической информации и услуг, используемых при создании оружия массового поражения, вооружения и военной техники
- Глава 25. Преступления против здоровья населения и общественной нравственности
  - Статья 237. Сокрытие информации об обстоятельствах, создающих опасность для жизни и здоровья людей
- Глава 29. Преступления против основ конституционного строя и безопасности государства
  - Статья 275. Государственная измена
  - Статья 276. Шпионаж
  - Статья 283. Разглашение государственной тайны
  - Статья 284. Утрата документов, содержащих государственную тайну

Особо важное значение имеет введение в Уголовный кодекс специальной главы, посвященной компьютерным преступлениям:

- Глава 28. Преступления в сфере компьютерной информации
  - Статья 272. Неправомерный доступ к компьютерной информации

1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, - *наказывается штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.*
2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой, либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, - *наказывается штрафом в размере от пятисот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или другого дохода осужденного за период от пяти до восьми месяцев, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.*

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

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

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

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

Большое значение имеет и **Гражданский кодекс Российской Федерации** принятый Государственной Думой 21 октября 1994 года. В частности, следующие главы и статьи:

- Глава 6. Общие положения.
  - Статья 138. Интеллектуальная собственность.
  - Статья 139. Служебная и коммерческая тайна.
    Информация составляет *служебную* или *коммерческую тайну* в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицом, к ней нет свободного доступа на законном основании и обладатель информации принимает меры к охране ее конфиденциальности.
- Глава 38. Выполнение научно-исследовательских, опытно-конструкторских и технологических работ.
  - Статья 771. Конфиденциальность сведений, составляющих предмет договора.
    Объем сведений , признаваемых конфиденциальными определяется в договоре.
- Глава 45. Банковский счет.
  - Статья 857. Банковская тайна.
- Глава 48. Страхование
  - Статья 946. Тайна страхования.

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

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

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

нимаемых мер защиты. В частности, такие вопросы возникают применительно к трактовке содержания категорий “служебная тайна” и “конфиденциальная информация”.

4.2. Важнейшие законодательные акты в области защиты информации

4.2.1. Закон РФ “О государственной тайне ”

Закон Российской Федерации от 21 июля 1993 года № 5485-1 **“О государственной тайне”** с изменениями и дополнениями, внесенными Федеральным законом от 6 октября 1997 года № 131-ФЗ **“О внесении изменений и дополнений в Закон Российской Федерации “О государственной тайне”** регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации.

Положения Закона обязательны для исполнения на территории Российской Федерации и за ее пределами органами представительной, исполнительной и судебной властей (далее - органы государственной власти), местного самоуправления, предприятиями, учреждениями и организациями независимо от их организационно-правовой формы и формы собственности, должностными лицами и гражданами Российской Федерации, взявшими на себя обязательства либо обязанными по своему статусу исполнять требования законодательства Российской Федерации о государственной тайне (статья 1).

В Законе используются следующие основные понятия:

- **государственная тайна** - защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации;
- **носители сведений, составляющих государственную тайну**, - материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов;
- **система защиты государственной тайны** - совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях;
- **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;
- **доступ к сведениям, составляющим государственную тайну** - санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну;
- **гриф секретности** - реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него;
- **средства защиты информации** - технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

Законодательство Российской Федерации о государственной тайне основывается на Конституции Российской Федерации, Законе Российской Федерации “О безопасности” и включает настоящий Закон, а также положения других актов законодательства, регулирующих отношения, связанные с защитой государственной тайны (статья 3).

В Законе определяются и законодательно закрепляются полномочия органов государственной власти и должностных лиц в области отнесения сведений к государственной тайне и их защиты (статья 4), а также определяется в общем виде перечень сведений, которые могут быть отнесены к государственной тайне (раздел 2 Закона № 5485-1 с изменениями, внесенными статьей 6 Закона № 131-ФЗ).

Засекречивание сведений и их носителей - введение в предусмотренном Законом порядке для сведений, составляющих государственную тайну, ограничений на их распространение и на доступ к их носителям. Засекречивание сведений осуществляется в соответствии с принципами законности, обоснованности и своевременности.

Законность засекречивания сведений заключается в соответствии засекречиваемых сведений положениям статей 5 и 7 Закона и законодательству Российской Федерации о государственной тайне.

Обоснованность засекречивания сведений заключается в установлении путем экспертной оценки целесообразности засекречивания конкретных сведений, вероятных экономических и иных последствий этого акта исходя из баланса жизненно важных интересов государства, общества и граждан.

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

Отнесение сведений к государственной тайне осуществляется в соответствии с их отраслевой, ведомственной или программно-целевой принадлежностью.

Обоснование необходимости отнесения сведений к государственной тайне в соответствии с принципами засекречивания сведений возлагается на органы государственной власти, предприятия, учреждения и организации, которыми эти сведения получены (разработаны).

Отнесение сведений к государственной тайне осуществляется руководителями органов государственной власти в соответствии с **Перечнем должностных лиц, наделенных полномочиями по отнесению сведений к государственной тайне**, утверждаемым Распоряжением Президента РФ от 30 мая 1997 года № 226-рп. Указанные лица несут персональную ответственность за принятые ими решения о целесообразности отнесения конкретных сведений к государственной тайне.

Закон четко определяет сведения, не подлежащие засекречиванию (статья 7):

- о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях;
- о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;

- о привилегиях, компенсациях и льготах, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям;
- о фактах нарушения прав и свобод человека и гражданина;
- о размерах золотого запаса и государственных валютных резервах Российской Федерации;
- о состоянии здоровья высших должностных лиц Российской Федерации;
- о фактах нарушения законности органами государственной власти и их должностными лицами.

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

В Законе устанавливаются три степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведений: **“особой важности”, “совершенно секретно”** и **“секретно”.**

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

Статья 12 Закона определяет реквизиты носителей сведений, составляющих государственную тайну.

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

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

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

Раздел VI, статья 20 Закона относит к органам, осуществляющим защиту государственной тайны на территории Российской Федерации:

- межведомственную комиссию по защите государственной тайны;
- органы федеральной исполнительной власти (Министерство безопасности Российской Федерации, Министерство обороны Российской Федерации, Федеральное агентство правительственной связи и информации при Президенте Российской Федерации), Служба внешней разведки Российской Федерации, Государственная техническая комиссия при Президенте Российской Федерации и их органы на местах;

- органы государственной власти, предприятия, учреждения и организации и их структурные подразделения по защите государственной тайны.

Допуск должностных лиц и граждан Российской Федерации к государственной тайне осуществляется в добровольном порядке.

Допуск лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов к государственной тайне осуществляется в порядке, устанавливаемом Правительством Российской Федерации.

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 настоящего Закона;
- письменное согласие на проведение в отношении их полномочными органами проверочных мероприятий;
- определение видов, размеров и порядка предоставления льгот, предусмотренных настоящим Законом;
- ознакомление с нормами законодательства Российской Федерации 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.

Объем проверочных мероприятий зависит от степени секретности сведений, к которым будет допускаться оформляемое лицо.

Закон (статья 27) определяет порядок допуска предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну и порядок сертификации средств защиты информации (статья 28).

Допуск предприятий, учреждений и организаций к 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, осуществляется путем получения ими в порядке, устанавливаемом Правительством Российской Федерации, лицензий на проведение работ со сведениями соответствующей степени секретности.

Лицензия на проведение указанных работ выдается на основании результатов специальной экспертизы предприятия, учреждения и организации и государственной аттестации их руководителей, ответственных за защиту сведений, составляющих государственную тайну, расходы по проведению которых относятся на счет предприятия, учреждения, организации, получающих лицензию.

Лицензия на проведение работ с использованием сведений, составляющих государственную тайну, выдается предприятию, учреждению, организации при выполнении ими следующих условий:

- выполнение требований нормативных документов, утверждаемых Правительством Российской Федерации, по обеспечению защиты сведений, составляющих государственную тайну, в процессе выполнения работ, связанных с использованием указанных сведений;

- наличие в их структуре подразделений по защите государственной тайны и специально подготовленных сотрудников для работы по защите информации, количество и уровень квалификации которых достаточны для обеспечения защиты государственной тайны;
- наличие у них сертифицированных средств защиты информации.

Средства защиты информации должны иметь сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности.

Организация сертификации средств защиты информации возлагается на Государственную техническую комиссию при Президенте Российской Федерации, Федеральное агентство правительственной связи и информации при Президенте Российской Федерации, Федеральную службу безопасности Российской Федерации, Министерство обороны Российской Федерации в соответствии с функциями, возложенными на них законодательством Российской Федерации. Сертификация осуществляется на основании требований государственных стандартов Российской Федерации и иных нормативных документов, утверждаемых Правительством Российской Федерации.

Координация работ по организации сертификации средств защиты информации возлагается на Межведомственную комиссию по защите государственной тайны.

4.2.2. Закон РФ “Об информации, информатизации и защите информации”

Федеральный закон от 20 февраля 1995 года № 24-ФЗ **“Об информации, информатизации и защите информации”** (далее для краткости - “Закон об информации”) является одним из основных базовых законов в области защиты информации, который регламентирует отношения, возникающие при формировании и использовании информационных ресурсов Российской Федерации на основе сбора, накопления, хранения, распространения и предоставления потребителям документированной информации, а также при создании и использовании информационных технологий, при защите информации и прав субъектов, участвующих в информационных процессах и информатизации.

В соответствие с этим Законом должны быть приведены ранее изданные Президентом Российской Федерации и Правительством Российской Федерации правовые акты, а также все законодательство России (статья 25 Закона).

Закон гласит, что:

- информационные ресурсы делятся на государственные и негосударственные (статья 6, часть 1);
- государственные информационные ресурсы Российской Федерации формируются в соответствии со сферами ведения как: федеральные информационные ресурсы; информационные ресурсы, находящиеся в совместном ведении Российской Федерации и субъектов Российской Федерации; информационные ресурсы субъектов Российской Федерации (статья 7, часть 1);
- государственные информационные ресурсы являются открытыми и общедоступными. Исключение составляет документированная информация, отнесенная законом к категории ограниченного доступа (статья 10, часть 1);

- документированная информация с ограниченного доступа по условиям ее правового режима подразделяется на информацию, отнесенную к государственной тайне, и конфиденциальную (статья 10, часть 2).
- конфиденциальная информация - документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации (статья 2);
- Персональные данные о гражданах, включаемые в состав федеральных информационных ресурсов, информационных ресурсов совместного ведения, информационных ресурсов субъектов Российской Федерации, информационных ресурсов местного самоуправления, а также получаемые и собираемые негосударственными организациями, отнесены к категории конфиденциальной информации (статья 11, часть 1).

Из содержания Закона следует, что:

- информация из любой области знаний и деятельности в принципе является открытой и общедоступной, если законодательством не предусмотрено ограничение доступа к ней в установленном порядке;
- категория "конфиденциальная информация", в соответствии с понятием, приведенным выше из статьи 2 "Закона об информации", объединяет все виды защищаемой информации (тайн). Это относится и к государственным и к негосударственным информационным ресурсам. При этом, исключение составляет информация, отнесенная к государственной тайне: она к конфиденциальной информации не относится, а является составной частью информации с ограниченным доступом (основание - статья 10, часть 2 указанного Закона). Этому положению "Закона об информации" не соответствует статья 8 Федерального закона **"Об участии в международном информационном обмене"** (1996 год), в которой делается ссылка на государственную тайну "или иную конфиденциальную информацию" (то есть информация, составляющая государственную тайну, является здесь составной частью конфиденциальной информации).

Все категории государственных информационных ресурсов можно представить следующим образом:

- открытая общедоступная информация во всех областях знаний и деятельности;
- информация с ограниченным доступом:
    - информация, отнесенная к государственной тайне;
    - конфиденциальная информация;
    - персональные данные о гражданах (относятся к категории конфиденциальной информации, но регламентируются отдельным законом)

В соответствии с "Законом об информации" режим защиты информации устанавливается (статья 21):

- в отношении сведений, отнесенных к государственной тайне, - уполномоченными органами на основании Закона Российской Федерации **"О государственной тайне"**;
- в отношении конфиденциальной информации - собственником информационных ресурсов или уполномоченным лицом на основании "Закона об информации";
- в отношении персональных данных - отдельным федеральным законом.

Принципиальным здесь является положение, что режим защиты конфиденциальной информации определяет ее собственник, то есть соответствующий орган государственной власти или управления, организация, учреждение, предприятие.

Категория “служебная тайна” ранее применялась для обозначения сведений ведомственного характера с грифом “секретно” и за ее разглашение предусматривалась уголовная ответственность. В настоящее время эта категория из Уголовного кодекса изъята и в прежнем ее понимании из правового поля исчезла в связи с принятием в июле 1993 года Закона **“О государственной тайне”** по двум причинам:

- во-первых, информация с грифом “секретно” теперь составляет государственную тайну;
- во-вторых, применение грифов секретности для других категорий информации не допускается в соответствии со статьей 8 Закона “О государственной тайне”.

Вместе с тем, **Гражданским кодексом Российской Федерации**, введенным в действие с 1995 года, предусмотрена категория “служебная тайна” в сочетании с категорией “коммерческая тайна”. Статья 139 Кодекса гласит:

1. Информация составляет служебную или коммерческую тайну в случае, если 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.
2. Информация, составляющая служебную или коммерческую тайну, защищается способами, предусмотренными настоящим Кодексом и другими законами.

Из этого следует, что произошло изменение содержания категории “служебная тайна”: с января 1995 года под ней (по аналогии с коммерческой тайной в негосударственных структурах) следует понимать служебную информацию в государственных структурах, имеющую коммерческую ценность. В отличие от коммерческой тайны (в коммерческих структурах) защищаемая государством конфиденциальная информация не ограничивается только коммерческой ценностью, поэтому служебная тайна является составной частью конфиденциальной информации. В государственных структурах еще может быть информация, имеющая политическую или иную ценность. Поскольку к служебной тайне она не относится, ей необходимо присваивать гриф “конфиденциально” или иной гриф (к примеру, “для служебного пользования”, применяемый в органах исполнительной власти и установленный постановлением Правительства Российской Федерации от 3 ноября 1994 г. № 1233).

Такая трактовка категории “служебная тайна” соответствует проекту Федерального закона **“О коммерческой тайне”**, где предусмотрено при передачи информации с грифом “коммерческая тайна” в государственные органы охранять ее как служебную тайну (статья 18, часть 1 проекта Закона).

За разглашение служебной тайны уголовная ответственность новым **Уголовным кодексом Российской Федерации** не предусмотрена, в отличие от коммерческой тайны (статья 183).

Кроме того, Федеральный закон от 6 мая 1998 года № 69-ФЗ **“О внесении изменений и дополнений в статью 15 Кодекса законов о труде Российской Федерации”** (СЗ РФ № 19-98, ст. 2065) дополнил статью 15 Кодекса частью второй следующего содержания: “В случаях, предусмотренных федеральными законами и иными нормативными правовыми

актами Российской Федерации, в трудовом договоре могут содержаться условия неразглашения работником сведений, составляющих служебную или коммерческую тайну, ставших известными работнику в связи с исполнением им своих должностных обязанностей".

Следует подчеркнуть, что в одном и том же органе государственной власти (управления), в государственной или коммерческой организации могут циркулировать несколько видов информации, как своей, так и "чужой", то есть других собственников информации, которые передали ее им в установленном порядке.

К примеру, в Центральном банке России это государственная тайна, конфиденциальная информация (в том числе служебная тайна), банковская тайна, коммерческая тайна коммерческих банков.

В коммерческом банке это государственная тайна и конфиденциальная информация, переданные ему государственными органами или организациями в установленном порядке; банковская тайна, коммерческая тайна о его коммерческой деятельности.

При этом следует подчеркнуть, что охрана в кредитных организациях, в Центральном банке России тайны об операциях, о счетах и вкладах клиентов и корреспондентов (банковская тайна), а также иных сведений, устанавливаемых кредитной организацией, предусмотрено статьей 26 Федерального закона **"О банках и банковской деятельности"**. Под иными сведениями, необходимо понимаются сведения о "производственной" (коммерческой) деятельности соответствующей организации, не подпадающие под понятие банковской тайны, но так же, как и она, не подлежащие, по решению этой организации, широкому распространению.

Очевидно, что организация защиты информации в государственных и коммерческих кредитных организациях имеет свою специфику и требует единого подхода и координации со стороны Центрального банка России.

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

- предотвращение утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования, блокирования информации и т.п., вмешательства в информацию и информационные системы;
- сохранение полноты, достоверности, целостности информации, ее массивов и программ обработки данных, установленных собственником или уполномоченным им лицом;
- сохранение возможности управления процессом обработки, пользования информацией в соответствии с условиями, установленными собственником или владельцем информации;
- обеспечение конституционных прав граждан на сохранение личной тайны и конфиденциальности персональной информации, накапливаемой в банках данных;
- сохранение секретности или конфиденциальности информации в соответствии с правилами, установленными действующим законодательством и другими законодательными или нормативными актами;
- соблюдение прав авторов программно-информационной продукции, используемой в информационных системах.

Статья 19 Закона устанавливает обязательность сертификации средств обработки и защиты документированной информации с ограниченным доступом, предназначенных для обслуживания граждан и организаций, а также обязательность получения лицензий для организаций, осуществляющих проектирование и производство средств защиты информации.

Статья 20 определяет основные цели защиты информации. В соответствии с этой статьей таковыми, в частности, являются:

- предотвращение утечки, хищения, утраты, искажения и подделки информации;
- предотвращение угроз безопасности личности, общества и государства;
- предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;
- защита конституционных прав на сохранение личной тайны и конфиденциальности персональных сведений;
- сохранение государственной тайны и конфиденциальности информации.

Пункт 3 статьи 21 возлагает контроль за соблюдением требований к защите информации, за эксплуатацией специальных средств защиты информации, а также обеспечение организационных мер защиты информационных систем, обрабатывающих информацию с ограниченным доступом в негосударственных структурах, на органы государственной власти.

Это означает, что контроль состояния защиты должен охватывать все три составляющие информации с ограниченным доступом, входящей в государственные информационные ресурсы:

- информацию, составляющую государственную тайну;
- конфиденциальную информацию;
- персональные данные о гражданах.

При этом, контроль в равной степени должен охватывать и негосударственные структуры при наличии у них (при передаче им на законном основании) указанных видов информации, входящих в государственные информационные ресурсы.

Очень важна статья 22, которая определяет права и обязанности субъектов в области защиты информации. В частности, пункты 2 и 5 обязывают владельца информационной системы обеспечивать необходимый уровень защиты конфиденциальной информации и оповещать собственников информационных ресурсов о фактов нарушения режима защиты информации. Пунктом 3 риск, связанный с использованием не сертифицированных информационных систем и средств их обеспечения и защиты, возлагается на собственника (владельца) систем и средств. Риск, связанный с использованием информации, полученной из таких систем, относится на потребителя информации. Пункт 4 устанавливает право собственника документов или информационной системы обращаться в организации, осуществляющие сертификацию средств защиты таких систем, для проведения анализа достаточности мер защиты его ресурсов и систем и получения консультаций.

Статья 23 Закона посвящена защите прав субъектов в сфере информационных процессов и информатизации. Статья устанавливает, что защита прав субъектов в данной сфере осуществляется судом, арбитражным судом и третейскими судами, которые могут создаваться на постоянной или временной основе.

4.3. Защита конфиденциальной информации

Защита сведений конфиденциального характера юридически обеспечивается **Перечнем сведений конфиденциального характера**, введенным Указом Президента Российской Федерации от 6 марта 1997 года № 188 и рассмотренными выше законодательными актами.

Согласно Указа, к сведениям конфиденциального характера относятся:

1. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.
2. Сведения, составляющие тайну следствия и судопроизводства.
3. Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна).
4. Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее).
5. Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна).
6. Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

4.4. Пакет руководящих документов Государственной технической комиссии при Президенте Российской Федерации

В 1992 году Государственная техническая комиссия при Президенте РФ опубликовала пять “Руководящих документов”, посвященных проблеме защиты от несанкционированного доступа (НСД) к информации, обрабатываемой средствами вычислительной техники (СВТ) и автоматизированными системами (АС) [51-54]:

1. “Руководящий документ. Концепция защиты средств вычислительной техники (СВТ) и автоматизированных систем (АС) от несанкционированного доступа (НСД) к информации”.- Гостехкомиссия России, 30 марта 1992 года.
2. “Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации”.- Гостехкомиссия России, 30 марта 1992 года.
3. “Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации”.- Гостехкомиссия России, 30 марта 1992 года.
4. “Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД в автоматизированных системах и средствах вычислительной техники”.- Гостехкомиссия России, 30 марта 1992 года.
5. “Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения”.- Гостехкомиссия России, 30 марта 1992 года.

В 1997 году к этим документам добавился еще один [50]:

6. “Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации”. //Защита Информации. Конфидент. - 1997. - № 6. - С. 26-31.

4.4.1. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации

Центральным элементом (идейной основой) набора руководящих документов Гостехкомиссии является **“ Руководящий документ. Концепция защиты средств вычислительной техники (СВТ) и автоматизированных систем (АС) от несанкционированного доступа (НСД) к информации”** [52]. В этом документе излагается система взглядов и основных принципов, которые закладываются в основу проблемы защиты информации от НСД, являющейся частью общей проблемы безопасности информации.

В “Концепции” различаются два понятия, соответствующие двум группам критериев безопасности - **показатели защищенности средств вычислительной техники** и **критерии защищенности автоматизированных систем**, аналогично тому, как в Европейских Критериях проводится деление на продукты и системы. Более точно, “Концепция” предусматривает существование двух относительно самостоятельных и, следовательно, имеющих отличие направлений в проблеме защиты информации от НСД (и только от НСД). Это - направление, связанное с СВТ, и направление, связанное с АС. Отличие двух направлений порождено тем, что СВТ разрабатываются и поставляются на рынок лишь как элементы, из которых в дальнейшем строятся функционально ориентированные АС, и поэтому, не решая прикладных задач, СВТ не содержат пользовательской информации.

Помимо пользовательской информации при создании автоматизированных систем появляются такие отсутствующие при разработке СВТ характеристики АС, как полномочия пользователей, модель нарушителя, технология обработки информации.

Существуют различные способы покушения на информационную безопасность: радиотехнические, акустические, программные и т.п. Среди них НСД выделяется как *“доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых СВТ или АС”*. Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения СВТ или АС.

В разделе 3 “Концепции” формулируются основные принципы защиты от НСД к информации:

3.1. Защита СВТ и АС основывается на положениях и требованиях существующих законов, стандартов и нормативно-методических документов по защите от НСД к информации.

3.2. Защита СВТ обеспечивается комплексом программно-технических средств.

3.3. Защита АС обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер.

3.4. Защита АС должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.

3.5. Программно-технические средства защиты не должны существенно ухудшать основные функциональные характеристики АС (надежность, быстродействие, возможность изменения конфигурации АС).

3.6. Неотъемлемой частью работ по защите является оценка эффективности средств защиты, осуществляемая по методике, учитывающей всю совокупность технических характеристик оцениваемого объекта, включая технические решения и практическую реализацию средств защиты.

3.7. Защита АС должна предусматривать контроль эффективности средств защиты от НСД. Этот контроль может быть либо периодическим, либо инициироваться по мере необходимости пользователем АС или контролирующими органами.

В качестве главного средства защиты от НСД к информации в разделе 6 “Концепции” рассматривается система разграничения доступа (СРД) субъектов к объектам доступа:

6.1. Обеспечение защиты СВТ и АС осуществляется:

- системой разграничения доступа (СРД) субъектов к объектам доступа;
- обеспечивающими средствами для СРД.

6.2. Основными функциями СРД являются:

- реализация правил разграничения доступа (ПРД) субъектов и их процессов к данным;
- реализация ПРД субъектов и их процессов к устройствам создания твердых копий;
- изоляция программ процесса, выполняемого в интересах субъекта, от других субъектов;
- управление потоками данных с целью предотвращения записи данных на носители несоответствующего грифа;
- реализация правил обмена данными между субъектами для АС и СВТ, построенных по сетевым принципам.

6.3. Обеспечивающие средства для СРД выполняют следующие функции:

- идентификацию и опознание (аутентификацию) субъектов и поддержание привязки субъекта к процессу, выполняемому для субъекта;
- регистрацию действий субъекта и его процесса; предоставление возможностей исключения и включения новых субъектов и объектов доступа, а также изменение полномочий субъектов;
- реакцию на попытки НСД, например, сигнализацию, блокировку, восстановление после НСД;
- тестирование;
- очистку оперативной памяти и рабочих областей на магнитных носителях после завершения работы пользователя с защищаемыми данными;
- учет выходных печатных и графических форм и твердых копий в АС;
- контроль целостности программной и информационной части как СРД, так и обеспечивающих ее средств.

6.4. Ресурсы, связанные как с СРД, так и с обеспечивающими ее средствами, включаются в объекты доступа.

6.5. Способы реализации СРД зависят от конкретных особенностей СВТ и АС. Возможно применение следующих способов защиты и любых их сочетаний:

•распределенная СРД и СРД, локализованная в программно-техническом комплексе (ядро защиты);

•СРД в рамках операционной системы, СУБД или прикладных программ;

•СРД в средствах реализации сетевых взаимодействий или на уровне приложений;

•использование криптографических преобразований или методов непосредственного контроля доступа;

•программная и (или) техническая реализация СРД.

В целом разработка Руководящих документов Гостехкомиссии России явилась следствием бурно развивающегося процесса внедрения новых информационных технологий. Документы достаточно оперативно заполнили правовой вакуум в области стандартов информационной безопасности в стране и на определенном этапе позволили решать актуальную задачу обеспечения безопасности информации. Поскольку разработка документов такого рода для России представляет достаточно новую область деятельности, можно рассматривать их как первую стадию формирования отечественных стандартов в области информационной безопасности.

На разработку этих документов большое влияние оказала “Оранжевая книга” Министерства обороны США [76], которое выразилось в ориентации на системы военного и специального применения, в использовании единой универсальной шкалы степени защищенности и в игнорировании вопросов ценности и времени жизни информации.

К недостаткам документов, помимо отсутствия требований к защите от угроз работоспособности, относится ориентация только на противодействие НСД и отсутствие требований к адекватности реализации политики безопасности. Собственно “политика безопасности” трактуется в этих документах исключительно как поддержание режима секретности и отсутствие НСД. Из-за этого средства защиты ориентируются на противодействие только внешним угрозам, а к структуре самой системы и ее функционированию не предъявляется никаких требований.

С точки зрения разработчиков данных руководящих документов основная и едва ли не единственная задача средств обеспечения безопасности - это обеспечение защиты от несанкционированного доступа к информации. Если средствам контроля и обеспечения целостности информации в них еще уделяется некоторое внимание, то поддержка работоспособности систем обработки информации (как мера защиты от угроз работоспособности) вообще не упоминается. Определенный уклон в сторону поддержания секретности объясняется тем, что эти документы были разработаны в расчете на применение в существующих информационных системах Министерства обороны и спецслужб России, а также недостаточно высоким уровнем технологий этих систем.

4.4.2. Документы Гостехкомиссии России о модели нарушителя в автоматизированной системе

Модель нарушителя определяется в 4-м разделе основного Руководящего документа Гостехкомиссии России “Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации” [52].

В качестве **нарушителя** в этом документе рассматривается субъект, имеющий доступ к работе с штатными средствами АС и СВТ как части АС.

Нарушители классифицируются по уровню возможностей, предоставляемых им штатными средствами АС и СВТ.

Выделяется четыре уровня этих возможностей.

Классификация является иерархической, т.е. каждый следующий уровень включает в себя функциональные возможности предыдущего.

Первый уровень определяет самый низкий уровень возможностей ведения диалога в АС - запуск задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации.

Второй уровень определяется возможностью создания и запуска собственных программ с новыми функциями по обработке информации.

Третий уровень определяется возможностью управления функционированием АС, т.е. воздействием на базовое программное обеспечение системы и на состав и конфигурацию ее оборудования.

Четвертый уровень определяется всем объемом возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств АС, вплоть до включения в состав СВТ собственных технических средств с новыми функциями по обработке информации.

Подчеркивается , что в своем уровне нарушитель является специалистом высшей квалификации, знает все о АС и, в частности, о системе и средствах ее защиты.

4.4.3. Классификация защищенности средств вычислительной техники. Классификация защищенности автоматизированных систем

Руководящие документы Гостехкомиссии России **“ Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации”** [53] и **“ Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации”** [51] определяют основные показатели защищенности по классам средств вычислительной техники (Таблица 1) и требования к классам защищенности автоматизированных систем (Таблица 2).

Таблица 4.1.

Распределение показателей защищенности по классам средств вычислительной техники

Наименование показателя	Класс защищенности					
	6	5	4	3	2	1
Дискреционный принцип контроля доступа	+	+	+	=	+	=
Мандатный принцип контроля доступа	-	-	+	=	=	=
Очистка памяти	-	+	+	+	=	=
Изоляция модулей	-	-	+	=	+	=

Наименование показателя	Класс защищенности					
	6	5	4	3	2	1
Маркировка документов	-	-	+	=	=	=
Защита ввода и вывода на отчужденный носитель информации	-	-	+	=	=	=
Сопоставление пользователя с устройством	-	-	+	=	=	=
Идентификация и аутентификация	+	=	+	=	=	=
Гарантии проектирования	-	+	+	+	+	+
Регистрация	-	+	+	+	=	=
Взаимодействие пользователя с КСЗ	-	-	-	+	=	=
Надежное восстановление	-	-	-	+	=	=
Целостность КСЗ	-	+	+	+	=	=
Контроль модификации	-	-	-	-	+	=
Контроль дистрибуции	-	-	-	-	+	=
Гарантии архитектуры	-	-	-	-	-	+
Тестирование	+	+	+	+	+	=
Руководство пользователя	+	=	=	=	=	=
Руководство по КСЗ	+	+	=	+	+	=
Тестовая документация	+	+	+	+	+	=
Конструкторская (проектная) документация	+	+	+	+	+	+

Обозначения:

“ - ” - нет требований к данному классу

“ + ” - новые или дополнительные требования

“ = ” - требования совпадают с требованиями к СВТ предыдущего класса

Седьмой класс присваивается средствам вычислительной техники, к которым предъявлялись требования по защите от несанкционированного доступа к информации, но при оценке защищенность средства оказалась ниже уровня требований шестого класса.

Таблица 4.2.

Требования к классам защищенности автоматизированных систем

Подсистемы и требования	Классы								
	3Б	**3А**	**2Б**	**2А**	**1Д**	**1Г**	**1В**	**1Б**	**1А**
I. Подсистема управления доступом									
А. Идентификация, проверка подлинности и контроль доступа субъектов:									
• в систему	+	+	+	+	+	+	+	+	+
• к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ				+		+	+	+	+
• к программам				+		+	+	+	+
• к томам, каталогам, файлам, записям, полям записей				+		+	+	+	+
В. Управление потоками информации				+			+	+	+
II. Подсистема регистрации и учета									
А. Регистрация и учет									
• входа/выхода субъектов доступа в/из системы (узла сети)	+	+	+	+	+	+	+	+	+
• выдачи печатных (графических) выходных документов		+		+		+	+	+	+
• запуска/завершения программ и 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				+			+	+	+
В. Учет носителей информации	+	+	+	+	+	+	+	+	+
С. Очистка (обнуление, обезличива-		+		+		+	+	+	+

Подсистемы и требования		Классы								
	ние) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
D.	Сигнализация попыток нарушения защиты							+	+	+
III. Криптографическая подсистема										
A.	Шифрование конфиденциальной информации				+				+	+
B.	Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах									+
C.	Использование аттестованных (сертифицированных) криптографических средств				+				+	+
IV. Подсистема обеспечения целостности										
A.	Обеспечение целостности программных средств и обрабатываемой информации	+	+	+	+	+	+	+	+	+
B.	Физическая охрана средств вычислительной техники и носителей информации	+	+	+	+	+	+	+	+	+
C.	Наличие администратора (службы) защиты информации в АС				+			+	+	+
D.	Периодическое тестирование СЗИ НСД	+	+	+	+	+	+	+	+	+
E.	Наличие средств восстановления СЗИ НСД	+	+	+	+	+	+	+	+	+
F.	Использование сертифицированных средств защиты		+		+			+	+	+

Обозначения:

“ + ” - требование к данному классу присутствует.

4.4.4. Показатели защищенности межсетевых экранов

В руководящем документе Гостехкомиссии России [55]: **“Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации”** устанавливается классификация межсетевых экранов (МЭ) по

уровня защищенности от несанкционированного доступа (НСД) к информации на базе перечня показателей защищенности и совокупности описывающих их требований.

Под сетями ЭВМ, распределенными автоматизированными системами (АС) в данном документе понимаются соединенные каналами связи системы обработки данных, ориентированные на конкретного пользователя.

МЭ представляет собой локальное (однокомпонентное) или функционально - распределенное средство (комплекс), реализующее контроль за информацией, поступающей в АС и/или выходящей из АС, и обеспечивает защиту АС посредством фильтрации информации, т.е. ее анализа по совокупности критериев и принятия решения о ее распространении в (из) АС.

Руководящий документ разработан в дополнение к Руководящим документам Гостехкомиссии России “Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации” и “Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации”.

Документ предназначен для заказчиков и разработчиков МЭ, а также сетей ЭВМ, распределенных автоматизированных систем с целью использования при формулировании и реализации требований по их защите от НСД к информации.

4.4.4.1. Общие положения

1. Данные показатели содержат требования к средствам защиты, обеспечивающим безопасное взаимодействие сетей ЭВМ, АС посредством управления межсетевыми потоками информации и реализованных в виде МЭ.
2. Показатели защищенности применяются к МЭ для определения уровня защищенности, который они обеспечивают при межсетевом взаимодействии.
   Конкретные перечни показателей определяют классы защищенности МЭ.

Деление МЭ на соответствующие классы по уровням контроля межсетевых информационных потоков с точки зрения защиты информации необходимо в целях разработки и применения обоснованных и экономически оправданных мер по достижению требуемого уровня защиты информации при взаимодействии ЭВМ, АС.

Дифференциация подхода к выбору функций защиты в МЭ определяется АС, для защиты которой применяется данный экран.

Устанавливается пять классов защищенности МЭ.

Каждый класс характеризуется определенной минимальной совокупностью требований по защите информации.

Самый низкий класс защищенности - пятый, применяемый для безопасного взаимодействия АС класса 1Д с внешней средой, четвертый - для 1Г, третий - 1В, второй - 1Б, самый высокий - первый, применяемый для безопасного взаимодействия АС класса 1А с внешней средой

Требования, предъявляемые к МЭ, не исключают требований, не исключают требований, предъявляемых к средствам вычислительной техники (СВТ) и АС в соответствии с

руководящими документами Гостехкомиссии России “Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации” и “Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации”

При включении МЭ в АС определенного класса защищенности, класс защищенности совокупной АС, полученной из исходной путем добавления в нее МЭ, не должен понижаться.

Для АС класса 3Б, 2Б должны применяться МЭ не ниже 5 класса.

Для АС класса 3А, 2А в зависимости от важности обрабатываемой информации должны применяться МЭ следующих классов:

- при обработке информации с грифом “секретно” - не ниже 3 класса;
- при обработке информации с грифом “совершенно секретно” - не ниже 2 класса;
- при обработке информации с грифом “особой важности” - не ниже 1 класса.

Таким образом, фактически, обмен информацией, составляющей государственную тайну, между автоматизированными системами классов 1Д - 1А или при наличии такой системы только на одном конце, данным документом не предусмотрен.

4.4.4.2. Перечень показателей по классам защищенности межсетевых экранов

Таблица 4.3

Показатели защищенности	**Классы защищенности**				
	5	**4**	**3**	**2**	**1**
Управление доступом (фильтрация данных и трансляция адресов	+	+	+	+	=
Идентификация и аутентификация	-	-	+	=	+
Регистрация	-	+	+	+	=
Администрирование: идентификация и аутентификация	+	=	+	+	+
Администрирование: регистрация	+	+	+	=	=
Администрирование: простота использования	-	-	+	=	+
Целостность	+	=	+	+	+
Восстановление	+	=	=	+	=
Тестирование	+	+	+	+	+
Руководство администратора защиты	+	=	=	=	=
Тестовая документация	+	+	+	+	+
Конструкторская (проектная) документация	+	=	+	=	+

Обозначения:

“-” - нет требований к данному классу;

“+” - новые или дополнительные требования;

“=” - требования совпадают с требованиями к МЭ предыдущего класса

5. ГОСУДАРСТВЕННАЯ СИСТЕМА ЛИЦЕНЗИРОВАНИЯ И СЕРТИФИКАЦИИ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

5.1. Основные руководящие документы, определяющие порядок лицензирования и сертификации в области защиты информации

Не проходящий и не снижающийся интерес к проблеме лицензирования и сертификации в области защиты информации, несмотря на относительно большой объем публикаций по данному вопросу, объясняется тем, что происходящие в стране процессы существенно затронули организацию системы защиты информации во всех ее сферах - разработки, производства, реализации, эксплуатации средств защиты, подготовки соответствующих кадров. Прежние традиционные подходы в современных условиях уже не в состоянии обеспечить требуемый уровень безопасности государственно значимой и частной конфиденциальной информации, циркулирующей в информационно-телекоммуникационных системах страны [20].

Существенным фактором, до настоящего времени оказывающим значительное влияние на положение дел в области защиты информации, является то, что до начала 90-х годов нормативное регулирование в данной области оставляло желать лучшего. Цели защиты информации в нашей стране достигались главным образом за счет реализации принципа “максимальной секретности ”, в соответствии с которым доступ ко многим видам информации был просто ограничен. Никаких законодательных и других нормативных актов, определяющих защиту информационных прав негосударственных организаций и отдельных граждан, не существовало. Средства криптографической защиты информации использовались только в интересах государственных органов, а их разработка была прерогативой исключительно специальных служб и немногих специализированных государственных предприятий. Указанные предприятия строго отбирались и категорировались по уровню доступа к разработке и производству этих средств. Сами изделия тщательно проверялись компетентными государственными органами и допускались к эксплуатации исключительно на основании специальных заключений этих органов. Любые работы в области криптографической защиты информации проводились на основании утвержденных Правительством страны специальных секретных нормативных актов, полностью регламентировавших порядок заказа , разработки, производства и эксплуатации шифровальных средств. сведения об этих средствах, их разработке, производстве, и использовании как в стране, так и за рубежом, были строго засекречены, а их распространение предельно ограничено. Даже простое упоминание о криптографических средствах в открытых публикациях было запрещено [25].

В настоящее время можно отметить, что правовое поле в области защиты информации получило достаточно весомое заполнение. Конечно, нельзя сказать, что процесс построения цивилизованных правовых отношений успешно завершен, и задача правового обеспечения деятельности в этой области уже решена. Важно другое - на наш взгляд, можно констатировать, что имеется неплохая законодательная база, вполне позволяющая, с одной стороны, предприятиям осуществлять свою деятельность по защите информации в соответствии с требованиями действующих нормативных актов, а с другой - уполномоченным государственным органам на законной основе регулировать рынок соответствующих товаров и

услуг, обеспечивая необходимый баланс интересов отдельных граждан, общества в целом и государства.

Нормы и требования российского законодательства в области лицензирования и сертификации включают в себя положения ряда нормативных актов Российской Федерации различного уровня. Первым по времени открытым правовым нормативным актом, регулирующим вопросы оборота средств криптографической защиты информации , является принятое 28 мая 1991 года постановление Верховного Совета СССР № 2195-1 **“О видах деятельности, которыми предприятия вправе заниматься только на основании специальных разрешений (лицензий)”**. Этим документом был утвержден перечень отдельных видов деятельности, которыми предприятия на территории страны вправе заниматься только при наличии у них специального разрешения или лицензии. В частности, к таким видам деятельности данное постановление относит и производство, ремонт, реализацию и эксплуатацию шифровальной техники.

Указом Президента РФ от 5 января 1992 года № 9 для выполнения работ по руководству разработкой, производством, реализацией, внедрением и эксплуатацией в государственных организациях технических и программных средств защиты информации была образована **Государственная техническая комиссия при Президенте Российской Федерации** (Гостехкомиссия России).

В свою очередь, Указом Президента РФ от 24 декабря 1991 года № 313 и Постановлением Верховного Совета Российской Федерации от 19 февраля 1993 года № 4524-1 был принят Закон РФ **“О федеральных органах правительственной связи и информации”** в соответствии с которым образовано Федеральное агентство правительственной связи и информации при Президенте Российской Федерации (ФАПСИ).

Статья 11 данного закона предоставила Федеральному агентству права по определению порядка разработки, производства, реализации, эксплуатации шифровальных средств, предоставления услуг в области шифрования информации, а также порядка проведения работ по выявлению электронных устройств перехвата информации в технических средствах и помещениях государственных структур. Одновременно Федеральному агентству этой статьей дано право осуществлять лицензирование указанных видов деятельности и сертификацию соответствующих товаров и услуг. Пунктом м) той же статьи 11 данного закона Федеральному агентству предоставлено право осуществлять лицензирование и сертификацию телекоммуникационных систем и комплексов высших органов государственной власти Российской Федерации и закрытых (защищенных) с помощью шифровальных средств систем и комплексов телекоммуникаций органов государственной власти субъектов Российской Федерации, федеральных органов исполнительной власти, а также организаций, предприятий, банков и иных учреждений, расположенных на территории России, независимо от их ведомственной принадлежности и форм собственности.

Полномочия государственных органов по лицензированию деятельности в области защиты информации, содержащей сведения, составляющие государственную тайну, а также по сертификации средств защиты такой информации определены Законом РФ от 21 июля 1993 года № 5485-1 **“О государственной тайне”** с изменениями и дополнениями, внесенными Федеральным законом от 6 октября 1997 года № 131-ФЗ **“О внесении изменений и дополнений в Закон Российской Федерации “О государственной тайне”.**

Статья 27 этого закона предписывает осуществлять допуск предприятий, учреждений и организаций к работам по созданию средств защиты секретной информации и оказанию услуг по защите сведений, составляющих государственную тайну, путем получения ими лицензий на данную деятельность. Статья 28 устанавливает обязательность сертификации технических средств, предназначенных для защиты секретных сведений, и определяет государственные органы, ответственные за проведение сертификации указанных средств (Гостехкомиссия России, ФАПСИ, Министерство обороны, и Министерство безопасности РФ, правопреемником которого является Федеральная служба безопасности России).

Во исполнении этого закона а августе 1993 года Правительством Российской Федерации принято специальной постановление, которое полностью определяет порядок создания и использования криптографических (шифровальных) средств, предназначенных для защиты информации, содержащей сведения , составляющие государственную тайну, начиная от стадии подготовки технического задания на проведение научно-исследовательских работ до серийного производства и установки шифровальной техники в сложные закрытые (защищенные) системы и комплексы обработки, хранения и передачи информации.

В начале 1994 года Президентом РФ и Правительством РФ был принят пакет нормативных актов, определивших порядок импорта и экспорта шифровальных средств и нормативно-технической документации к ним на территории Российской Федерации. В первую очередь, это распоряжение Президента России от 11 февраля 1994 года № 74-П **“О контроле за экспортом из Российской Федерации отдельных видов сырья, материалов, оборудования, технологий и научно-технической информации, которые могут быть применены при создании вооружения и военной техники”**. Данным распоряжением утвержден соответствующий перечень, в котором, в частности, указывается, что аппаратура, узлы, компоненты, программное обеспечение и технология производства, специально разработанные или модифицированные для использования в криптографии или выполнения криптографических функций, подлежат экспортному контролю. Кроме того, порядок импорта и экспорта шифровальных средств регулируется постановлением правительства от 15.04.94 № 331 **“О внесении дополнений и изменений в постановление Правительства Российской Федерации от 06.11.92 № 854 “О лицензировании и квотировании экспорта и импорта товаров (работ, услуг) на территории Российской Федерации”** и от 10.12.92 № 959 **“О поставках продукции и отходов производства, свободная реализация которых запрещена”**, а также постановлением от 01.07.94 № 758 **“О мерах по совершенствованию государственного регулирования экспорта товаров и услуг”**. Затем 31 октября 1996 г. этот перечень был дополнен постановлением Правительства № 1299, которым утверждено **“Положение о порядке лицензирования экспорта и импорта товаров (работ, услуг) в Российской Федерации”**.

Перечисленные документы установили, в частности, что ввоз и вывоз средств криптографической защиты информации (шифровальной техники) и нормативно-технической документации к ней может осуществляться исключительно на основании лицензии Министерства внешних экономических связей Российской Федерации, выдаваемой на основании решения ФАПСИ о выдаче лицензий. Кроме того, данные документы определили общий порядок выдачи экспортных лицензий на шифровальные средства. направленный на предотвращение утечки секретных сведений и технологий при вывозе из страны средств защиты информации.

Предоставленные Гостехкомиссии России и ФАПСИ права по определению порядка осуществления и лицензирования деятельности в области защиты информации нашли свое отражение в **“Положение о государственном лицензировании деятельности в области защиты информации”**, которое утверждено 27 апреля 1994 года совместным решением № 10 Гостехкомиссии России и ФАПСИ, разграничившим сферы компетенции этих двух ведомств и определившим механизм практического лицензирования, действующего в настоящее время.

Обязательное государственное лицензирование деятельности в области защиты информации криптографическими методами, а также в области выявления электронных устройств перехвата информации в технических средствах и помещениях государственных структур введено постановление правительства от 24.12.94 № 1418 **“О лицензировании отдельных видов деятельности”**. Данное постановление распространяет механизм обязательного лицензирования на все виды деятельности в области криптографической защиты информации, независимо от ее характера и степени секретности, на все субъекты этой деятельности любых организационно-правовых форм, включая и физических лиц.

Как уже отмечалось, важным шагом в деле правового обеспечения деятельности в области защиты информации явилось принятие Федерального закона от 20.02.95 № 24-ФЗ **“Об информации, информатизации и защите информации”**. Данный закон впервые официально вводит понятие “конфиденциальной информации”, которая рассматривается как документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации, и устанавливает общие правовые требования к организации защиты такой информации в процессе ее обработки, хранения и циркуляции в технических устройствах и информационных и телекоммуникационных системах и комплексах и организации контроля за осуществлением мероприятий по защите конфиденциальной информации. При этом следует подчеркнуть, что Закон не разделяет государственную и частную информацию как объект защиты в том случае, если доступ к ней ограничивается.

Кроме того, закон определяет на государственно-правовом уровне электронную цифровую подпись как средство защиты информации от несанкционированного искажения или подмены (имитозащиты) и подтверждения подлинности отправителя и получателя информации (аутентификации сторон). В соответствии со статьей 5 “юридическая сила документа, хранимого, обрабатываемого и передаваемого с помощью автоматизированных информационных и телекоммуникационных систем, может подтверждаться электронной цифровой подписью”. При этом “юридическая сила электронной цифровой подписи признается при наличии в автоматизированной системе программно-технических средств, обеспечивающих идентификацию подписи, и соблюдении установленного режима их использования”. Далее закон раскрывает требования, предъявляемые к специализированным программно-техническим средствам, реализующим электронною цифровую подпись, и порядку их использования в информационно-телекоммуникационных системах.

Подписанный 3 апреля 1995 года Указ Президента Российской Федерации № 334 **“О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации”** запрещает любую деятельность, связанную с разработкой, производством, реализацией и эксплуатацией шифровальных средств, предоставлением услуг в области шифрования информации, без лицензии ФАПСИ. Пункты 2,3 данного до-

кумента устанавливают обязательное использование исключительно сертифицированных средств защиты информации во всех государственных структурах, в том числе и в государственных банках Российской Федерации, на предприятиях, работающих по государственному заказу, а также на предприятиях и в организация при их информационном взаимодействии с центральным банком России и его структурными подразделениями. Таким образом, обязательность сертификации распространяется не только на средства защиты информации, содержащей сведения, составляющие государственную тайну, но и на средства защиты любой государственно значимой информации независимо от грифа ее секретности. Кроме того, Указ формирует механизм реализации перечисленных выше законодательных актов, возлагая ответственность за их выполнение на ФАПСИ, а также правоохранительные, таможенные и налоговые органы страны.

5.2. Виды деятельности, подлежащие лицензированию

В течении первой половины 1995 года Правительством Российской Федерации во исполнение закона **“О государственной тайне”** приняты Постановление от 15 апреля 1995 года № 333 **“О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны”** и постановление от 26.06.95 № 608 **“О сертификации средств защиты информации”**.

Указанные постановления формируют механизм получения предприятиями и организациями, независимо от их организационно правовой формы, лицензии на право осуществления любой деятельности, связанной с информацией, составляющей государственную тайну, а также общий порядок сертификации средств, предназначенных для защиты секретной информации.

Постановление Правительства РФ № 333 от 15 апреля 1995 года **“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”** (с дополнениями, внесенными Постановлением Правительства РФ № 509 от 23 апреля 1996 года и Постановлением Правительства РФ № 513 от 30 апреля 1997 года) вводит соответствующее Положение, устанавливающее порядок лицензирования деятельности предприятий, учреждений и организаций независимо от организационно-правовых форм 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.

Лицензирование деятельности в области защиты информации на территории Российской Федерации осуществляется специальными органами Федеральной службы безопасности Российской Федерации, Государственной технической комиссии при Президенте РФ и Федерального агентства правительственной связи и информации при Президенте РФ, а также Службой внешней разведки РФ (СВР) - за рубежом.

Федеральная служба безопасности Российской Федерации осуществляет:

1. Предоставление лицензии на допуск к проведению работ, связанных с использованием сведений, составляющих государственную тайну (за исключением предприятий ФСБ, ФАПСИ, Минобороны, ФПС, СВР, Гостехкомиссии, допуск которых осуществляется соответствующими руководителями министерств и ведомств).
2. Оформление допуска руководителю предприятия (до подачи заявления на выдачу лицензии).

Кроме того, ФСБ России осуществляет на основании Указа Президента РФ от 9 января 1996 года № 21 лицензирование деятельности по производству, реализации, приобретению в целях продажи, ввозу в Российскую Федерацию и вывозу за ее пределы, а также использование специальных технических средств, предназначенных для негласного получения информации, которые могут применяться только соответствующими органами при проведении оперативно-розыскных мероприятий в соответствии с Федеральным законом от 12 августа 1995 года № 144-ФЗ **“Об оперативно-розыскной деятельности”**.

Распределение функций между Гостехкомиссией и ФАПСИ определено в упомянутом выше **“Положении о государственном лицензировании деятельности в области защиты информации”**, которое утверждено совместным решением Гостехкомиссии России и ФАПСИ от 27 апреля 1994 года № 10.

Государственная техническая комиссия при Президенте Российской Федерации осуществляет:

Предоставление лицензии на право проведения следующих видов работ, связанных с разработкой, созданием и эксплуатацией средств защиты информации:

- сертификация, сертификационные испытания защищенных технических средств обработки информации (ТСОИ), технических средств защиты информации, технических средств контроля эффективности мер защиты информации, защищенных программных средств обработки информации, программных средств по требованиям безопасности, программных средств защиты информации, программных средств контроля защищенности информации;
- аттестование систем информатизации, автоматизированных систем управления, систем связи и передачи данных, технических средств приема, передачи и обработки подлежащей защите информации, технических средств и систем, не обрабатывающих эту информацию, но размещенных в помещениях, где она обрабатывается (циркулирует) , а также помещений, предназначенных для ведения переговоров, содержащих охраняемые сведения, на соответствие требованиям руководящих и нормативных документов по безопасности информации и контроль защищенности информации в этих системах, технических средствах и помещениях;
- разработка, производство, реализация, монтаж, наладка, установка, ремонт, сервисное обслуживание защищенных ТСОИ, технических средств защиты информации, технических средств контроля эффективности мер защиты информации, защищенных программных средств обработки информации, программных средств защиты информации, программных средств контроля защищенности информации;
- проведение специсследований на побочные электромагнитные излучения и наводки (ПЭМИН) ТСОИ;
- проектирование объектов в защищенном исполнении;
- подготовка и переподготовка кадров в области защиты информации по видам деятельности, перечисленным в данном перечне.

Федеральное агентство правительственной связи и информации при Президенте Российской Федерации осуществляет:

Предоставление лицензии на право проведения следующих видов работ, связанных с разработкой, созданием и эксплуатацией криптографических (шифровальных) средств защиты информации:

- разработка, производство, проведение сертификационных испытаний, реализация, монтаж, наладка, установка и ремонт шифровальных средств, предназначенных для криптографической защиты информации при ее обработке, хранении и передаче по каналам связи, а также предоставление услуг по шифрованию информации;
- эксплуатация негосударственными предприятиями шифровальных средств, предназначенных для криптографической защиты информации, не содержащей сведений, составляющих государственную тайну;
- разработка, производство, проведение сертификационных испытаний, реализация, монтаж, наладка, установка и ремонт систем и комплексов телекоммуникаций высших органов государственной власти Российской Федерации, а также закрытых (с помощью шифровальных средств) систем и комплексов телекоммуникаций органов государственной власти субъектов Российской Федерации, центральных органов федеральной исполнительной власти, организаций, предприятий, банков и иных учреждений, расположенных на территории Российской Федерации, независимо от их ведомственной принадлежности и форм собственности;
- разработка, производство, проведение сертификационных испытаний, реализация, монтаж, наладка, установка, ремонт, сервисное обслуживание специализированных защищенных ТСОИ, технических средств защиты информации, технических средств контроля эффективности мер защиты информации, защищенных программных средств обработки информации, программных средств защиты информации, программных средств контроля защищенности информации, предназначенных для использования в высших органах государственной власти Российской Федерации;
- проведение работ по выявлению электронных устройств перехвата информации в помещениях государственных структур на территории Российской Федерации;
- проведение работ по выявлению электронных устройств перехвата информации в технических средствах государственных структур на территории Российской Федерации;
- проведение специсследований на побочные электромагнитные излучения и наводки (ПЭМИН) специализированных защищенных ТСОИ, предназначенных для использования в высших органах государственной власти Российской Федерации;
- проектирование в защищенном исполнении объектов высших органов государственной власти Российской Федерации;
- подготовка и переподготовка кадров в области защиты информации по видам деятельности, перечисленным в данном перечне.

При принятии решения о необходимости лицензирования работ в области защиты информации необходимо учитывать следующие обстоятельства:

- лицензии только Гостехкомиссии и ФАПСИ не предоставляют права проведения работ, связанных с использованием сведений, составляющих государственную тайну;
- лицензия ФСБ не предоставляет права проведения работ, находящихся в компетенции Гостехкомиссии и ФАПСИ.

Постановлением от 15.04.95 № 333 устанавливает, что лицензия на право деятельности по проведению работ, связанных с использованием сведений, составляющих государственную тайну, с созданием средств защиты информации и оказанием услуг по защите государственной тайны, может быть выдана предприятию или организации, независимо от формы его собственности, исключительно на основании результатов специальной экспертизы заявителя, в ходе которой будет установлено наличие на данном предприятии необходимых условий для сохранения доверенных ему секретных сведений, и государственной аттестации их руководителей, ответственных за защиту сведений, составляющих государственную тайну.

Постановление от 26 июня 1995 года № 608 устанавливает общие принципы организации систем сертификации средств защиты информации, содержащей сведения, составляющие государственную тайну, всеми ведомствами Российской Федерации, наделенными законом правом проводить подобную сертификацию. Статьи Положения определяют:

- участников системы сертификации средств защиты информации;
- права и обязанности участников;
- схемы проведения сертификационных испытаний;
- порядок выдачи, приостановления и аннулирования сертификатов;
- порядок оплаты услуг по сертификации;
- порядок контроля за качеством сертифицированных изделий;
- ответственность сторон за выполнение ими своих обязательств в системе сертификации.

Кроме того, данным положением к средствам защиты информации отнесены и средства контроля эффективности защиты информации.

Федеральный закон от 5 июня 1996 года № 85-ФЗ **“Об участии в международном информационном обмене”** определяет необходимость сертификации средств международного информационного обмена и необходимость лицензирования деятельности в области международного информационного обмена при работе с конфиденциальной информацией. Закон предоставляет уполномоченным государственным органам (ФСБ, Гостехкомиссии и ФАПСИ) право:

- участвовать в определении перечней документированной информации, вывоз которой из Российской Федерации, и иностранных информационных продуктов, ввоз которых в Российскую Федерацию, ограничен;
- определять порядок лицензирования деятельности в области международного информационного обмена при работе с конфиденциальной информацией;
- определить порядок сертификации средств и аттестации систем международного информационного обмена.

5.3. Основные принципы и правила системы лицензирования

5.3.1. Общие принципы и правила лицензирования

Лицензирование - это процесс, осуществляемый в отношении таких категорий, как “деятельность” (направления, виды деятельности) “субъект” (физическое лицо, предприятие, организация или иное юридическое лицо), когда некоторый субъект в результате проведения комплекса мероприятий, состав, правила и порядок которых предписываются зако-

нодательными и нормативными актами, получает право на осуществление определенного вида деятельности.

Рассматриваемые правила и принципы, положенные в основу деятельности государственных органов по лицензированию в области защиты информации и построения соответствующей системы, вытекают из приведенных выше нормативных актов и основаны на предоставленных им законодательством правах и полномочиях.

Лицензирование в области защиты информации является обязательным.

Данное правило устанавливает, что для занятия деятельностью в области защиты информации одного желания мало и необходимо получение права на ее осуществление. Причем распространяется это требование на все без исключения направления и отдельные виды деятельности. Поскольку не существует определений понятий “направление” и “отдельный вид деятельности”, они вводятся в виде перечисления в соответствующих нормативных актах.

Деятельность в области защиты информации физических и юридических лиц, не прошедших лицензирование, запрещена.

Из данного правила вытекает, что субъекты, не получившие права на осуществление права в области защиты информации и продолжающие ее осуществлять, нарушая установленный порядок, занимаются тем самым противоправной деятельностью. В отношении таких субъектов могут быть применены санкции, предусмотренные действующим Гражданским кодексом и законодательством об административной и уголовной ответственности.

Лицензии ФСБ, Гостехкомиссии и ФАПСИ и их решения о выдаче лицензии на право осуществления деятельности в области защиты информации, лицензирование которой относится к компетенции соответствующей организации, выдаются, в основном, юридическим лицам - предприятиям, организациям и учреждениям, независимо от их организационно-правовой формы (далее - предприятия).

Данное правило, однако, лишь на первый взгляд ущемляет интересы физических лиц, которым не предоставляются права на промышленную, коммерческую деятельность, связанную со средствами защиты информации, в первую очередь - с шифровальными средствами. Включение данного постулата обусловлено рядом факторов. Во-первых, разработка (производство, монтаж, наладка и т.д.) средств защиты информации и шифровальных средств требует участия высококлассных специалистов разного профиля. Во-вторых, требованиям, предъявляемым, например, ФАПСИ к заявителю, физическое лицо удовлетворить просто не в состоянии. В-третьих, для проведения работ в этой области, как правило, необходимо обеспечение выполнения режимных требований и (для ознакомления, например, с нормами требований по безопасности) наличия допуска к сведениям, составляющим государственную тайну.

Лицензии выдаются конкретным юридическим лицам - предприятиям, а не министерствам, ведомствам или ассоциациям в целом. Если разрешаемая в лицензии деятельность не является для лицензиата основной, то в лицензии указывается структурное подразделение, которому предоставляется право осуществления данного вида деятельности.

Лицензии и решения о выдаче лицензии выдаются только предприятиям, зарегистрированным на территории Российской Федерации.

Лицензия выдается только на основании результатов специальной экспертизы заявителя на соответствие требованиям к предприятию на право деятельности в области защиты информации по заявленному направлению работ и аттестации руководителя предприятия или лиц, уполномоченных им для руководства лицензируемой деятельностью.

Данное положение устанавливает одну из основных норм, определяющих сущностные и процедурные аспекты системы лицензирования: лицензия может быть выдана не каждому заявителю, то есть предприятию, подавшему все необходимые и правильно оформленные документы, а только предприятию, обладающему соответствующими возможностями, достаточными для осуществления заявленных видов деятельности. Проверка возможностей предприятия и осуществляется в ходе специальной экспертизы путем экспертных оценок специалистами специально создаваемых комиссий, с учетом профиля заявляемых видов деятельности, факта удовлетворения требованиям предъявляемым к предприятиям. С данными требованиями заявитель может быть ознакомлен в соответствующем лицензионном центре Гостехкомиссии или ФАПСИ. Кроме того, по результатам специальной экспертизы заявителя определяются состав и конкретная формулировка решенных видов деятельности, а также условия их осуществления. Уточнение формулировок для различных видов деятельности и заявителей может быть проведено с учетом следующих факторов:

- уровня конфиденциальности защищаемой информации;
- уровня секретности сведений, используемых при осуществлении заявляемой деятельности;
- типа используемого криптографического алгоритма;
- способа технической реализации изделия;
- уровня квалификации персонала;
- назначения изделия, наличия или отсутствия сертификата на него;
- страны-производителя изделия;
- категории помещений и технических средств.

Решение о выдаче лицензии дается предприятию, подавшему заявление на его получение, на основании результатов технической экспертизы изделия и (или) специальной экспертизы заявителя.

Основными задачами технической экспертизы являются установление соответствия предъявляемого изделия заявляемым характеристикам (классу, типу средств) и проверка возможного использования в коммерческих средствах защиты информации, в первую очередь - в шифрсредствах, технических средств, алгоритмов, программ и способов их реализации, составляющих государственную тайну.

Лицензия действует на всей территории Российской Федерации, если иное не оговорено в ней особо.

Могут, например, налагаться следующие ограничения:

- для региональных представителей, работающих по договорам на реализацию шифрсредств, - рамках сферы их деятельности;
- для фирм-разработчиков - разработка криптографических средств защиты и защищенных средств и систем в интересах региональных государственных и коммерческих структур.

Лицензии и решения о выдаче лицензии подписываются Председателем Гостехкомиссии или Генеральным директором ФАПСИ или лицом, их замещающим, и заверяется гербовой печатью.

Передача лицензии другим юридическим лицам запрещена.

Лицензия имеет ограниченный срок действия, по истечении которого осуществляется переоформление лицензии в порядке, предусмотренном для ее выдачи.

Данные нормы определены Постановлением Правительства Российской федерации от 24 декабря 1994 года № 1418 для всех систем лицензирования.

Лицензирование осуществляется на платной основе.

Размер платы за рассмотрение заявления и за выдачу лицензий фиксирован. Размер платы за специальную экспертизу определяется договором на ее проведение.

Для получения лицензий или решения о выдаче лицензии предприятие обязано представить определенный перечень документов, состав которых определяется нормативными актами Правительства Российской Федерации и ФАПСИ.

Представляемые заявителем документы регистрируются в уполномоченном подразделении Федерального агентства по мере их поступления. Заявление регистрируется только при наличии всех требуемых для оформления лицензии документов.

Рассмотрение заявления и специальная экспертиза должны проводиться в сроки, ограниченные соответствующими нормативными актами.

На настоящий момент продолжительность рассмотрения заявления установлена сроком 30 суток с момента поступления всех необходимых документов (с возможностью увеличения этого срока в отдельных случаях еще максимум на 60 суток). Специальная экспертиза имеет аналогичную продолжительность с момента заключения договора на ее проведение.

Отказ заявителю в выдаче лицензии должен быть мотивирован.

Заявителю может быть отказано в получении лицензии в следующих случаях:
- при наличии в документах, представленных заявителем, недостоверной или искаженной информации;
- отрицательного заключения по результатам специальных экспертиз, установивших несоответствие условиям, необходимым для осуществления заявленного вида деятельности и условиям безопасности;
- отрицательного заключения по результатам аттестации руководителей предприятия или лица, уполномоченного им на ведение лицензируемой деятельности;
- отрицательного заключения по результатам технических экспертиз.

При ликвидации предприятия выданная лицензия теряет юридическую силу.

В случае реорганизации предприятия, изменения его дислокации или наименования юридического лица, утраты лицензии осуществляется ее переоформление.

Переоформление лицензии в указанных случаях, за исключением изменения наименования юридического лица, осуществляется в по рядке, предусмотренном для ее выдачи.

Выданная лицензия может быть приостановлена или аннулирована.

Приостановление или аннулирование лицензии осуществляется в случаях:
- представления лицензиатом соответствующего заявления;
- обнаружения недостоверных данных в документах, представленных для получения лицензии;
- нарушения лицензиатом условий действия лицензии;

- невыполнения лицензиатом предписаний или распоряжений государственных органов или приостановлении ими деятельности предприятия в соответствии с законодательством Российской федерации;
- ликвидации предприятия.

Приостановление действия лицензии влечет за собой прекращение деятельности лицензиата по виду деятельности (работ, услуг), указанному в лицензии, до устранения выявленных нарушений.

Решение ФАПСИ о выдаче лицензии на ввоз (вывоз) шифровальных средств выдается только на конкретную партию изделий. Наличие заключенных договоров не является основанием для выдачи положительного решения о возможности ввоза (вывоза) шифровальных средств.

Данные нормы соответствуют установленному порядку внешнеэкономической деятельности. Заключаемые договора, как правило, содержат статью, учитывающую форс-мажорные обстоятельства, предусматривающие возможный отказ уполномоченных государственных органов в выдаче лицензии на ввоз (вывоз) шифровальных средств. Конкретная партия товара определяется объемом, этапностью и сроками поставок, оговоренных конкретным договором.

Деятельность по лицензированию в области зашиты информации осуществляется на основании следующих принципов:
- соответствия действующим Российским законодательным и нормативным актам;
- системного и комплексного подхода к решению вопросов лицензирования и сертификации;
- обеспечения надежной защиты информации, составляющей государственную тайну, или иной конфиденциальной информации;
- дифференцированного подхода к отдельным видам деятельности и средствам защиты;
- наложения на лицензиата обязательств по выполнению требований Российского законодательства и иных нормативных актов в области защиты информации;
- соответствия заявителей и лицензиатов требованиям по профессиональной подготовке, нормативно методической, технической и технологической оснащенности, режимным требованиям, проверяемым в ходе проведения обязательной экспертизы заявителей и постоянного контроля за деятельностью лицензиатов;
- четкой регламентации предоставляемых лицензиату прав и полномочий, а также механизма его взаимодействия с ФАПСИ;
- централизованности выдачи, приостановления и отзыва лицензий и сертификатов;
- доступности и открытости систем лицензирования и сертификации в рамках выше перечисленных принципов.

Соответственно лицензирование деятельности предприятия в области защиты информации включает следующие действия:
- выдачу лицензий (решений о выдаче лицензий) - подачу, рассмотрение, заявление на лицензирование, оформление и выдачу лицензий (решений о выдаче лицензий), переоформление лицензий;
- проведение специальной экспертизы заявителя;
- проведение аттестации руководителя предприятия или лиц уполномоченных им для руководства лицензируемой деятельности;
- проведение технической экспертизы изделий.

5.3.2. Лицензирование средств криптографической защиты информации

В соответствии с упомянутыми выше законами, а также на основании Закона Российской Федерации от 10 июня 1993 года № 5151-1 **“О сертификации продуктов и услуг”** ФАПСИ 15 ноября 1993 года зарегистрировало в Госстандарте России **“Систему сертификации средств криптографической защиты информации”** РОСС.RU.0001.030001. Данный документ определил организационную структуру системы сертификации шифровальных средств ФАПСИ, а также установил основные правила проведения сертификационных исследований и испытаний криптографических средств защиты информации и закрытых с их помощью систем и комплексов обработки, хранения и передачи информации.

Если разработка, производство, реализация шифровальных средств осуществляется относительно небольшим числом предприятий и организаций, то вопросы лицензирования эксплуатации подобных средств и оказания услуг с их использованием затрагивает интересы несравненно большего числа предприятий, организаций и учреждений. В первую очередь к таким организациям следует отнести банки и другие финансово-кредитные организации, широко применяющие шифровальные средства и средства электронной цифровой подписи для защиты информации, составляющей банковскую или коммерческую тайну, но не содержащей сведений, составляющих государственную тайну

В общем случае, как и все иные юридические лица, банк может заявлять права на осуществление любой деятельности связанной с защитой информации в системах электронного документооборота. Поэтому более правильно, с учетом ситуации, которая дефакто сложилась в стране, говорить о видах деятельности, на которые необходимо получить лицензию.

На наш взгляд, таких видов деятельности три (в соответствии с перечнем видов деятельности, подлежащих лицензированию ФАПСИ):

- эксплуатация шифровальных средств защиты информации при ее обработке, хранении и передаче по каналам связи, и (или) средств электронной цифровой подписи (независимо от способа реализации и контекста использования этих средств), а также шифровальных средств для защиты электронных платежей с использованием пластиковых кредитных карточек и смарт-карт;
- оказание услуг по защите (шифрованию) информации;
- монтаж, установка, наладка шифровальных средств для защиты информации при ее обработке, хранении и передаче по каналам связи, и (или) средств электронной цифровой подписи, шифровальных средств для защиты электронных платежей с использованием пластиковых кредитных карточек и смарт-карт.

Как уже отмечалось выше, в соответствии с имеющимися законодательными и нормативными актами, лицензию должно получать каждое юридическое лицо, осуществляющее деятельность в области защиты информации. Для представляющих наибольший интерес защищенных криптографическими средствами систем обмена и расчета “банк-клиент” это означает, что в классическом варианте за лицензией на эксплуатацию шифровальных средств должен обращаться как сам банк так и его клиенты, являющиеся абонентами сети электронного документооборота. Однако, учитывая особенности банковского документооборота, ФАПСИ проработало вопрос о возможности применения иного порядка лицензирования установки, эксплуатации сертифицированных шифровальных средств и предоставления услуг по шифрованию информации не содержащей сведений, составляющих государственную тайну, в корпоративных сетях типа “банк-клиент”, системах финансового и фон-

дового рынка при защите информации по уровню “С”. В принципе, данный порядок лицензирования перечисленных видов деятельности может быть распространен на другие предприятия, организации и учреждения Российской Федерации.

Под **уровнем “С”** при этом понимается криптографическая защита информации на уровне потребителя. Информационно-телекоммуникационные системы создаются предприятием самостоятельно на основе сертифицированных средств криптографической защиты информации (СКЗИ), предназначенных для защиты конфиденциальной информации, встраивание которых в прикладные системы должно происходить с выполнением интерфейсных и криптографических протоколов, определенных технической документацией на СКЗИ.

Если коротко характеризовать разработанный порядок, то можно сказать, что банку (или предприятию-организатору сети) будет выдаваться лицензия на право эксплуатации всей защищенной криптографическими средствами сети, включающей всех его клиентов, А именно:

1. Лицензия на право установки, эксплуатации сертифицированных ФАПСИ шифровальных средств и предоставления услуг по шифрованию информации, не содержащей сведения составляющих государственную тайну, в конкретных корпоративных сетях типа “банк-клиент”, системах финансового и фондового рынка, предприятий, организаций и учреждений Российской Федерации при защите информации по уровню “С”, может выдаваться заявителю, который будет эксплуатировать сеть указанного типа (далее - организатор сети). Обязанности по обеспечению безопасности применения СКЗИ устанавливаются договорами, заключаемыми организатором сети с пользователями сети. Пользователи сети эксплуатируют сертифицированные СКЗИ без оформления лицензий. При необходимости Лицензионный центр ФАПСИ выдает пользователям такой сети по их заявкам заверенную копию лицензии организатора сети с указанием их наименования и юридического адреса. Вместе с тем, наличие подобной лицензии или ее копии не освобождает организатора сети и пользователей его корпоративной сети от необходимости получения отдельных лицензий на право эксплуатации иных средств криптографической защиты информации;
2. Для создания соответствующих условий осуществления лицензируемой деятельности заявитель в праве приобрести у изготовителя или его представителя опытную партию сертифицированных средств криптографической защиты информации, а также комплект необходимой технической или эксплуатационной документации до получения лицензии.
3. Вместо представления органа Государственной власти Российской Федерации заявитель в данном случае вправе представлять копию государственной лицензии на основной вид своей деятельности (например, копию банковской лицензии).
4. Специальная экспертиза заявителей на право установки, эксплуатации сертифицированных ФАПСИ шифровальных средств и предоставления услуг по шифрованию информации, не содержащей сведений, составляющих государственную тайну, в корпоративных сетях типа “банк-клиент”, системах финансового и фондового рынка, предприятий, организаций и учреждений Российской Федерации при защите информации по уровню “С” проводится аттестационным центром на основании заявки и представленного заявителем перечня сведений, подтверждающих выполнения им требований ФАПСИ, а также условий действия сертификатов соответствия на эксплуатируемые шифровальные средства.

В настоящий момент ФАПСИ разработало несколько видов требований к предприятиям, претендующим на получение лицензии Федерального агентства. Имеющиеся типовые требования конкретизируются и дифференцируются с учетом специфики отдельных видов деятельности и заявителей. Требования к заявителю на право установки, эксплуатации сертифицированных ФАПСИ шифровальных средств и предоставления услуг по шифрованию информации при защите информации по уровню “С”, приведены в Приложении.

Требования к заявителю на право установки, эксплуатации шифровальных средств и предоставления услуг по шифрованию информации

К заявителю на право установки, эксплуатации сертифицированных ФАПСИ шифровальных средств и предоставления услуг по шифрованию информации при защите информации по уровню “С” предъявляются следующие требования:

1. На предприятии-заявителе руководством должны быть выделены должностные лица, ответственные за разработку и практическое осуществление мероприятий по обеспечению функционирования и безопасности СКЗИ.
2. Вопросы обеспечения функционирования и безопасности СКЗИ должны быть отражены в специально разработанных документах, утвержденных руководством предприятия, с учетом эксплуатационной документации на СКЗИ.
3. На предприятии должны быть созданы условия, обеспечивающие сохранность конфиденциальной информации, доверенной предприятию юридическими и физическими лицами, пользующимися его услугами.
4. Размещение, специальное оборудование, охрана и режим в помещениях, в которых размещены СКЗИ (далее - помещения), должны обеспечивать безопасность информации, СКЗИ и шифрключей, сведение к минимуму возможности неконтролируемого доступа к СКЗИ, просмотра процедур работы с СКЗИ посторонними лицами.
5. Порядок допуска в помещения определяется внутренней инсгрукцией, которая разрабатывается с учетом специфики и условий функционирования конкретной структуры предприятия.
6. При расположении помещений на первых и последних этажах зданий, а также при наличии рядом с окнами балконов, пожарных лестниц и т.п., окна помещений оборудуются металлическими решетками, ставнями, охранной сигнализацией или другими средствами, препятствующими несанкционированному доступу в помещения. Эти помещения должны иметь прочные входные двери, на которые устанавливаются надежные замки.
7. Для хранения шифрключей, нормативной и эксплуатационной документации, установочных дискет помещения обеспечиваются металлическими шкафами (хранилищами, сейфами), оборудованными внутренними замками с двумя экземплярами ключей. Дубликаты ключей от хранилищ и входных дверей должны храниться в сейфе ответственного лица, назначаемого руководством предприятия.
8. Устанавливаемый руководителем предприятия порядок охраны помещений должен предусматривать периодический контроль технического состояния средств охранной и пожарной сигнализации и соблюдения режима охраны.
9. Размещение и установка СКЗИ осуществляется в соответствии с требованиями документации на СКЗИ.
10. Системные блоки ЭВМ с СКЗИ должны быть оборудованы средствами контроля их вскрытия.
11. Все поступающие для использования шифрключи и установочные дискеты должны браться на предприятии на поэкземплярный учет в выделенных для этих целей журналах.
12. Учет и хранение носителей шифрключей и установочных дискет, непосредственная работа сними поручается руководством предприятия специально выделенным работникам предприятия. Эти работники несут персональную ответственность за сохранность шифрключей.

13. Учет изготовленных для пользователей шифрключей, регистрация их выдачи для работы, возврата от пользователей и уничтожения ведется на предприятии.
14. Хранение шифрключей, установочных дискет допускается в одном хранилище с другими документами при условиях, исключающих их непреднамеренное уничтожение или иное, не предусмотренное правилами пользования СКЗИ, применение. Наряду с этим должна быть предусмотрена возможность раздельного безопасного хранения рабочих и резервных шифрключей, предназначенных для использования в случае компрометации рабочих шифрключей в соответствии с правилами пользования СКЗИ.
15. При пересылке шифрключей клиентам предприятия должны быть обеспечены условия транспортировки, исключающие возможность физических повреждений и внешнего воздействия на записанную ключевую информацию.
16. В случае отсутствия у оператора СКЗИ индивидуального хранилища, шифрключи по окончании рабочего дня должны сдаваться лицу, ответственному за их хранение.
17. Уполномоченными лицами периодически должен проводиться контроль сохранности входящего в состав СКЗИ оборудования, а также всего используемого программного обеспечения для предотвращения внесения программно-аппаратных закладок и программ-вирусов.
18. К работе с СКЗИ допускаются решением руководства предприятия только сотрудники, знающие правила его эксплуатации, владеющие практическими навыками работы на ЭВМ, изучившие правила пользования, эксплуатационную документацию и прошедшие обучение работе с СКЗИ.
19. Руководитель предприятия или лицо, уполномоченное на руководство заявленными видами деятельности, должно иметь представление о возможных угрозах информации при ее обработке, передаче, хранении, методах и средствах защиты информации.

5.4. Сертификация средств защиты информации

5.4.1. Основные принципы и правила системы сертификации средств защиты информации

Постановление от 26 июня 1995 года № 608 устанавливает общие принципы организации систем сертификации средств защиты информации, содержащей сведения, составляющие государственную тайну, всеми ведомствами Российской Федерации, наделенными законом правом проводить подобную сертификацию. Статьи Постановления определяют:

- участников системы сертификации средств защиты информации;
- права и обязанности участников;
- схемы проведения сертификационных испытаний;
- порядок выдачи, приостановления и аннулирования сертификатов;
- порядок оплаты услуг по сертификации;
- порядок контроля за качеством сертифицированных изделий;
- ответственность сторон за выполнение ими своих обязательств в системе сертификации.

Кроме того, данным положением к средствам защиты информации отнесены и средства контроля эффективности защиты информации.

Сертификация — это процесс, осуществляемый в отношении такой категории, как “изделие” (товар, средство) когда в результате выполнения комплекса мероприятий, определенных правилами и порядком ее проведения, устанавливается, удостоверяется или подтверждается качество изделия. Таким образом, сертификация есть деятельность некоторой третьей стороны, независимой от изготовителя (продавца) и потребителя продукции или услуг, по подтверждению соответствия этих продукции или услуг установленным требованиям.

Сертификация средств защиты информации осуществляется Гостехкомиссией России и ФАПСИ. При этом, сертификация средств, отнесенных к компетенции ФАПСИ, определяется **“Системой сертификации” средств криптографической защиты информации (СКЗИ)”** РОСС.RU.0001.030001.

Данный документ представляет собой нормативный акт, который включает в себя положения и нормы, определяющие правила и общий порядок проведения сертификации в рассматриваемой предметной области. Он базируется на Законе Российской федерации “О сертификации продукции и услуг”, иных нормативных актах, утвержденных Госстандартом России, и соответствует вытекающим из них требованиям к порядку, схеме проведения, а также организационной структуре систем сертификации. тем самым учитываются сложившиеся к настоящему времени международные правила организации и проведения работ по сертификации продукции. С другой стороны, учтены и обобщены особенности и накопленный многолетний опыт работы в области защиты информации, оценки качества разрабатываемых и производимых средств защиты.

Порядок проведения сертификации средств защиты информации основан на следующих принципах и правилах:

1. Обязательность сертификации изделий, обеспечивающих защиту государственной тайны, или обязательность сертификации которых установлена нормативными актами Российской Федерации.

В настоящее время такое требование, в частности, установлено для средств защиты информации в системах электронного документооборота, используемых для обмена с Центральным Банком России, а также для средств и защищенных систем государственных предприятий или предприятий, на которых размещен государственный заказ.

2. На сертификацию принимаются изделия только от заявителей, имеющих лицензию на соответствующие виды деятельности.

Оформление установленным порядком права на осуществление деятельности в области защиты информации является первичным. Разрабатывать алгоритмы и средства защиты на их базе как продукцию, товар, предлагаемый на рынок, могут только предприятия, имеющие лицензию. Принятие на сертификацию только готовых изделий в целом, они их или отдельных компонент. В различных публикациях специалисты неоднократно указывали, что сами по себе даже высоконадежные средства защиты, в том числе криптографические алгоритмы или отдельные блоки и модули (аппаратные, аппаратно-программные и программные), реализующие часть процесса защиты, не могут обеспечить требуемого уровня защиты информации в комплексе, Например без реализации специальных мер эти средства могут быть просто обойдены или необходимая информация может быть получена за счет побочных .электромагнитных излучений и наводок, Для систем и комплексов, которые включают совокупность некоторого множества явно различимых как самостоятельное из-

делие функционально и конструктивно законченных элементов, возможно оформление сертификата на каждый из них.

3. Процедура сертификации осуществляется в отношении только технических средств или технической части системы защиты, с учетом условий их эксплуатации.

4. Двухступенчатость процесса сертификации при независимости организаций, проводящих экспертизу и сертификационные испытания: сертификация средств защиты информации осуществляется Центральным органом по сертификации, а испытания проводятся в аккредитованных испытательных центрах (лабораториях).

5. Дифференцированность подхода к уровню защиты различных видов информации.

6. Обязательность использования криптографических алгоритмов, являющихся стандартами или ранее рекомендованных либо разработанных ФАПСИ.

Специально подчеркнем, что факт одобрения ФАПСИ алгоритма до его технической реализации является одним из основных требований к представляемым на сертификацию изделиям криптозащиты. Это одобрение может быть осуществлено путем утверждения алгоритма:

- в качестве государственного стандарта;
- Правительством Российской Федерации;
- ФАПСИ

Отсюда следует, что изделия, реализованные на базе собственных оригинальных алгоритмов, ранее не представлявшихся в ФАПСИ, а равные изделия, реализующие алгоритмы иностранной разработки, или импортные шифровальные средства на сертификацию не принимаются

Например, в зависимости от полноты реализуемой защиты, для системы конфиденциального электронного документооборота устанавливаются три уровня обеспечения безопасности (сертификации):

- уровень “А” — сертификат выдается на систему защиты в целом и подтверждает соответствие реализации средств шифрования заданным криптографическим алгоритмам, комплексное выполнение требований ФАПСИ к шифровальным средствам с учетом их программного окружения, наличие защищенной (без недокументированных возможностей) аппаратно-программной среды;

- уровень “В” - сертификат выдается на систему защиты, включающую шифровальные средства и их программное окружение, и подтверждает соответствие реализации средств шифрования заданным криптографическим алгоритмам и требованиям ФАПСИ, выполнение требований ФАПСИ к программному окружению шифровальных средств;

- уровень “С” - сертификат выдается только на шифровальные средства и подтверждает соответствие реализации средств шифрования заданным криптографическим алгоритмам и требованиям.

6. Принятие Центральным органом по сертификации и испытательными центрами (лабораториями) ответственности за выполнение возложенных на них функций в соответствии с действующим законодательством и договорными обязательствами.

7. Сертификационные испытания средств защиты информации могут осуществляться только аккредитованными испытательными сертификационными центрами. Действитель-

ное соответствие изделия государственным стандартам и гарантию удовлетворения требований по безопасности удостоверяет только сертификат Гостехкомиссии или ФАПСИ.

8. Принятие и неуклонное соблюдение заявителем правил, установленных в системе сертификации.

Действие выданного сертификата может быть приостановлено или сертификат может быть вообще аннулирован по результатам инспекционного контроля за сертифицированными средствами защиты информации.

Причинами приостановления и аннулирования сертификата могут быть:

- изменение нормативных и методических документов на средства защиты информации или их элементов, на испытания и контроль;
- изменения конструкции, состава или комплектности средства защиты информации;
- невыполнение требований технологии или технических условий на изделие;
- отказ заявителя в допуске для проведения научно-технического и инспекционного контроля.

Организационная структура системы сертификации включает в себя Гостехкомиссию или ФАПСИ как Государственный орган по сертификации средств защиты информации, Центральный орган системы сертификации и Испытательные центры (лаборатории) средств защиты информации, а также заявителей.

В заключение следует отметить, что системы лицензирования и сертификации проходят сейчас стадию совершенствования с точки зрения развития правовой базы, механизма и правил их функционирования. Отсюда, разумеется, следует, что отдельные положения могут быть изменены, уточнены или дополнены.

ЧАСТЬ 3. ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

6. АДМИНИСТРАТИВНЫЙ УРОВЕНЬ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

После определения правовых основ безопасности автоматизированных (АС) следует осуществление *практических мероприятий* по созданию системы обеспечения безопасности информации (ОБИ). Указанные мероприятия включают следующие этапы [14, 24, 45, 56, 57, 60, 62, 70]:

1. *Разработка политики безопасности;*
2. *Проведение анализа рисков;*
3. *Планирование обеспечения информационной безопасности;*
4. *Планирование действий в чрезвычайных ситуациях;*
5. *Подбор механизмов и средств обеспечения информационной безопасности.*

Первые два этапа обычно трактуются как выработка политики безопасности и составляют так называемый административный уровень системы ОБИ предприятия.

Третий и четвертый этапы заключаются в разработке процедур безопасности. На этих этапах формируется уровень планирования системы ОБИ.

На последнем этапе практических мероприятий определяется программно-технический уровень системы ОБИ.

Законы и стандарты в области информационной безопасности являются лишь отправным нормативным базисом системы ОБИ информационной системы. Основой практического построения интегрированной системы является создание *административного уровня* системы, определяющее генеральное направление работ по ОБИ.

Целью административного уровня является разработка программы работ в области информационной безопасности и обеспечение ее выполнения. Программа представляет официальную политику безопасности, отражающую собственный концептуальный подход организации к ОБИ. Конкретизация политики безопасности выражается в планах по информационной защите АС.

6.1. Разработка политики безопасности

В “Оранжевой книге” [76] *политика безопасности* (security policy) трактуется как набор норм, правил и практических приемов, которые регулируют управление, защиту и распределение ценной информации. На практике политика безопасности трактуется несколько шире — как совокупность документированных административных решений, направленных на обеспечение безопасности информационного ресурса. Результатом политики является высокоуровневый документ, представляющий систематизированное изложение целей, задач, принципов и способов достижения информационной безопасности.

Данный документ представляет методологическую основу практических мер (процедур) по реализации ОБИ и содержит следующие группы сведений.

1. Основные положения информационной безопасности.
2. Область применения.
3. Цели и задачи обеспечения информационной безопасности.
4. Распределение ролей и ответственности.
5. Общие обязанности.

Основные положения определяют важность ОБИ, общие проблемы безопасности, направления их решения, роль сотрудников, нормативно-правовые основы.

Областью применения политики безопасности являются основные активы и подсистемы АС, подлежащие защите. Типовыми активами являются программно-аппаратное и информационное обеспечение АС, персонал, в отдельных случаях информационная инфраструктура предприятия.

Цели, задачи, критерии ОБИ вытекают из функционального назначения предприятия. Например, для режимных организаций на первое место ставится соблюдение конфиденциальности. Для сервисных информационных служб реального времени важным является обеспечение доступности (оперативной готовности) подсистем. Для информационных хранилищ актуальным может быть обеспечение целостности данных и т.д. Здесь указываются законы и правила организации, которые следует учитывать при проведении работ по ОБИ.

Типовыми целями могут быть следующие:

- обеспечение уровня безопасности, соответствующего нормативным документам предприятия;
- следование экономической целесообразности в выборе защитных мер;
- обеспечение соответствующего уровня безопасности в конкретных функциональных областях АС;
- обеспечение подотчетности всех действий пользователей с информационными ресурсами и анализа регистрационной информации;
- выработка планов восстановления после критических ситуаций и обеспечения непрерывности работы АС и др.

Если предприятие не является изолированным, цели и задачи рассматриваются в более широком контексте: должны быть оговорены вопросы безопасного взаимного влияния локальных и удаленных подсистем.

В рассматриваемом документе могут быть конкретизированы некоторые стратегические принципы безопасности (вытекающие из целей и задач ОБИ). Таковыми являются стратегии действий в случае нарушения политики безопасности предприятия и сторонних организаций, взаимодействия с внешними организациями, правоохранительными органами, прессой и др. В качестве примера можно привести две стратегии ответных действий на нарушение безопасности:

- “выследить и осудить”, когда злоумышленнику позволяют продолжить действия с целью его компрометации и наказания (данную стратегию одобряют правоохранительные органы!);
- “защититься и продолжить”, когда организация опасается за уязвимость информационных ресурсов и оказывает максимальное противодействие нарушению.

Обстоятельства, позволяющие выбрать стратегию, приведены в таблице 6.1.

Таблица 6.1.

Доводы за выбор стратегии ответных действий на нарушение

Защититься и продолжить	Выследить и осудить
♦ активы ИВС недостаточно защищены, ♦ продолжительность вторжения сопряжена с финансовым риском, ♦ неизвестен круг пользователей, ♦ пользователи могут привлечь к ответственности организацию ИВС за нанесенный ущерб и др.	♦ ИВС хорошо защищена, имеются надежные средства резервирования, ♦ имеют место повторяющиеся и частые атаки, ♦ действия злоумышленника можно контролировать, ♦ организация имеет положительный опыт работы с правоохранительными и правозащитными органами и др.

Политика безопасности затрагивает всех пользователей компьютеров в организации. Поэтому важно решить так называемые политические вопросы наделения всех категорий пользователей соответствующими правами, привилегиями и обязанностями.

Для этого определяется круг лиц, имеющий доступ к подсистемам и сервисам АС. Для каждой категории пользователей описываются правильные и неправильные способы использования ресурсов — что запрещено и разрешено. Здесь специфицируются уровни и регламентация доступа различных групп пользователей. Следует указать какое из правил умолчания на использование ресурсов принято в организации, а именно:

- что явно не запрещено, то разрешено или
- что явно не разрешено, то запрещено.

Одним из самых уязвимых мест в ОБИ является распределение прав доступа. В политике безопасности должна быть утверждена схема управления распределением прав доступа к сервисам — централизованная или децентрализованная, или иная. Должно быть четко определено, кто распоряжается правами доступа к сервисам и какими именно правами. Целесообразно детально описать практические процедуры наделения пользователей правами. Здесь следует указать должностных лиц, имеющих административные привилегии и пароли для определенных сервисов.

Права и обязанности пользователей определяются применительно к безопасному использованию подсистем и сервисов АС. При определении прав и обязанностей администраторов следует стремиться к некоторому балансу между правом пользователей на тайну и обязанностью администратора контролировать нарушения безопасности.

Важным элементом политики является распределение ответственности. Политика не может предусмотреть всего, однако она должна для каждого вида проблем найти ответственного.

Обычно выделяется несколько уровней ответственности. На первом уровне каждый пользователь обязан работать в соответствии с политикой безопасности (защищать свой счет), подчиняться распоряжениям лиц, отвечающих за отдельные аспекты безопасности, ставить в известность руководство обо всех подозрительных ситуациях. Системные администраторы отвечают за защиту соответствующих информационно-вычислительных подсистем. Администраторы сетей должны обеспечивать реализацию организационно-технических мер, необходимых для проведения в жизнь политики безопасности АС. Более высокий уровень - руководители подразделений отвечают за доведение и контроль положений политики безопасности.

С практической точки зрения, политику безопасности целесообразно разделить на несколько уровней. Как правило, выделяют два-три уровня.

Верхний уровень носит общий характер и определяет политику организации в целом. Здесь основное вниманию уделяется: порядку создания и пересмотра политики безопасности; целям, преследуемым организацией в области информационной безопасности; вопросам выделения и распределения ресурсов; принципам технической политики в области выбора методов и средств защиты информации; координированию мер безопасности; стратегическому планированию и контролю; внешним взаимодействиям и другим вопросам, имеющим общеорганизационный характер.

На указанном уровне формулируются главные цели в области информационной безопасности (определяемые сферой деятельности предприятия): обеспечение конфиденциальности, целостности и/или доступности.

Средний уровень политики безопасности выделяют в случае структурной сложности организации либо при необходимости обозначить специфичные подсистемы организации. Это касается отношения к перспективным, еще не достаточно апробированным технологиям. Например, использование новых сервисов Internet, организация связи и обработка информации на домашних и портативных компьютерах, степень соблюдения положений компьютерного права и др. Кроме того, на среднем уровне политики безопасности могут быть выделены особо значимые контуры АС организации, например, обрабатывающие секретную или критично важную информацию.

За разработку и реализацию политики безопасности верхнего и среднего уровней отвечают руководитель службы безопасности, администраторы безопасности АС, администратор корпоративной сети.

Нижний уровень политики безопасности относится к конкретным службам или подразделениям организации и детализирует верхние уровни политики безопасности. Данный уровень необходим, когда вопросы безопасности конкретных подсистем требуют решения на управленческом, а не только на техническом уровне.

Понятно, что на данном уровне определяются конкретные цели, частные критерии и показатели информационной безопасности, определяются права конкретных групп пользователей, формулируются соответствующие условия доступа к информации и т.п. Здесь из конкретных целей выводятся (обычно формальные) *правила безопасности*, описывающие, кто, что и при каких условиях может делать или не может. Более детальные и формальные правила упростят внедрения системы и настройку средств ОБИ.

На этом уровне описываются механизмы защиты информации и используемые программно-технические средства для их реализации (в рамках, конечно, управленческого уровня, но не технического).

За политику безопасности нижнего уровня отвечают системные администраторы.

В рамках разработки политики безопасности проводится анализ рисков (risk analysis). Это делается с целью минимизации затрат на ОБИ. Напомним, что основной принцип безопасности — затраты на средства защиты не должны превышать стоимости защищаемых объектов. При этом если политика безопасности оформляется в виде высокоуровневого документа, описывающего общую стратегию, то анализ рисков (как приложение) оформляется в виде списка активов, нуждающихся в защите. Рассмотрим этап анализа риска подробнее.

6.2. Проведение анализа риска

Использование АС связано с определенной совокупностью рисков, под которыми понимается стоимостные выражения событий (обычно вероятностных), ведущих к потерям. Если риск не приемлем, то необходимо предпринять защитные меры, не превышающие по стоимости возможный ущерб.

Анализ риска главным образом необходим для следующего:

- выявления уязвимости АС и ее системы защиты,
- определения необходимых и достаточных затрат на ОБИ,
- выбора конкретных мер, методов, средств и систем защиты,
- повышения информированности и компетентности персонала АС.

В целом, периодический анализ риска необходим для планирования компромисса между степенью безопасности АС и ее качественными характеристиками, как-то: стоимость, производительность, функциональность, удобство работы, масштабируемость, совместимость и др.

6.2.1. Основные этапы анализа риска

Работа по анализу риска состоит в том, чтобы оценить величину рисков, выработать меры по их уменьшению и затем убедиться, что риски заключены в приемлемые рамки. Алгоритм анализа риска представлен на рисунке 6.1.

Анализ риска — процесс нелинейный и взаимосвязанный. Практически все его этапы связаны между собой, и по завершении почти любого из них может выявиться необходимость возврата к предыдущему.

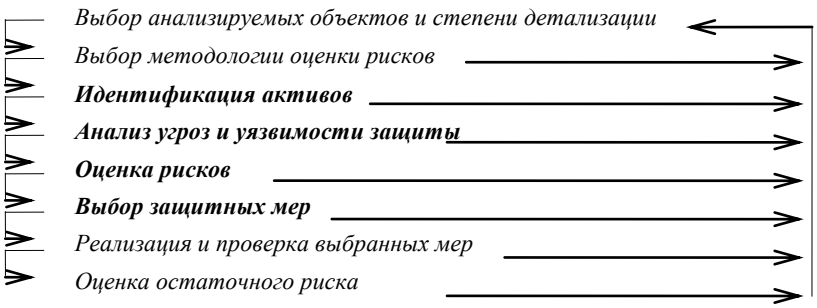

Рис. 6.1. Алгоритм анализа риска

6.2.2. Предварительный этап анализа риска

На начальном этапе методом экспертной оценки решаются общие вопросы проведения анализа риска.

Первым делом выбираются компоненты АС и степень детальности их рассмотрения. Всеобъемлющий анализ требует рассмотрения всей информационной инфраструктуры. Но на практике из принципа разумной достаточности могут быть выделены и подвергнуты большей детализации отдельные наиболее важные компоненты и службы, в первую очередь, где риски велики или неизвестны. Более тщательному анализу подвергаются новые и модифицированные компоненты АС, а также компоненты, где имели место новые инциденты и нарушения безопасности.

Далее выбираются методологии оценки рисков как процесса получения количественной или качественной оценки ущерба, который может произойти в случае реализации угроз безопасности АС. Методологии носят частный характер, присущий организации и АС, и зависят от конкретного множества дестабилизирующих факторов и условий функционирования АС, возможности их количественной оценки, степени их неточности, неполноты, нечеткости и т.д. На практике, с учетом допустимой приближенной оценки рисков, часто используют простые наглядные методы, основанные на элементах теории вероятности и математической статистики.

6.2.3. Идентификация активов

Основу процесса анализа риска составляет определение: что надо защищать, от кого и как. Для этого выявляются активы (компоненты АС), нуждающиеся в защите. Некоторые активы (например, технические и программные средства) идентифицируются очевидным образом. Про некоторые активы (люди, расходные материалы) часто забывают. При идентификации активов могут быть затронуты и нематериальные ценности, способные, однако, пострадать от нарушения режима безопасности, например: репутация компании, моральный климат в коллективе.

В таблице 6.2. представлены основные категории активов АС предприятия.

Таблица 6.2.

Основные активы информационной системы предприятия

Категории активов	**Компоненты информационной системы**
Аппаратное обеспечение	Компьютеры, периферийные устройства, коммуникационные линии, сетевое оборудование и их составные части
Программное обеспечение	Исходные, объектные и загрузочные модули операционных систем, вспомогательных системных и коммуникационных программ, инструментальных средств разработки, прикладных программных пакетов
Информационное обеспечение	Вводимые и обрабатываемые, хранимые, передаваемые и резервные (сохранные копии) данные и метаданные
Персонал	Обслуживающий персонал и пользователи
Документация	Конструкторская, техническая, пользовательская и иная документация
Расходные материалы	Бумага, магнитные носители, картриджи и т.д.

В некоторых специфичных АС активы, уникальные для организации, могут быть выделены в отдельные группы, например: коммуникационное, алгоритмическое или лингвистическое обеспечение. Кроме того, могут подлежать защите части инфраструктуры, в частности подсистемы электроснабжения и др.

В процессе идентификации активов фиксируются технологии ввода, хранения, обработки и передачи информации в системе. Главным результатом процесса идентификации активов является получение детальной информационной структуры организации и способов использования информации. Дальнейшие этапы анализа риска основываются именно на данной, зафиксированной на некоторый момент времени, информации.

6.2.4. Анализ угроз

После идентификации активов АС следует рассмотреть все возможные угрозы указанным активам, оценить риски и ранжировать их по степени возможного ущерба.

Под угрозой обычно понимают любое событие (действие), которое потенциально может нанести ущерб АС путем нарушения нарушению конфиденциальности, целостности или доступности информации. Угрозы могут быть преднамеренными, являющимися следствием умышленных (злонамеренных) действий людей, и непреднамеренные, вызванные ошибками человека или сбоями и отказами работы технических и программных средств, или стихийными действиями.

В таблице 6.3. приведены примеры общих угроз, способных привести к нарушению конфиденциальности, целостности и доступности информации.

Таблица 6.3.

Примеры угроз информационной системы

Реализация угроз	Объекты воздействия			
	Информационное обеспечение	**Программное обеспечение**	**Техническое обеспечение**	**Персонал**
Нелегальное ознакомление (чтение)	НСД, копирование, размножение, хищение, перехват, дешифрование	НСД, внедрение вирусов и закладок, использование дефектов, ошибки	НСД, внедрение закладок, нарушение режимов работы, хищение носителей, отказы, ошибки	некомпетентность, халатность, разглашение, подкуп, вербовка
Несанкционированное уничтожение или модификация	НСД, искажение, удаление, модификация	НСД, внедрение вирусов и закладок, использование дефектов, ошибки	НСД, внедрение закладок, нарушение режимов работы, отказы, ошибки	некомпетентность, халатность, подкуп, вербовка
Отказ в обслуживании	НСД, удаление, искажение адресации	НСД, искажение, удаление, подмена, внедрение вирусов и закладок, использование дефектов, ошибки	НСД, внедрение закладок, разрушение, перегрузка, выход из строя, нарушение режимов работы, отказы, ошибки	некомпетентность, халатность, нарушение режимов работы, болезнь

В реальной жизни список существенно полнее и конкретнее. Например, распространенными угрозами в среде Интернет являются: нарушение работы сетевых устройств и служб, макровирусы, передаваемые вместе с присоединяемыми файлами электронной почты, вандалы — плохо отлаженные апплеты Java и ActiveX, перехват электронной почты, взлом корпоративных сетей, кража или неавторизованное изменение корпоративной информации.

При анализе угроз необходимо выявить их источники (см. табл. 6.4) и условия реализации. Это поможет в выборе дополнительных средств защиты. Часто одни угрозы могут быть следствием или условием проявления ряда других угроз. Например, несанкционированный доступ (в различных формах его проявления) к ресурсам облегчает реализацию практически любой угрозы: от порчи магнитного носителя до комплексной удаленной атаки.

Таблица 6.4.

Обобщенные источники угроз безопасности информационной системы

Внешние источники угроз	Внутренние источники угроз
• атмосферные явления, стихийные бедствия, катастрофы, аварии • деятельность конкурирующих экономических структур, • деятельность преступных группировок и лиц и др.	• нарушение персоналом режимов безопасности, • отказы и сбои аппаратных средств и носителей информации • ошибки программного обеспечения, • деятельность преступных группировок и лиц и др.

6.2.5. Оценка рисков

После идентификации угрозы необходимо оценить риск проявления угрозы. В большинстве случаев возможно получить количественную оценку риска. Она может быть получена на базе экспертного опроса, оценена статистически или рассчитана по некоторой математической зависимости (адекватной конкретной угрозе конкретному активу).

Кроме вероятности осуществления угрозы, важен размер ожидаемых потерь. В общем случае ожидаемые потери рассчитываются по следующей формуле: $\boldsymbol{e = p \cdot v}$, где $\boldsymbol{p}$ — вероятностная оценка риска проявления угрозы, $\boldsymbol{v}$ — ущерб при реализации угрозы. Однако, как вероятности угрозы, так и ожидаемые потери не всегда можно оценить количественно. Например, рассчитать замену компьютера достаточно просто, но трудно оценить потенциальный ущерб в случае задержки выдачи данных, искажения информации, разглашения отдельных сведений и т.д. Некоторые инциденты могут нанести ущерб репутации фирмы, вызвать социальную напряженность в коллективе, повлечь юридическое преследование предприятия со стороны пользователей и т.д.

Приведем примеры простых способов оценки вероятностей проявления угроз и возможных потерь:

1. Экспертная оценка событий. Методы экспертных оценок применяются при оценке трудно предсказуемых угроз, например стихийных бедствий, и являются самыми неточными.
2. Методика определения приемлемости уровня риска по трехбалльной шкале [45]. Согласно методике, оцениваемым рискам и ущербам ставятся оценки по трехбалльной шкале *{1, 2, 3}*. Полученные два множества оценок рисков и ущербов перемножаются. Множество возможных значений будет следующим: *{1, 2, 3, 4, 6, 9}*. Полагается, что первые два значения характеризуют низкий уровень риска, третий и четвертый — средний, два последних — высокий.
3. Методика определения приемлемости уровня риска с учетом видимости угроз и их последствий [60]. Здесь вводится понятие видимости угрозы для внешнего мира — мера информации о системе, доступной злоумышленнику (и вызывающей нездоровый интерес). Согласно указанной методике, оцениваемым рискам, видимости, физическим ущербам и моральным ущербам ставятся оценки по трехбалльной шкале *{1, 2, 3}*. Значения рисков умножаются на значения для видимости, а значения для физического ущерба

умножаются на значения для морального ущерба. Затем полученные два числа складываются. Считается, что уровень риска низкий, если итоговое число меньше *7*, высокий, если итоговое число больше *11*, иначе — средний.

4. Статистическая оценка событий и использование статистических моделей (отражающих законы распределения конкретных типов угроз). Данный метод позволяет получить приемлемые результаты для оценки часто проявляемых регистрируемых угроз, например: сбоев и отказов вычислительного процесса.
5. Использование аналитических моделей (возможно в виде таблиц) потенциального ущерба в зависимости от заранее определенных коэффициентов. Примером может быть модель IBM [84], где логарифмическая степень возможных потерь приближенно вычисляется по следующей формуле:

$$E \approx (0.3)(10^{P+V-3}),$$

где: $V \approx \log_{10} v$ — коэффициент, характеризующий значение возможного ущерба при реализации угрозы;

$P \approx 3 + \log_{10} 3p$ — коэффициент, характеризующий возможную частоту возникновения соответствующей угрозы.

Физически коэффициент P представляет логарифмическую частоту угрозы, рассчитываемую согласно следующей таблице.

Таблица 6.5.

Логарифмическая частота угрозы

P	**Частота проявления угрозы**
1	Раз в 300 лет
2	Раз в 30 лет
3	Раз в 3 года (1000 дней)
4	Раз в 100 дней
5	Раз в 10 дней
6	Раз в день
7	10 раз в день
8	100 раз в день

Более научно-обоснованным является метод многофакторных испытаний. Здесь определяют наиболее значимые факторы (проявившиеся признаки), оказывающие влияние на оцениваемую величину, в данном случае — это вероятность реализации угрозы или ожидаемые потери. Затем, рассчитывают коэффициенты, соответствующие факторам, и получают математическую зависимость (полином) от соответствующих факторов, например:

$$e = \sum_{i=0}^{k} b_i x_i + \sum_{i \neq j}^{k} b_{ji} x_i x_j + \sum_{i=1}^{k} b_{ii} x_i^2,$$

где: b_i - коэффициент i-го фактора, k - число факторов.

В случае выбора двух наиболее значимых факторов, указанный метод сводится к простому методу наименьших квадратов. В пассивном методе многофакторных испытаний анализируется статистический материал (значения факторов и оцениваемой величины), в активном — проводятся собственные ускоренные испытания.

Следует оговориться, что методы анализа риска обычно не отличаются высокой точностью. Дело в том, что основная задача анализа риска (как инструмента планирования) оценить уровень возможных потерь и уровень затрат на защиту. Для практики, когда разнородные исходные данные имеют приближенный или субъективный характер оценки, высокая точность расчета и не требуется. Иногда вообще невозможно оценить точность результата.

6.2.6. Выбор и проверка защитных мер

Для уменьшения размера ущерба необходим выбор соответствующих мер защиты: организационных, физических, программно-технических и др. Каждая угроза может быть предотвращена различными способами. Поэтому на данном этапе решается задача анализа и синтеза мер, методов и средств защиты по критерию эффективность/стоимость с учетом, конечно, технической политики организации и других жизненно важных характеристик АС.

После выбора способов защиты АС производится проверка их эффективности. Если остаточные риски стали опять-таки неприемлемы, весьма разумно повторить этапы анализа риска.

Завершая подраздел, следует отметить, что разработка политики безопасности и проведение анализа риска являются кропотливыми научно-техническими задачами. Поэтому важно правильно подобрать коллектив разработчиков. Обычно этим профессионально занимается группа информационной безопасности предприятия. Однако возможно привлечение администраторов и разработчиков систем и сетей, специалистов по аудиту и управлению, психологов, представителей службы режима.

7. ПЛАНИРОВАНИЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Политика безопасности определяет - что нужно защищать, а процедуры защиты - как надо защищать. Поэтому после определения официальной политики безопасности следует подготовить конкретизирующие ее плановые документы, описывающие практические процедуры защиты при работе АС. Таких документов обычно два:

1. План защиты (security plan);
2. План обеспечения непрерывной работы и восстановления функционирования АС (contingency and recovery plan).

7.1. План защиты

План защиты — документ, определяющий текущую реализацию системы ОБИ и необходимый в повседневной работе. План защиты периодически пересматривается с целью совершенствования и приведения в соответствии с текущим состоянием АС и системы ОБИ.

Указанный план необходим для следующего:

- определения общих правил обработки информации в АС, ее систему ОБИ, подготовку специалистов и т.п.
- фиксирования текущего состояния и состава АС и системы ОБИ,
- определения должностных обязанностей и степени ответственности сотрудников.

План может содержать следующие группы сведений:

1. Общие положения, отражающие политику безопасности;
2. Текущее состояние системы и ее уязвимость;
3. Рекомендации по реализации системы защиты;
4. Ответственность персонала;
5. Порядок ввода в действие средств защиты;
6. Порядок пересмотра средств защиты.

Следует помнить, что дублирование сведений в различных документах не допустимо. То есть в планах отражаются лишь требующие конкретизации положения политики безопасности.

В нашей стране стандарты и рекомендации в области информационной безопасности корпоративных сетей находятся на стадии становления. Потому основное содержание плана защиты мы рассмотрим в контексте Руководства по информационной безопасности предприятия в США [65, 68, 77, 79].

Итак, общие положения плана отражают политику безопасности и анализ риска. Это является базой выработки процедур безопасности, в деталях описывающие шаги, предпринимаемые организацией для ОБИ.

Следующим разделом плана является детальное описание текущего состояния АС и ее уязвимости. Данный раздел является отражением анализа риска. В [46] перечислены наиболее характерные уязвимости АС предприятия, на которые следует особо обратить внимание при составлении плана защиты, это:

- точки доступа;
- неправильно сконфигурированные системы;
- программные ошибки;
- внутренние враги.

Следует, однако, помнить, что в каждой организации есть собственные, присущие только ей, уязвимые места: для этого и проводится анализ риска.

Стержнем плана являются рекомендации по реализации системы ОБИ, т.е. реальному воплощению политики безопасности в жизнь. Здесь целесообразно отметить следующие сведения:

1. Рекомендации по выбору общих средств и способов защиты. Выбираемые средства защиты образуют первостепенную линию обороны. Поэтому важно, чтобы средства и способы ОБИ были выбраны правильно. Например, если самой большой угрозой для АС считается стихийные бедствия, то, видимо, нет смысла использовать биометрические устройства для аутентификации. С другой стороны, если велика опасность в несанкционированных действиях со стороны сотрудников организации, то следует сделать упор на средствах регистрации и аудита совершаемых действий.
2. Определение стратегий защиты. Важнейшим способом защиты активов является использование нескольких различных стратегий (принцип эшелонированности обороны). Если одна линия обороны прорвана, вступает следующая стратегия. Например, хранение съемного винчестера в личном сейфе может удачно сочетаться с динамическим кодированием информации на нем. Комбинация из нескольких несложных стратегий может оказаться более прочной, чем один даже сложный метод защиты.
3. Физическая защита. Понятно, что свободный физический доступ является плацдармом для поражения информационного ресурса предприятия. Теоретически, одни программно-аппаратные средства не обеспечивают абсолютной защиты АС. Кроме того, некоторые механизмы безопасности выполняют свои функции исключительно при условии физической защиты. Поэтому, критически важные коммуникационные каналы, серверы, системы хранения информации и другие важные компоненты АС должны находиться в физически защищенных помещениях.
4. Выявление неавторизованной деятельности. Для этого могут использоваться следующие способы и средства:
    A. Анализ сообщений пользователей. Пользователи в своей работе сталкиваются с различными некорректными ситуациями, отдельные из которых могут свидетельствовать о неавторизованной деятельности нарушителей либо собственной оплошности. Например, пользователь (соблюдающий политику безопасности) зафиксировал более поздний вход в систему, чем был на самом деле. Или пользователь обнаружил истощение или изменение личных ресурсов (памяти на диске), неудачу при входе в систему, появление неизвестных файлов или еще что-то необычное.
    B. Отслеживание использования системы с помощью несложных пакетных файлов и программ. Такие программы можно разработать самому. К примеру, создать стандартный список пользователей и прав к ним (с помощью команд ОС) и его периодически сравнивать с текущим списком (опять же командой ОС). Обычно администратор с помощью “подручных” команд и утилит может: сравнивать текущий список активных пользователей, контролировать учетные записи с целью опреде-

ления профиля использования системы (необычные записи и др.), просматривать системные средства регистрации (syslog в UNIX), контролировать сообщения об ошибках - неудачных входах, выявлять запуск программ, которые неавторизованы или к ним нет прав у нарушителя.

C. Мониторинг системы администратором. Мониторинг представляет собой оперативное получение и анализ информации о состоянии АС с помощью специализированных средств контроля. Это является наиболее мощным средством выявления неавторизованной деятельности в режиме реального времени.

D. Ведение и анализ регистрационного журнала системы. Это позволяет фиксировать заданные события, связанные с информационной безопасностью. Важность анализа (аудита) регистрационных журналов трудно переоценить: они важны и для обнаружения и отслеживания нарушителя, выявления слабых мест в системе защиты, оптимизации производительности и безопасности, наконец, выявления пассивных сотрудников и др.

Для мониторинга и аудита обычно требуются специализированные системы контроля и сетевые анализаторы.

5. В разделе могут быть освещены действия в случае подозрений неавторизованной деятельности, однако, подробное изложение данного вопроса представлено в плане обеспечения непрерывной работы и восстановления.
6. Правила безопасной работы персонала. Обычно правила делятся в соответствии с категориями персонала, а именно:
   - правила безопасной работы, различные действия, процедуры докладов пользователей,
   - правила администрирования, конфигурационного управления, процедуры сохранения/восстановления, процедуры докладов администраторов.
7. Ресурсы для предупреждения нарушений безопасности. В данном разделе описываются программные, аппаратные и процедурные ресурсы, реализующие политику безопасности. Интегрированная система безопасности корпоративной сети обычно включает следующие средства (см. раздел 2):
   - системы и средства аутентификации (действия администратора, запрос-ответные парольные системы, система Kerberos, интеллектуальные карты и др.);
   - средства обеспечения целостности информации (контрольные суммы, иммитовставки, хеширование);
   - средства обеспечения конфиденциальности (шифрование) и средства аутентификации источника данных (электронная подпись);
   - сетевые соединения, межсетевые экраны и средства ограничения сетевого доступа (шлюзовые маршрутные таблицы, фильтрующие маршрутизаторы).

Особо в плане могут быть выделены типы процедур безопасности АС предприятия.

Перечислим наиболее типичные процедуры защиты информации:

1. Проверка системной безопасности. Элементом таких проверок является ревизия политики безопасности и защитных механизмов. Примерами могут быть плановые учения и отдельные проверки некоторых процедур.
2. Процедуры управления счетами. Это необходимо для предотвращения несанкционированного доступа к системе. Должны быть процедуры управления счетами и администраторов и пользователей. Администратор отвечает за заведение, удаление счетов и осу-

ществляет общий контроль. Пользователь может контролировать - пользовался ли кто-нибудь его счетом.
3. Процедуры управления паролями (процедуры выбора пароля и смены пароля).
4. Процедуры конфигурационного управления**.**

После рекомендаций по реализации защиты в плане могут быть конкретизирована ответственность и обязанности персонала.

Заканчивается план определением общих вопросов жизненного цикла системы защиты: внедрение, эксплуатация, сопровождение и снятие с эксплуатации. Здесь могут быть определены сроки и периодичность проверки систем защиты в соответствии с порядком пересмотра политики безопасности и анализа риска.

7.2. План обеспечения непрерывной работы и восстановления функционирования автоматизированной системы

Частью реакции на нарушения безопасности является предварительная подготовка ответных мер. Под этим понимается поддержание должного уровня защиты так, чтобы ущерб мог быть ограничен, а в дальнейшем исключен. Указанный план определяет действия персонала АС в критических ситуациях с целью обеспечения непрерывной работы и восстановления функционирования АС. Он должен исключить двусмысленности, возникающие во время инцидента.

Необходимость указанного плана диктуется следующим:
- предотвращением угрозы жизни людей,
- экономическими целями,
- требованиями по защите секретной, критически важной (особенно невосстановимой) информации,
- нежелательной оглаской в прессе,
- правовым аспектом (например, возможно преследование организации в судебном порядке).

Кроме того, наличие плана благотворно влияет на моральную обстановку в коллективе. Руководство знает, что при неблагоприятных условиях не придется начинать все сначала, пользователи уверены — какая-то часть их труда будет сохранена.

Обычно план состоит из двух частей, описывающих:
1. Меры реагирования на нарушения безопасности.
2. Восстановительные работы.

7.2.1. Меры реагирования на нарушения

Данные меры направлены на обнаружение и нейтрализацию нарушений. Они преследуют две основные цели:
- ограничение распространения угрозы и снижение ущерба,
- недопущение повторных нарушений.

В соответствии с этим строится указанная часть плана, которая содержит следующие группы сведений:

1. Основные положения.
2. Оценка инцидента.
3. Оповещение.
4. Ответные меры.
5. Правовой аспект.
6. Регистрационная документация.

В основных положениях документа формулируются цели политики безопасности в вопросах реакции на нарушения. Важно заранее определить приоритеты при решении спорных вопросов. После уяснения целей и приоритетов, они подлежат упорядочиванию по степени важности. В таблице 7.1. представлен пример типовых целей и приоритетов системы безопасности АС предприятия.

Таблица 7.1.

Вариант упорядочивания целей и приоритетов

Цели	**Приоритеты**
• Гарантировать целостность критически важных подсистем. • Сохранить и восстановить данные. • Сохранить и восстановить сервисы. • Выяснить причину инцидента. • Предотвратить развитие инцидента и будущие инциденты. • Избежать нежелательной огласки. • Найти виновников. • Наказать нарушителей.	• Защита жизни и здоровья людей. • Защита секретных и критически важных данных. • Защита прочих данных. • Предотвратить повреждение системы. • Минимизировать урон вычислительным ресурсам.

Большинство нарушений безопасности достаточно трудно идентифицируются. Для выявления нарушений безопасности в документе могут быть определены признаки нарушений. Таковыми могут быть: отказы подсистем, неестественная активность и ненормальные действия некоторых пользователей, новые файлы со странными именами, рассогласование в учетной информации, необычно низкая производительность, подозрительные пробы (многочисленные неудачные попытки входа), подозрительное изменение размеров и дат файлов или их удаление, появление новых пользовательских счетов, попытки записи в системные файлы, аномалии (звуковые сигналы и сообщения) и т.д. и т.п.

Идентификации инцидента сопутствует определение масштаба его последствия. Здесь целесообразно выяснить: затрагивает ли нарушение несколько организаций и подсистем АС, находится ли под угрозой критически важная информация, какой источник нарушения, каковы могут быть потенциальные потери, какие материальные и временные ресурсы могут понадобиться для ликвидации нарушения и др.

В плане описываются схема оповещения конкретных лиц, указываются руководство и ответственные лица, оговариваются вопросы взаимодействия с группами быстрого реагирования (собственная группа или внешняя), связи с общественностью (могут быть подготовлены пресс-релизы), с правоохранительными органами. Здесь же рекомендуется осветить стандартные формулировки докладов.

При выработке ответных мер определяются следующие процедуры:

- сдерживания распространения нарушения (как ограничить атакуемую область),
- ликвидации последствий,
- восстановление,
- анализ случившегося с извлечением уроков.

Очень важно, чтобы реакции на нарушения были тщательно зарегистрированы. По крайней мере, фиксируются: системные события (следует приобщить к документации регистрационный журнал системы), все действия с указанием времени, все телефонные разговоры.

7.2.2. Восстановительные работы

После нарушения следует предпринять ряд действий по восстановлению нормального функционирования АС. Этому посвящена данная часть плана. Основными положениями документа являются следующие:

1. Оперативный пересмотр политики.
2. Устранение слабостей.
3. Усвоение уроков.
4. Совершенствование политики и процедур.

Оперативный пересмотр политики начинается со следующих действий:

- переучета системных активов (как инцидент повлиял на состояние системы),
- пересмотра программы ОБИ с учетом извлекших уроков,
- производства нового анализа риска,
- проведения следствия против нарушителей.

Самым ответственным пунктом является описание процесса восстановления и устранения слабостей системы. Здесь перечисляются следующие процедуры:

- определения механизма вторжения,
- оценки нанесенного ущерба,
- определения порядка восстановительных работ,
- подведения итогов с уяснением уроков после восстановления,
- определения порядка ведения журнала безопасности.

После этого описывается порядок “разбора полетов”. Здесь рекомендуется составить отчет, в котором описывается инцидент и его ликвидация, описываются дополнительные ресурсы: дополнительные и новые методы, устройства и средства защиты информации, библиотека по ОБИ. Здесь же определяется порядок формирования группы из системных администраторов, которая станет ядром службы безопасности предприятия.

В заключении документа описывается порядок пересмотра политики ОБИ и порядок доклада об инцидентах.

7.3. Реализация планов

Планы, как известно, являются не догмой, а руководством к действию. Поэтому рассмотрим подробнее основные *процедуры обеспечения безопасности* АС. Многие из них являются обычными действиями администраторов по поддержанию нормального функционирования системы, однако так или иначе, они связаны с информационной безопасностью.

К основным процедурам обеспечения безопасности относятся:

- проверка системы и средств безопасности;
- управление паролями;
- управление счетами;
- поддержка пользователей;
- сопровождение программного обеспечения;
- конфигурационное управление;
- резервное копирование;
- управление носителями;
- документирование.

Систематические проверки безопасности — необходимое условие надежного функционирования АС. Проверки должны включать: проведение учений и регламентные работы по контролю политики и всей системы безопасности, постоянное тестирование основных процедур, программно-аппаратных механизмов и средств. Важным элементом проверки является определение достаточной степени полноты проверок и периодичности с целью получения уверенности в защищенности АС.

Управление паролями является наиболее важной процедурой обеспечения безопасности работы пользователей. По данным CERT/CC не менее 80% инцидентов в АС связаны с плохим выбором паролей. Процедуры управления паролями варьируются от эпизодических просьб по смене пароля до анализа устойчивости системы аутентификации. Для последнего используются сетевые анализаторы либо программы вскрытия паролей.

Управление счетами - рутинные действия администратора по предотвращению НСД. Администратор отвечает за заведение, контроль длительности действия и ликвидацию счетов, а также осуществляет общий контроль. Важно, чтобы пользователи сами принимали активное участие в проверке безопасности собственных систем, например, отслеживали время использования своего счета. Так же как и с паролями, администратор должен периодически контролировать легитимность использования счетов путем использования сетевых анализаторов и анализа системных журналов.

Поддержка пользователей состоит в обучении, консультировании, оказании помощи при их работе в системе, а также в контроле соблюдения ими правил безопасности и выяснении причин возникших проблем или подозрительных событий. Для обучения и консультирования могут быть определены специальные часы занятий. Для оказания помощи в работе, кроме администратора системы, может назначаться специальная группа сопровождения пользователей или группа реагирования на нарушения. Целесообразно вести учет всех вызовов пользователями. Это способствует проведению оценки и совершенствованию качества системы безопасности. Важным является выяснение причин возникших трудностей. Это позволяет оперативно выявить разного рода нарушения, в том числе неавторизованную деятельность злоумышленника.

Первая обязанность администратора - это эксплуатация и научно-техническое сопровождение вверенного ему программного обеспечения. В связи с этим, администратор должен выполнять следующие действия:

- контролировать безопасность вычислительного процесса с целью выявления компьютерных вирусов, сбоев и отказов функционирования программ и запуска неавторизованных программ и процессов;

- контролировать целостность программного обеспечения (неавторизованную модификацию) на предмет выявления программных закладок, недокументированных функций и других программных дефектов;
- обеспечивать восстановление программ с эталонных копий (возможно, с привлечением сил и средств фонда алгоритмов и программ предприятия), их обновление, замену и другие вопросы, касающиеся жизненного цикла программного обеспечения.

Процедуры конфигурационного управления. Администратор обеспечивает функциональную совместимость компонентов системы и их настройку с целью максимальной производительности и безопасности. Следует отметить, что зачастую именно ошибки в конфигурации систем являются причиной незащищенности распределенных АС. Дело в том, что конфигурирование особенно сетевых и устаревших аппаратных компонентов может быть делом очень трудным и требовать высокой квалификации технических работников. Поэтому стараются выбирать стандартные настройки подсистем. Это упрощает установку, администрирование и развитие системы, но может не соответствовать специфическим особенностям безопасности АС. Кроме того, стандартные конфигурации более уязвимы перед внешними вторжениями. Поэтому на практике нестандартное конфигурирование, как правило, используют для экранирующих систем - для исключения “стандартных” атак. Конфигурации внутренних систем, расположенных за межсетевым экраном, делают стандартными.

Резервное копирование - традиционный способ обеспечения работоспособности системы на случай порчи или утраты информационно-программного ресурса АС. При оценке возможных нарушений производится оценка возможности восстановления информации и программ и требуемые для этого ресурсы. Исходя из этого, рассчитывается периодичность и полнота создания резервных копий. Разуметься, копии должны храниться так, чтобы исключить их утрату вместе с оригиналом. Обычно их содержат в отдельных защищенных помещениях или/и специальных сейфах на случай пожара, затопления, всплеска радиации или другого стихийного бедствия и действия злоумышленника.

Управление носителями включает процедуры по их хранению, учету, выдаче, контролю правильности использования и уничтожения носителей. Сюда относится контроль и учет выдачи информации и на печатающие устройства. На некоторых предприятиях имеются ограничения на использование определенных носителей. Например, разрешается пользоваться только зарегистрированными носителями.

Вся деятельность по безопасности отягощена документированием. Система документации очень разнообразна: от идеологии фирмы и конструкторской документации до журнала выдачи магнитных носителей и учета времени работы. Основное внимание в документировании уделяется вопросам сбора, выдачи и хранения документов. Важно выделить документы, действительно важные для безопасности системы. Последнее время наметилась тенденция в реализации безбумажной технологии - создание электронных архивов документов администратора безопасности. Однако здесь следует знать, что такие документы пока в России юридической силы не имеют.

8. МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В предыдущих разделах по практические мероприятиям построения интегрированной системы информационной безопасности предприятия мы рассмотрели административный уровень и уровень планирования системы ОБИ — политику и практические процедуры. После них следует самый ответственный момент — выработка программно-технические мер.

Последние заключаются в выборе механизмов (подсистем) и средств ОБИ (см. табл. 8.1). В данном разделе мы подробно рассмотрим основные механизмы и обозначим некоторые средства их реализации.

Таблица 8.1.

Основные механизмы и средства интегрированной системы информационной безопасности предприятия

Основные механизмы	Основные средства
• идентификация и аутентификация • разграничение доступа • регистрация и аудит • криптография • экранирование	• средства контроля доступа • средства шифрования информации • средства антивирусной защиты • средства межсетевого экранирования • средства гарантированного хранения • средства защиты от сбоев электропитания и защиты кабельной системы • инструментальные средства администратора безопасности

8.1. Идентификация и аутентификация

Основой любых систем ОБИ являются идентификация и аутентификация, так как все механизмы защиты информации рассчитаны на работу с поименованными субъектами и объектами АС. Напомним, что в качестве субъектов АС могут выступать как пользователи, так и процессы, а в качестве объектов АС — информация и другие информационные ресурсы системы.

Присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным перечнем называется *идентификацией.* Идентификация обеспечивает выполнение следующих функций ОБИ:

- установление подлинности и определение полномочий субъекта при его допуске в систему,
- контролирование установленных полномочий в процессе сеанса работы;
- регистрация действий и др.

Аутентификацией (*установлением подлинности)* называется проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности. Другими словами, аутентификация заключается в проверке: является ли подключающийся субъект тем, за кого он себя выдает.

Общая процедура идентификации и аутентификации пользователя при его доступе в АС представлена на рис. 8.1. Если в процессе аутентификации подлинность субъекта установлена, то система защиты информации должна определить его полномочия (совокупность прав). Это необходимо для последующего контроля и разграничения доступа к ресурсам.

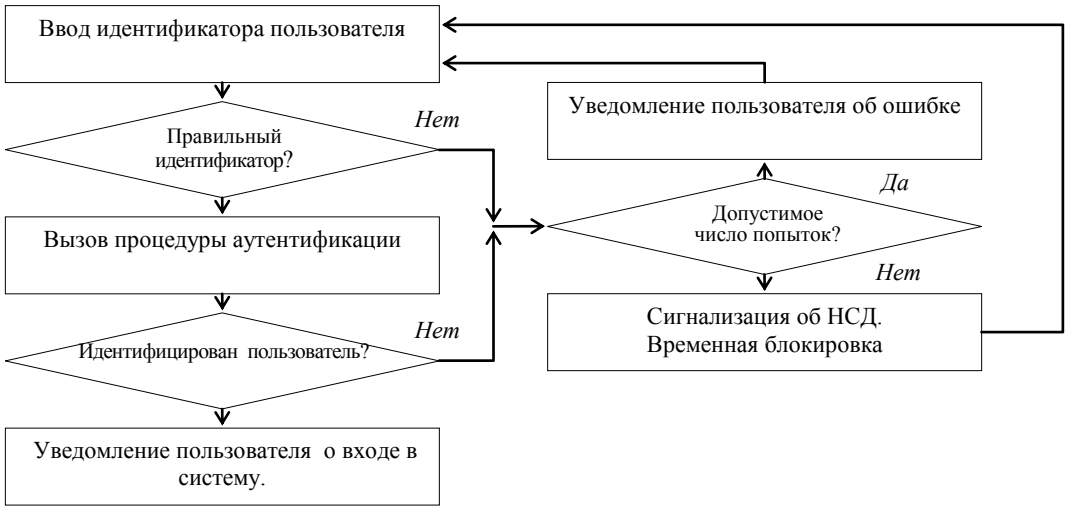

Рис. 8.1. Классическая процедура идентификации и аутентификации

По контролируемому компоненту системы способы аутентификации можно разделить на аутентификацию партнеров по общению и аутентификацию источника данных. Аутентификация партнеров по общению используется при установлении (и периодической проверке) соединения во время сеанса. Она служит для предотвращения таких угроз, как маскарад и повтор предыдущего сеанса связи. Аутентификация источника данных — это подтверждение подлинности источника отдельной порции данных.

По направленности аутентификация может быть односторонней (пользователь доказывает свою подлинность системе, например при входе в систему) и двусторонней (взаимной).

Обычно методы аутентификации классифицируют по используемым средствам. В этом случае указанные методы делят на четыре группы:

1. Основанные на знании лицом, имеющим право на доступ к ресурсам системы, некоторой секретной информации — пароля.
2. Основанные на использовании уникального предмета: жетона, электронной карточки и др.
3. Основанные на измерении биометрических параметров человека — физиологических или поведенческих атрибутах живого организма.
4. Основанные на информации, ассоциированной с пользователем, например с его координатами.

Рассмотрим эти группы.

1. Наиболее распространенными простыми и привычными являются методы аутентификации, основанные на *паролях* — секретных идентификаторах субъектов. Здесь при вводе субъектом своего пароля подсистема аутентификации сравнивает его с паролем, хранящимся в базе эталонных данных в зашифрованном виде. В случае совпадения паролей подсистема аутентификации разрешает доступ к ресурсам АС.

Парольные методы следует классифицировать по степени изменяемости паролей:

- методы, использующие постоянные (многократно используемые) пароли,
- методы, использующие одноразовые (динамично изменяющиеся) пароли.

В большинстве АС используются многоразовые пароли. В этом случае пароль пользователя не изменяется от сеанса к сеансу в течение установленного администратором системы времени его действительности. Это упрощает процедуры администрирования, но повышает угрозу рассекречивания пароля. Известны множество способов вскрытия пароля: от подсмотра через плечо до перехвата сеанса связи. Вероятность вскрытия злоумышленником пароля повышается, если пароль несет смысловую нагрузку (год рождения, имя девушки), небольшой длины, набран на одном регистре, не имеет ограничений на период существования и т.д. Важно, разрешено ли вводить пароль только в диалоговом режиме или есть возможность обращаться из программы. В последнем случае, возможно запустить программу по подбору паролей - “дробилку”.

Более надежный способ — использование одноразовых или динамически меняющихся паролей.

Известны следующие методы парольной защиты, основанные на одноразовых паролях:

- методы модификации схемы простых паролей;
- методы “запрос-ответ”;
- функциональные методы.

В первом случае пользователю выдается список паролей. При аутентификации система запрашивает у пользователя пароль, номер в списке которого определен по случайному закону. Длина и порядковый номер начального символа пароля тоже могут задаваться случайным образом.

При использовании метода “запрос-ответ” система задает пользователю некоторые вопросы общего характера, правильные ответы на которые известны только конкретному пользователю.

Функциональные методы основаны на использовании специальной функции парольного преобразования ***f(x)***. Это позволяет обеспечить возможность изменения (по некоторой формуле) паролей пользователя во времени. Указанная функция должна удовлетворять следующим требованиям:

- для заданного пароля *x* легко вычислить новый пароль ***y = f(x)***;
- зная ***x*** и ***y***, сложно или невозможно определить функцию ***f(x)***.

Наиболее известными примерами функциональных методов являются: метод функционального преобразования и метод “рукопожатия”.

Идея метода функционального преобразования состоит в периодическом изменении самой функции ***f(x)***. Последнее достигается наличием в функциональном выражении динамически меняющихся параметров, например функции от некоторой даты и времени. Пользователю сообщается исходный пароль, собственно функция и периодичность смены пароля. Нетрудно видеть, что паролями пользователя на заданных ***n***-периодах времени будут следующие: ***x, f(x), f(f(x)), ... $f(x)^{n-1}$***.

Метод “рукопожатия” состоит в следующем. Функция парольного преобразования известна только пользователю и системе защиты. При входе в АС подсистема аутентификации генерирует случайную последовательность ***x***, которая передается пользователю. Пользователь вычисляет результат функции ***y=f(x)*** и возвращает его в систему. Система сравнивает собственный вычисленный результат с полученным от пользователя. При совпадении указанных результатов подлинность пользователя считается доказанной.

Достоинством метода является то, что передача какой-либо информации, которой может воспользоваться злоумышленник, здесь сведена к минимуму.

В ряде случаев пользователю может оказаться необходимым проверить подлинность другого удаленного пользователя или некоторой АС, к которой он собирается осуществить доступ. Наиболее подходящим здесь является метод “рукопожатия”, так как никто из участников информационного обмена не получит никакой конфиденциальной информации.

Отметим, что методы аутентификации, основанные на одноразовых паролях, также не обеспечивают абсолютной защиты. Например, если злоумышленник имеет возможность подключения к сети и перехватывать передаваемые пакеты, то он может посылать последние как собственные.

2. В последнее время получили распространение комбинированные методы идентификации, требующие, помимо знания пароля, наличие карточки (token) — специального устройства, подтверждающего подлинность субъекта.

Карточки разделяют на два типа:

- пассивные (карточки с памятью);
- активные (интеллектуальные карточки).

Самыми распространенными являются пассивные карточки с магнитной полосой, которые считываются специальным устройством, имеющим клавиатуру и процессор. При использовании указанной карточки пользователь вводит свой идентификационный номер. В случае его совпадения с электронным вариантом, закодированным в карточке, пользователь получает доступ в систему. Это позволяет достоверно установить лицо, получившее доступ к системе и исключить несанкционированное использование карточки злоумышленником (например, при ее утере). Такой способ часто называют двукомпонентной аутентификацией.

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

К достоинству использования карточек относят то, что обработка аутентификационной информации выполняется устройством чтения, без передачи в память компьютера. Это исключает возможность электронного перехвата по каналам связи.

Недостатки пассивных карточек следующие: они существенно дороже паролей (см. рис. 9.2), требуют специальные устройства чтения, их использование подразумевает специ-

альные процедуры безопасного учета и распределения. Их также необходимо оберегать от злоумышленников, в первую очередь, естественно, не оставлять в устройствах. Известны случаи подделки пассивных карточек.

Интеллектуальные карточки кроме памяти имеют собственный микропроцессор. Это позволяет реализовать различные варианты парольных методов защиты, как-то: многоразовые пароли, динамически меняющиеся пароли, обычно запрос-ответные методы. Все карточки обеспечивают двухкомпонентную аутентификацию.

К указанным достоинствам интеллектуальных карточек следует добавить их многофункциональность. Их можно применять не только для целей безопасности, но и, например, для финансовых операций. Сопутствующим недостатком карточек является их высокая стоимость.

Перспективным направлением развития карточек является наделение их стандартом расширения портативных систем PCMCIA (PC Card). Такие карточки являются портативными устройствами типа PC Card, которые вставляются в разъем PC Card и не требуют специальных устройств чтения. В настоящее время они достаточно дороги.

3. Методы аутентификации, основанные на измерении биометрических параметров человека, обеспечивают почти 100%-ую идентификацию, решая проблемы утери или утраты паролей и личных идентификаторов. Однако методы нельзя использовать при идентификации процессов или данных (объектов данных), они только начинают развиваться (имеются проблемы со стандартизацией и распространением), требуют пока сложного и дорогостоящего оборудования. Это обусловливает их использование пока только на особо важных объектах и системах, главным образом в МО РФ.

Примерами внедрения указанных методов являются системы идентификации пользователя по рисунку радужной оболочки глаза, отпечаткам ладони, формам ушей, инфракрасной картине капиллярных сосудов, по почерку, по запаху, по тембру голоса и даже по ДНК (см. табл. 8.2).

Таблица 8.2.

Примеры методов биометрии

Физиологические методы	**Поведенческие методы**
• Снятие отпечатков пальцев • Сканирование радужной оболочки глаза • Сканирование сетчатки глаза • Геометрия кисти руки • Распознавание черт лица	• Анализ подписи • Анализ тембра голоса • Анализ клавиатурного почерка

Новым направлением является использование биометрических характеристик в интеллектуальных расчетных карточках, жетонах-пропусках и элементах сотовой связи. Например, при расчете в магазине предъявитель карточки кладет палец на сканер в подтверждение, что карточка действительно его.

Назовем наиболее используемые биометрические атрибуты и соответствующие системы.

A. Отпечатки пальцев. Такие сканеры имеют небольшой размер, универсальны, относительно недороги. Биологическая повторяемость отпечатка пальца составляет 10^{-5}%. В настоящее время пропагандируются правоохранительными органами из-за крупных ассигнований в электронные архивы отпечатков пальцев.
B. Геометрия руки. Соответствующие устройства используются, когда из-за грязи или травм трудно применять сканеры пальцев. Биологическая повторяемость геометрии руки около 2-х %.
C. Радужная оболочка глаза. Данные устройства обладают наивысшей точностью. Теоретическая вероятность совпадения двух радужных оболочек составляет 1 из 10^{78}.
D. Термический образ лица. Системы позволяют идентифицировать человека на расстоянии до десятков метров. В комбинации с поиском данных по базе данных такие системы используются для опознания авторизованных сотрудников и отсеивания посторонних. Однако при изменении освещенности сканеры лица имеют относительно высокий процент ошибок.
E. Голос. Проверка голоса удобна для использования в телекоммуникационных приложениях. Необходимые для этого 16-разрядная звуковая плата и конденсаторный микрофон стоят менее 25 $. Вероятность ошибки составляет 2-5%. Данная технология подходит для верификации по голосу по телефонным каналам связи, она более надежна по сравнению с частотным набором личного номера. Сейчас развиваются направления идентификации личности и его состояния по голосу — возбужден, болен, говорит правду, не в себе и т.д.
F. Ввод с клавиатуры. Здесь при вводе, например, пароля отслеживаются скорость и интервалы между нажатиями.
G. Подпись. Для контроля рукописной подписи используются дигитайзеры.

4. Новейшим направлением аутентификации является доказательство подлинности удаленного пользователя по его местонахождению. Данный защитный механизм основан на использовании системы космической навигации, типа GPS (Global Positioning System) [82]. Пользователь, имеющий аппаратуру GPS, многократно посылает координаты заданных спутников, находящихся в зоне прямой видимости. Подсистема аутентификации, зная орбиты спутников, может с точностью до метра определить месторасположение пользователя. Высокая надежность аутентификации определяется тем, что орбиты спутников подвержены колебаниям, предсказать которые достаточно трудно. Кроме того, координаты постоянно меняются, что сводит на нет их перехват. В данном случае, есть мнение, что изящная территориально-распределенная атака на компьютерные системы под силу лишь программистам Ракетно-Космических Сил.

Аппаратура GPS проста и надежна в использовании и сравнительно недорога. Это позволяет ее использовать в случаях, когда авторизованный удаленный пользователь должен находиться в нужном месте.

Суммируя возможности средств аутентификации, ее можно классифицировать по уровню информационной безопасности на три категории:

1. Статическая аутентификация;
2. Устойчивая аутентификация;
3. Постоянная аутентификация.

Первая категория обеспечивает защиту только от НСД в системах, где нарушитель не может во время сеанса работы прочитать аутентификационную информацию. Примером средства статической аутентификации являются традиционные постоянные пароли. Их эф-

фективность преимущественно зависит от сложности угадывания паролей и, собственно, от того, насколько хорошо они защищены.

Для компрометации статической аутентификации нарушитель может подсмотреть, подобрать, угадать или перехватить аутентификационные данные и т.д.

Устойчивая аутентификация использует динамические данные аутентификации, меняющиеся с каждым сеансом работы. Реализациями устойчивой аутентификации являются системы, использующие одноразовые пароли и электронные подписи. Усиленная аутентификация обеспечивает защиту от атак, где злоумышленник может перехватить аутентификационную информацию и силиться использовать ее в следующих сеансах работы.

Однако устойчивая аутентификация не обеспечивает защиту от активных атак, в ходе которых маскирующийся злоумышленник может оперативно (в течение сеанса аутентификации) перехватить, модифицировать и вставить информацию в поток передаваемых данных.

Постоянная аутентификация обеспечивает идентификацию каждого блока передаваемых данных, что предохраняет их от несанкционированной модификации или вставки. Примером реализации указанной категории аутентификации является использование алгоритмов генерации электронных подписей для каждого бита пересылаемой информации.

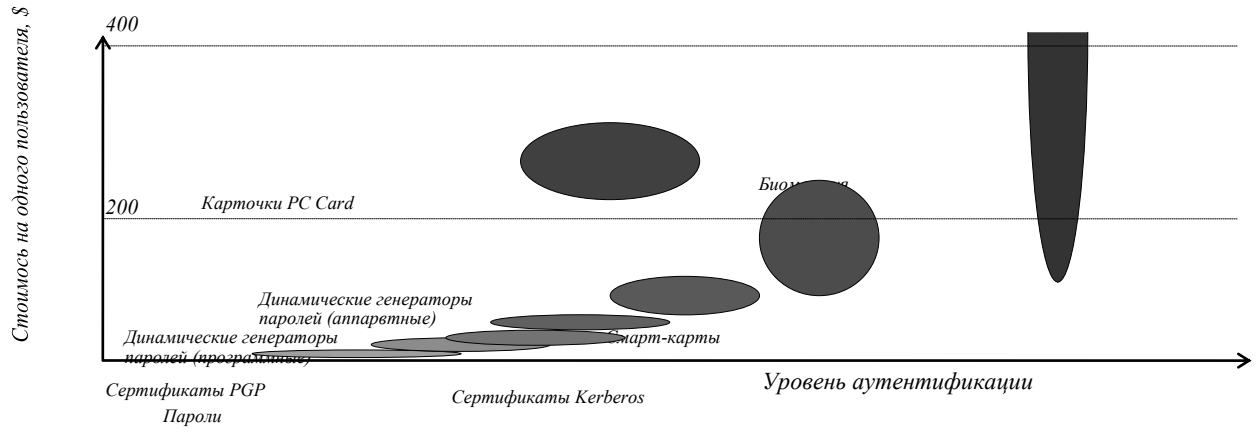

Рис. 8.2. Стоимость и уровень технологий аутентификации

8.2. Разграничение доступа

После выполнения идентификации и аутентификации необходимо установить полномочия (совокупность прав) субъекта для последующего контроля санкционированного использования вычислительных ресурсов, доступных в АС. Такой процесс называется *разграничением (логическим управлением) доступа*.

Обычно полномочия субъекта представляются: списком ресурсов, доступным пользователю, и правами по доступу к каждому ресурсу из списка. В качестве вычислительных

ресурсов могут быть программы, информация, логические устройства, объем памяти, время процессора, приоритет и т.д.

Можно выделить следующие методы разграничения доступа [33]:

- разграничение доступа по спискам,
- использование матрицы установления полномочий,
- разграничения доступа по уровням секретности и категориям,
- парольное разграничение доступа.

1. При разграничении доступа по спискам задаются соответствия:

- каждому пользователю — список ресурсов и прав доступа к ним или
- каждому ресурсу — список пользователей и их прав доступа к данному ресурсу.

Списки позволяют установить права с точностью до пользователя. Здесь нетрудно добавить права или явным образом запретить доступ. Списки используются в большинстве ОС и СУБД.

2. Использование матрицы установления полномочий подразумевает применение матрицы доступа (таблицы полномочий). В указанной матрице строками являются идентификаторы субъектов, имеющих доступ в АС, а столбцами — объекты (информационные ресурсы) АС. Каждый элемент матрицы может содержать имя и размер предоставляемого ресурса, право доступа (чтение, запись и др.), ссылку на другую информационную структуру, уточняющую права доступа, ссылку на программу, управляющую правами доступа и др.

Данный метод предоставляет более унифицированный и удобный подход, т.к. вся информация о полномочиях хранится в виде единой таблицы, а не в виде разнотипных списков. Недостатками матрицы являются ее возможная громоздкость и неоптимальность (большинство клеток - пустые).

Таблица 8.3.

Фрагмент матрицы установления полномочий

Субъект	**Каталог d:\Heap**	**Программа prty**	**Принтер**
Пользователь 1	cdrw	e	w
Пользователь 2	r		w с 9:00 до 17:00

c - создание, d - удаление, r - чтение, w - запись, e - выполнение.

3. Разграничения доступа по уровням секретности и категориям состоят в том, что ресурсы АС разделяются в соответствии с уровнями секретности или категорий.

При разграничении по уровню секретности выделяют несколько уровней, например: общий доступ, конфиденциально, секретно, совершенно секретно. Полномочия каждого пользователя задаются в соответствии с максимальным уровнем секретности, к которому он допущен. Пользователь имеет доступ ко всем данным, имеющим уровень (гриф) секретности не выше, чем он имеет.

При разграничении по категориям задается и контролируется ранг категории, соответствующей пользователю. Соответственно, все ресурсы АС декомпозируют по уровню важности, причем определенному уровню соответствует некоторый ранг персонала (типа: руководитель, администратор, пользователь).

4. Парольное разграничение, очевидно, представляет использование методов доступа субъектов к объектам по паролю. При этом используются все методы парольной защиты. Очевидно, что постоянное использование паролей создает неудобства пользователям и временные задержки. Поэтому указанные методы используют в исключительных ситуациях.

На практике обычно сочетают различные методы разграничения доступа. Например, первые три метода усиливают парольной защитой.

В завершении подраздела заметим, что в ГОСТ Р 50739-95 **"Средства вычислительной техники. Защита от несанкционированного доступа к информации"** и в документах Гостехкомиссии [53, 54] определены два вида (принципа) разграничения доступа:

- дискретное управление доступом,
- мандатное управление доступом.

Дискретное управление доступом (discretionary access control) представляет собой разграничение доступа между поименованными субъектами и поименованными объектами. Субъект с определенным правом доступа может передать это право любому другому субъекту. Данный вид организуется на базе методов разграничения по спискам или с помощью матрицы.

Мандатное управление доступом (mandatory access control) — разграничение доступа субъектов к объектам, основанное на характеризуемой меткой конфиденциальности информации, содержащейся в объектах, и официальном разрешении (допуске) субъектов обращаться к информации такого уровня конфиденциальности. Иначе, для реализации мандатного управления доступом каждому субъекту и каждому объекту присваивают классификационные метки, отражающие их место в соответствующей иерархии. С помощью этих меток субъектам и объектам должны быть назначены классификационные уровни, являющиеся комбинациями уровня иерархической классификации и иерархических категорий. Данные метки должны служить основой мандатного принципа разграничения доступа. Ясно, что методы разграничения доступа по уровням секретности и категориям являются примерами мандатного управления доступом.

8.3. Регистрация и аудит

Регистрация представляет собой механизм подотчетности системы ОБИ, фиксирующий все события, касающиеся безопасности, такие как: вход и выход субъектов доступа, запуск и завершение программ, выдача печатных документов, попытки доступа к защищаемым ресурсам, изменение полномочий субъектов доступа и статуса объектов доступа и т.д. Для сертифицируемых по безопасности АС список контролируемых событий определен рабочим документом Гостехкомиссии РФ [51]. Эффективность системы ОБИ принципиально повышается в случае дополнения регистрации аудитом — анализом протоколируемой информации. Это позволяет оперативно выявлять нарушения, определять слабые места в системе защите, анализировать закономерности системы, оценивать работу пользователей и т.д.

Реализация механизма регистрации и аудита преследует следующие цели [15]:

- обеспечение подотчетности пользователей и администраторов;
- обеспечение возможности реконструкции последовательности событий;
- обнаружение попыток нарушений информационной безопасности;

- предоставление информации для выявления и анализа проблем.

Кроме того, механизм регистрации и аудита является психологическим средством, напоминающим потенциальным нарушителям о неотвратимости возмездия за проступки и оплошности.

Практическими средствами регистрации и аудита могут быть следующие:
- различные системные утилиты и прикладные программы,
- регистрационный (системный или контрольный) журнал (audit trail).

Первое средство является обычно дополнением к мониторингу, осуществляемого администратором системы. Комплексный подход к протоколированию и аудиту обеспечивается при использовании регистрационного журнала.

Регистрационный журнал — это хронологически упорядоченная совокупность записей результатов деятельности субъектов системы, достаточная для восстановления, просмотра и анализа последовательности действий, окружающих или приводящих к выполнению операций, процедур или совершению событий при транзакции с целью контроля конечного результата. Типовая запись регистрационного журнала представлена на рисунке 8.3.

Тип записи	*Дата*	*Время*	*Терминал*	*Пользователь*	*Событие*	*Результат*

Рис. 8.3. Типовая запись регистрационного журнала

Место и модель подсистемы регистрации в рамках сетевого фильтра системы проиллюстрированы на рисунке 8.4.

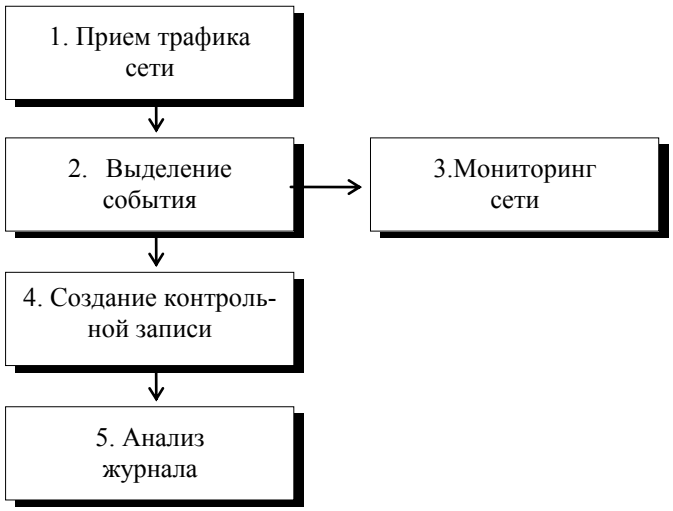

Рис. 8.4. Схема сетевого фильтра

Процесс ведения регистрационного журнала состоит из четырех этапов:
1. Сбор и хранение;
2. Защита;

3. Интеграция;
4. Анализ.

На первом этапе определяются данные, подлежащие сбору и хранению, период чистки и архивации журнала, степень централизации управления, место и средства хранения журнала, возможность регистрации шифрованной информации и др.

Регистрируемые данные должны быть защищены, в первую очередь от несанкционированной модификации и, возможно, раскрытия. Дополнительные требования по безопасности определяются концентрацией информации обо всей АС, множеством сегментов АС с различными уровнями доступа, разницей зон административной ответственности и др.

Этап интеграции необходим для объединения и согласования форматов регистрируемых данных из различных систем. Некоторые системы не имеют механизмов контроля и регистрации данных. Возможно, здесь придется разработать программы дополнительного контроля данных и программы трансформации данных в единый формат.

Самым важным этапом является анализ регистрационной информации. Известны несколько методов анализа информации с целью выявления НСД.

А. Статистические методы. Здесь накапливается среднестатистические параметры функционирования подсистем (исторический профиль трафика) и сравниваются с текущими. Наличие определенных отклонений может сигнализировать о возможности появления некоторых угроз. Например, так выявляются: сбои в работе сервера из-за лавинного потока запросов (queue storm), быстро распространяемый компьютерный вирус, нарушитель, маскирующиеся под легального пользователя, но ведущий себя иначе (“маскарад”) и др.

В. Эвристические методы. В данном случае в логических правилах системы поддержки принятия решений закодированы известные сценарии НСД, характеристики наблюдаемой системы, сигнализирующие о нарушениях, или модели действий, по совокупности приводящие к НСД. Понятно, что данные методы идентифицируют только известные угрозы, определенные в базе знаний системы поддержки принятия решений.

8.4. Криптография

Самым надежным техническим методом ОБИ является криптография, обеспечивающая шифрование и расшифровывание конфиденциальных данных. Криптография также используется для подтверждения подлинности источника данных и контроля целостности данных. Заметим, что криптография всегда являлась обязательным элементом безопасных АС. Однако особое значение криптографические методы получили с развитием распределенных открытых сетей, в которых нельзя обеспечить физическую защиту каналов связи.

Классические криптографические методы разделяют на два основных типа:

- *симметричные*;
- *асимметричные*.

В симметричных методах для шифрования и расшифровывания используется один и тот же секретный ключ.

Наиболее известным стандартом на симметричное шифрование с закрытым ключом является стандарт для обработки информации в государственных учреждениях США DES (Data Encryption Standard). Алгоритм DES использует ключ длиной 56 бит, что требует от

злоумышленника перебора 72 квадриллионов возможных ключевых комбинаций. Более криптостойкая (но втрое менее быстродействующая) версия алгоритма DES — Triple DES позволяет задать ключ длиной 112 бит.

Другим популярным алгоритмом шифрования является IDEA (International Data Encryption Algorithm), отличающийся применением ключа длиной 128 бит. Он считается более стойким, чем DES.

Отечественный подобный стандарт шифрования данных — ГОСТ 28147-89 “Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования” определяет алгоритм симметричного шифрования с ключом длиной до 256 бит.

Общая технология использования симметричного метода шифрования представлена на рис. 8.5.

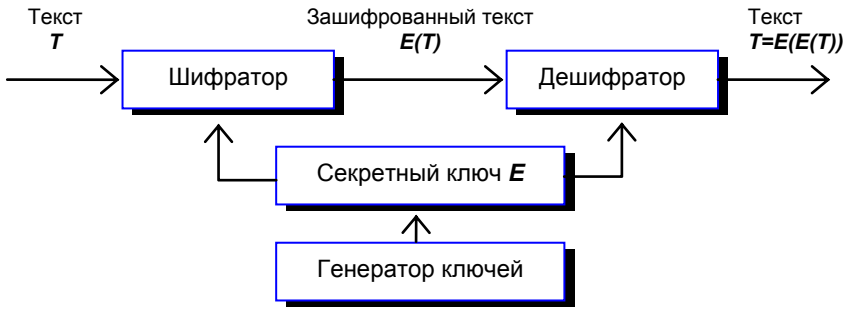

Рис. 8.5. Использование симметричного метода шифрования с закрытым ключом

К достоинствам симметричных методов относят высокое быстродействие и простоту.

Основным недостатком указанных методов является то, что ключ должен быть известен и отправителю, и получателю. Это существенно усложняет процедуру назначения и распределения ключей между пользователями. По существу, в открытых сетях должен быть предусмотрен физически защищенный канал передачи ключей.

Названный недостаток послужил причиной разработки методов шифрования с открытым ключом —асимметричных методов.

2. Асимметричные методы используют два взаимосвязанных ключа: для шифрования и расшифрования. Один ключ является закрытым и известным только получателю. Его используют для расшифрования. Второй из ключей является открытым, т.е. он может быть общедоступным по сети и опубликован вместе с адресом пользователя. Его используют для выполнения шифрования.

Формально асимметричный метод можно описать следующим образом. Обозначим результат шифрования текста ***T*** с помощью открытого ключа — ***E(T)***, а результат расшифровки текста с помощью закрытого ключа — ***D(T)***. Тогда асимметричный метод должен отвечать следующим трем требованиям:

1). D(E(T)) = T;
2). ***D*** практически невозможно определить по ***E***;

3). ***E*** нельзя взломать.

Преимущество указанного метода состоит в уменьшении количества ключей, с которыми приходится оперировать. Однако данный алгоритм имеет существенный недостаток — требует значительной вычислительной мощности. Использование асимметричного метода шифрования представлено на рисунке 8.6.

В настоящее время наиболее известными и надежными являются следующие асимметричные алгоритмы:

- RSA (Rivest, Shamir, Adleman),
- Эль Гамаля.

Алгоритм RSA принят в качестве следующих международных стандартов: ISO/IEC/DIS 9594-8 и X.509. Алгоритм использует факт, что нахождение больших (например, 100-битных) простых чисел в вычислительном отношении осуществляется легко, однако разложение на множители произведения двух таких чисел в вычислительном отношении представляется невыполнимым.

Другим известным методом является алгоритм Эль Гамаля, положенный в основу стандарта NIST[1] — MD 20899. Алгоритм основан на возведении в степень по модулю большого простого числа.

Следует сказать, что, если алгоритмы типа DES определяют длину данных и ключа в битах, то асимметричные алгоритмы могут быть реализованы при любой длине ключа. Чем ключ длиннее, тем выше криптостойкость системы, но больше время шифрования и расшифровывания.

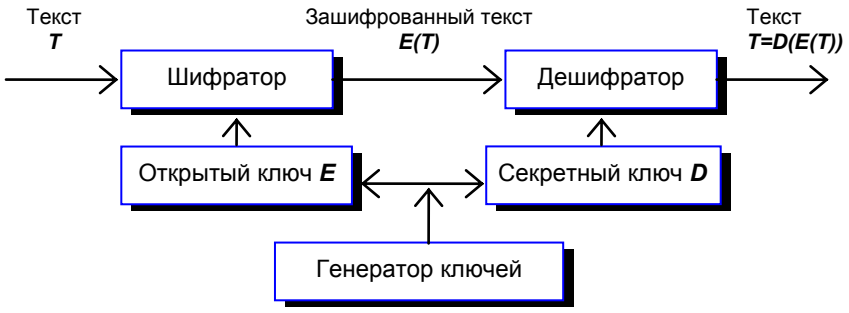

Рис. 8.6. Использование метода шифрования с открытым ключом

Как отмечалось, основным недостатком асимметричных алгоритмов является их низкое быстродействие: данные алгоритмы в несколько тысяч раз медленнее симметричных алгоритмов! Поэтому для исключения данного недостатка используют технологии сочетания симметричных и асимметричных методов шифрования. В частности, текст шифруется быстродействующим симметричным алгоритмом, а секретный (случайный) ключ, сопровождающий текст, — асимметричным алгоритмом.

Важным преимуществом асимметричных методов является возможность идентификации отправителя путем использования его *электронной подписи*. Идея технологии элек-

[1] Национальный институт стандартов и технологий США (бывший ANSI).

тронной подписи состоит в следующем. Отправитель передает два экземпляра одного сообщения: открытое и расшифрованное его закрытым ключом (т.е. обратно шифрованное). Получатель шифрует с помощью открытого ключа отправителя расшифрованный экземпляр. Если он совпадет с открытым вариантом, то личность и подпись отправителя считается установленной.

Формально выражаясь, асимметричный метод обеспечивает реализацию электронной подписи при выполнении следующего тождества:

$$E(D(T)) = D(E(T)) = T.$$

При практической реализации электронной подписи также шифруется не все сообщение, а лишь специальная контрольная сумма - хэш (hash total), защищающая послание от нелегального изменения. Важно, что электронная подпись здесь гарантирует как целостность сообщения, так и удостоверяет личность отправителя.

Вопросы реализации электронной подписи и вычисления ее хэша определены в отечественных стандартах “Информационная технология. Криптографическая защита информации”, а именно: ГОСТ Р 34.10-94 **“Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма”** и ГОСТ 34.11-94 **“Функция хэширования”**.

В заключении раздела отметим, что криптографические методы используются также для контроля целостности информации и программ. Для этого применяется шифрованная контрольная сумма исходного текста (имитоприставка), вычисленная с применением секретного ключа. В отличии от традиционной контрольной суммы (используемой для защиты от программно-аппаратных сбоев и ошибок), имитоприставка обеспечивает практически абсолютную защиту как от непреднамеренной, так и преднамеренной модификации данных или программы.

8.5. Экранирование

Механизмом обеспечения целостности данных в информационно-вычислительных сетях является *экранирование*, выполняющее функции разграничения информационных потоков на границе защищаемой сети. С одной стороны, это повышает безопасность объектов внутренней сети за счет игнорирования неавторизованных запросов из внешней среды. Указанное уменьшает уязвимость внутренних объектов потому, что сторонний нарушитель должен преодолеть некоторый защитный барьер — межсетевой экран, в котором механизмы ОБИ сконфигурированы особо тщательно и жестко. С другой стороны, экранирование позволяет контролировать информационные потоки, исходящие во внешнюю среду, что повышает режим конфиденциальности АС. Кроме функций разграничения доступа, экранирование обеспечивает регистрацию информационных обменов.

Функции экранирования выполняет межсетевой экран или брандмауэр (firewall), под которым понимают программную или программно-аппаратную систему, ко

торая выполняет контроль информационных потоков, поступающих в АС и/или выходящих из АС, и обеспечивает защиту АС посредством фильтрации информации. Фильтрация информации состоит в анализе информации по совокупности критериев и принятии решения о ее распространении в/из АС [30].

В общем случае межсетевой экран выполняет свои функции, контролируя все информационные потоки между двумя сегментами сети или сетями (рис. 8.7).

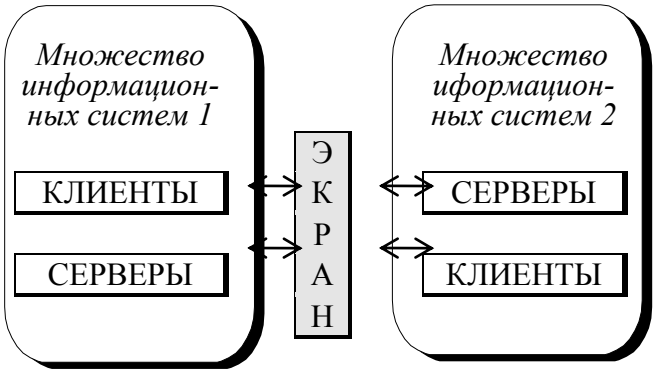

Рис. 8.7. Экран как средство разграничения доступа

Межсетевые экраны классифицируют следующим образом:

- на внешние и внутренние, обеспечивающие защиту соответственно от внешней сети или защиту между сегментами сети,
- по уровню фильтрации, соответствующему эталонной модели OSI ISO.

Говоря о внешних и внутренних сетевых экранах, следует отметить следующее. Внешние обычно имеют дело только с протоколом TCP/IP метасети Интернет. Для внутренних сетевых экранов может иметь место многопротокольность. Например, при использовании сетевой ОС Novell Netware, следует принимать во внимание протокол SPX/IPX.

Работа всех межсетевых экранов основана на использовании информации разных уровней модели OSI (см. табл. 8.4). Как правило, чем выше уровень модели OSI, на котором межсетевой экран фильтрует пакеты, тем выше обеспечиваемый им уровень защиты. Межсетевые экраны разделяют на четыре типа:

- межсетевые экраны с фильтрацией пакетов;
- шлюзы сеансового уровня;
- шлюзы прикладного уровня;
- межсетевые экраны экспертного уровня.

Таблица 8.4.

Типы межсетевых экранов и уровни модели ISO OSI

№	Уровень модели OSI	Протоколы Интернет	Тип межсетевого экрана
	Прикладной	Telnet, FTP, DNS, NFS, PING, SMTP, HTTP	•Шлюз прикладного уровня •Межсетевой экран экспертного уровня
	Представления данных		•
	Сеансовый	TCP, UDP	•Шлюз сеансового уровня
	Транспортный	TCP, UDP	
	Сетевой	IP, ICMP	•Межсетевой экран с фильтрацией пакетов
	Канальный		
	Физический		

1. Межсетевые экраны с фильтрацией пакетов (packet-filtering firewall) представляют собой маршрутизаторы или работающие на сервере программы, сконфигурированные таким образом, чтобы фильтровать входящие и исходящие пакеты. Поэтому такие экраны называют иногда пакетными фильтрами. Фильтрация осуществляется путем анализа IP-адреса источника и приемника, а также портов входящих TCP- и UDP-пакетов и сравнением их с сконфигурированной таблицей правил.

Данные системы просты в использовании, дешевы, оказывают минимальное влияние на производительность АС. Основным недостатком является их уязвимость для IP-спуфинга - замены адресов IP. Кроме того, они сложны при конфигурировании: для их установки требуется знание сетевых, транспортных и прикладных протоколов.

2. Шлюзы сеансового уровня (circuit-level gateway) контролируют допустимость *сеанса* связи. Они следят за подтверждением (квитированием) связи между авторизованным клиентом и внешним хостом (и наоборот), определяя, является ли запрашиваемый сеанс связи допустимым. При фильтрации пакетов шлюз сеансового уровня основывается на информации, содержащейся в заголовках пакетов сеансового уровня протокола TCP, т. е. функционирует на два уровня выше, чем межсетевой экран с фильтрацией пакетов. Кроме того, указанные системы обычно имеют функции трансляции сетевых адресов, которая скрывает внутренние IP-адреса, т.е. исключают IP-спуфинг. Однако, т.к. системы контролируют пакеты только на сеансовом уровне, то и отсутствует контроль содержимого пакетов, генерируемых различными службами. Для исключения указанного недостатка применяются шлюзы прикладного уровня.

3. Шлюзы прикладного уровня (application-level gateway) проверяют содержимое каждого проходящего через шлюз пакета и могут фильтровать отдельные виды команд или информации в протоколах прикладного уровня, которые им поручено обслуживать. Это более совершенный и надежный тип брандмауэра, использующий программы-посредники (proxies) прикладного уровня или агенты. Агенты составляются для конкретных служб Internet (HTTP, FTP, telnet и т.д.) и служат для проверки сетевых пакетов на наличие достоверных данных. Однако шлюзы прикладного уровня снижают уровень производительности

системы из-за повторной обработки в программе-посреднике. Это незаметно при работе в Internet из-за узости каналов связи, но существенно при работе во внутренней сети - intranet. К недостаткам можно добавить необходимость (а значит и дополнительные временные и экономические затраты) в разработке новых программ-посредников при внедрении новой службы Internet.

4. Межсетевые экраны экспертного уровня (stateful inspection firewall) сочетают в себе элементы всех трех описанных выше категорий. Как и межсетевые экраны с фильтрацией пакетов, они работают на сетевом уровне модели OSI, фильтруя входящие и исходящие пакеты на основе проверки IP-адресов и номеров портов. Межсетевые экраны экспертного уровня также выполняют функции шлюза сеансового уровня, определяя, относятся ли пакеты к соответствующему сеансу. И наконец, брандмауэры экспертного уровня берут на себя функции шлюза прикладного уровня, оценивая содержимое каждого пакета в соответствии с политикой безопасности, выработанной в конкретной организации.

Специфика указанных межсетевых экранов состоит в том, что для обеспечения защиты они перехватывают и анализируют каждый пакет на прикладном уровне модели OSI. Вместо применения связанных с приложениями программ-посредников, брандмауэры экспертного уровня используют *специальные алгоритмы распознавания и обработки данных* на уровне приложений. С помощью этих алгоритмов пакеты сравниваются с известными шаблонами данных, что, теоретически, должно обеспечить более эффективную фильтрацию пакетов.

Поскольку брандмауэры экспертного уровня допускают прямое соединение между авторизованным клиентом и внешним хостом, то они оказывают меньшее влияние на производительность, чем шлюзы прикладного уровня. Спорным остаются вопрос: обеспечивают они меньшую безопасность АС по сравнению со шлюзами прикладного уровня или нет.

9. АНТИВИРУСНЫЕ СРЕДСТВА

9.1. Уровни и методы антивирусной защиты

Известно, что нельзя добиться 100 %-ой защиты ПК от компьютерных вирусов отдельными программными средствами. Поэтому для уменьшения потенциальной опасности внедрения компьютерных вирусов и их распространения по корпоративной сети необходим комплексный подход, сочетающий различные административные меры, программно-технические средства антивирусной защиты, а также средства резервирования и восстановления. Делая акцент на программно-технических средствах, можно выделить три основных уровня антивирусной защиты:

1. *Поиск и уничтожение известных вирусов.*
2. *Поиск и уничтожение неизвестных вирусов.*
3. *Блокировка проявления вирусов.*

1. При поиске и уничтожении известных вирусов наиболее распространенным является метод сканирования. Указанный метод заключается в выявлении компьютерных вирусов по их уникальному фрагменту программного кода (сигнатуре, программному штамму). Для этого создается некоторая *база данных сканирования* с фрагментами кодов известных компьютерных вирусов. Обнаружение вирусов осуществляется путем сравнения данных памяти компьютера с фиксированными кодами базы данных сканирования. В случае выявления и идентификации кода нового вируса, его сигнатура может быть введена в базу данных сканирования. В виду того, что сигнатура известна, то существует возможность корректного восстановления (обеззараживания) зараженных файлов и областей. Следует добавить, что некоторые системы хранят не сами сигнатуры, а, например, контрольные суммы или имитоприставки сигнатур.

Антивирусные программы, выявляющие известные компьютерные вирусы, называются *сканерами* или детекторами. Программы, включающие функции восстановления зараженных файлов, называют *полифагами* (фагами), докторами или дезинфекторами. Примером сканера-полифага является знакомая программа Aidstest.

Принято разделять сканеры на следующие:

- транзитные, периодически запускаемые для выявления и ликвидации вирусов,
- резидентные (постоянно находящиеся в оперативной памяти), проверяющие заданные области памяти системы при возникновении связанных с ними событий (например, проверка файла при его копировании или переименовании).

К недостаткам сканеров следует отнести то, что они позволяют обнаружить вирусы, которые уже проникали в вычислительные системы, изучены и для них определена сигнатура. Для эффективной работы сканеров необходимо оперативно пополнять базу данных сканирования. Однако с увеличением объема базы данных сканирования и числа различных типов искомых вирусов снижается скорость антивирусной проверки. Само собой, если время сканирования будет приближаться ко времени восстановления, то необходимость в антивирусном контроле может стать не столь актуальной.

Некоторые вирусы (мутанты и полиморфные) кодируют или видоизменяют свой программный код. Это затрудняет или делает невозможным выделить сигнатуру, а следовательно, обнаружить вирусы методом сканирования.

Для выявления указанных маскирующихся вирусов используются специальные методы. К ним можно отнести метод эмуляции процессора. Метод заключается в имитации выполнения процессором программы и подсовывания вирусу фиктивных управляющих ресурсов. Обманутый таким образом вирус, находящийся под контролем антивирусной программы, расшифровывает свой код. После этого, сканер сравнивает расшифрованный код с кодами из своей базы данных сканирования.

2. Выявление и ликвидация неизвестных вирусов необходимы для защиты от вирусов, пропущенных на первом уровне антивирусной защиты. Наиболее эффективным методом является контроль целостности системы (обнаружение изменений). Данный метод заключаются в проверке и сравнении текущих параметров вычислительной системы с эталонными, соответствующими ее незараженному состоянию. Понятно, что контроль целостности не являются прерогативой исключительно системы антивирусной защиты. Он обеспечивает защищенность информационного ресурса от несанкционированных модификации и удаления в результате различного рода нелегитимных воздействий, сбоев и отказов системы и среды.

Для реализации указанных функций используются программы, называемые *ревизорами*. Работа ревизора состоит из двух этапов: фиксирование эталонных характеристик вычислительной системы (в основном диска) и периодическое сравнение их с текущими характеристиками. Обычно контролируемыми характеристиками являются контрольная сумма, длина, время, атрибут “только для чтения” файлов, дерево каталогов, сбойные кластеры, загрузочные сектора дисков. В сетевых системах могут накапливаться среднестатистические параметры функционирования подсистем (в частности исторический профиль сетевого трафика), которые сравниваются с текущими.

Ревизоры, как и сканеры, делятся на транзитные и резидентные.

К недостаткам ревизоров, в первую очередь резидентных, относят создаваемые ими всякие неудобства и трудности в работе пользователя. Например, многие изменения параметров системы вызваны не вирусами, а работой системных программ или действиями пользователя-программиста. По этой же причине ревизоры не используют для контроля зараженности текстовых файлов, которые постоянно меняются. Таким образом, необходимо соблюдение некоторого баланса между удобством работы и контролем целостности системы.

Ревизоры обеспечивают высокий уровень выявления неизвестных компьютерных вирусов, однако они не всегда обеспечивают корректное лечение зараженных файлов. Для лечения зараженных файлов неизвестными вирусами обычно используются эталонные характеристики файлов и предполагаемые способы их заражения.

Кроме этого ревизоры не определяют зараженные файлы, создаваемые или копируемые в систему.

Примерами ревизоров являются программы: MSAV ОС MS-DOS и ADinf фирмы “Диалог-Наука”.

Разновидностью контроля целостности системы является метод программного самоконтроля, именуемые вакцинацией. Идея методов состоит в присоединении к защищаемой программе модуля (*вакцины*), контролирующего характеристики программы, обычно ее контрольную сумму.

Помимо статистических методов контроля целостности, для выявления неизвестных и маскирующихся вирусов используются эвристические методы. Они позволяет выявить по известным признакам (определенным в базе знаний системы) некоторые маскирующиеся или новые модифицированные вирусы известных типов. В качестве примера признака вируса можно привести код, устанавливающий резидентный модуль в памяти, меняющий параметры таблицы прерываний и др. Программный модуль, реализующий эвристический метод обнаружения вирусов, называют *эвристическим анализатором*. Примером сканера с эвристическим анализатором является программа Dr Web фирмы “Диалог-Наука”.

К недостаткам эвристических анализаторов можно отнести ошибки 1-го и 2-го рода: ложные срабатывания и пропуск вирусов. Соотношение указанных ошибок зависит от уровня эвристики.

Понято, что если для обнаруженного эвристическим анализатором компьютерного вируса сигнатура отсутствует в базе данных сканирования, то лечение зараженных данных может быть некорректным.

3. Блокировка проявления вирусов предназначена для защиты от деструктивных действий и размножения компьютерных вирусов, которым удалось преодолеть первые два уровня защиты. Методы основаны на перехвате характерных для вирусов функций. Известны два вида указанных антивирусных средства:

- программы-фильтры,
- аппаратные средства контроля.

Программы-фильтры, называемые также резидентными сторожами и мониторами, постоянно находятся в оперативной памяти и перехватывают заданные прерывания, с целью контроля подозрительной действий. При этом они могут блокировать “опасные” действия или выдавать запрос пользователю.

Действия, подлежащие контролю, могут быть следующими: модификация главной загрузочной записи (MBR) и загрузочных записей логических дисков и ГМД, запись по абсолютному адресу, низкоуровневое форматирование диска, оставление в оперативной памяти резидентного модуля и др. Как и ревизоры, фильтры часто являются “навязчивыми” и создают определенные неудобства в работе пользователя. Примером фильтра является программа Vsafe ОС MS-DOS.

Встроенные аппаратные средства ПК обеспечивают контроль модификации системного загрузчика и таблицы разделов жесткого диска, находящихся в главном загрузочном секторе диска (MBR). Включение указанных возможностей в ПК осуществляется с помощью программы Setup, расположенной в ПЗУ. Следует указать, что программу Setup можно обойти в случае замены загрузочных секторов путем непосредственного обращения к портам ввода-вывода контроллеров жесткого и гибкого дисков.

Наиболее полная защита от вирусов может быть обеспечена с помощью специальных контроллеров аппаратной защиты. Такой контроллер подключается к ISA-шине ПК и на аппаратном уровне контролирует *все* обращения к дисковой подсистеме компьютера. Это не

позволяет вирусам маскировать себя. Контроллер может быть сконфигурирован так, чтобы контролировать отдельные файлы, логические разделы, “опасные” операции и т.д. Кроме того, контроллеры могут выполнять различные дополнительные функции защиты, например, обеспечивать разграничение доступа и шифрование.

Примером специальных контроллеров аппаратной защиты является плата Sheriff предприятия ФомСофт.

К недостаткам указанных контроллеров, как ISA-плат, относят отсутствие системы автоконфигурирования, и как следствие, возможность возникновения конфликтов с некоторыми системными программами, в том числе антивирусными.

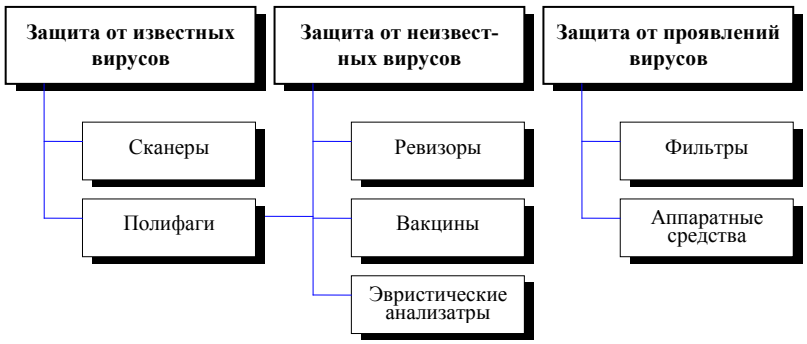

Рис. 9.1. Уровни и средства антивирусной защиты

При работе в глобальных сетях общего пользования, в частности в Internet, кроме традиционных способов антивирусной защиты данных компьютеров, становится актуальным антивирусной контроль всего проходящего трафика. Это может быть осуществлено путем реализации антивирусного прокси-сервера либо интеграции антивирусной компоненты с межсетевым экраном. В последнем случае межсетевой экран передает антивирусной компоненте (или серверу) допустимый, например, SMTP, FTP и HTTP-трафик. Содержащиеся в нем файлы проверяются на предмет наличия вирусов и, затем, направляются пользователям. Можно сказать, мы имеем дело с новым уровнем антивирусной защиты — уровнем межсетевого экранирования.

9.2. Обзор современных антивирусных средств

В настоящее время наблюдается тенденция в интегрировании различных антивирусных средств с целью обеспечения надежной многоуровневой защиты. На российском рынке наиболее мощными являются антивирусный комплект DialogueScience’s Anti-Virus kit (DSAV) АО “ДиалогНаука” и интегрированная антивирусная система AntiViral Toolkit Pro (AVP) ЗАО “Лаборатория Касперского”[2]. Указанные комплексы высоко зарекомендовали себя в нашей стране, особенно при обеспечении антивирусной защиты информационных систем малого и среднего офиса. Рассмотрим их по порядку.

[2] Созданная на базе антивирусного отдела НТЦ “КАМИ”.

9.2.1. Комплект антивирусных средств DSAV

До последнего времени самым популярным в России являлся комплект антивирусных средств DSAV АО “ДиалогНаука”, обеспечивающий защиту примерно от 16000 компьютерных вирусов в среде DOS и Windows 3.1x. Состав комплекта представлен в таблице 9.1.

Таблица 9.1.

Антивирусы	**Назначение**
Aidstest	сканер-полифаг немаскирующихся вирусов
Dr.Web	сканер-полифаг с эвристическим анализатором полиморфных вирусов
Adinf	ревизор диска
ADinf Cure Module	приложение ревизора диска — полифаг известных и неизвестных вирусов

Предшественником комплекса является один из первых отечественных транзитных сканеров-полифагов программа Aidstest, ориентированная на простые немаскирующиеся компьютерные вирусы. Будучи уже раритетом, Aidstest поставляется как бесплатное приложение DSAV.

Программа Dr. Web является наиболее популярным в стране транзитным сканером-полифагом с эвристическим анализатором. Основная направленность Dr. Web состоит в обнаружение полиморфных вирусов. В настоящее время Dr. Web реализует наиболее эффективный эвристический анализатор неизвестных вирусов в мире. По данным журнала Virus Bulletin, это обеспечивает обнаружение до 80-91% неизвестных вирусов, в т.ч. 99% макровирусов! На международных конкурсах Dr.Web несколько раз входил в тройку самых лучших антивирусов для DOS. Продукт достаточно компактный, что позволяет запускать его с дискеты.

ADinf — наиболее популярный транзитный ревизор диска. Работает с диском непосредственно по секторам (не по файлам) путем прямого обращения к функциям BIOS без использования функций DOS. Это исключает маскировку Stealth-вирусов и обеспечивает высокое быстродействие программы.

ADinf Cure Module — лечащий модуль ревизора диска. Программа позволяет восстанавливать зараженные данные в исходное незараженное состояние. Это осуществляется на основе фиксируемых ревизором характеристик системы и заложенных в лечащий модуль информации о типовых методах заражения. В настоящее время ADinf Cure Module обеспечивает корректное восстановление зараженных файлов на 97-100%.

Комплект DSAV совместим и может поставляться с платой Sheriff.

В настоящее комплект работает в среде DOS/Windows 3.x., однако анонсированы версии сканера-полифага Dr.Web для Novell Netware, Windows 95, Windows NT, OS/2 и ревизора ADinf для Windows 95 и Windows NT.

9.2.2. Интегрированная антивирусная система AVP

Система AVP первоначально представляла тандем двух программ: сканера и ревизора. В настоящее время AVP претерпела существенные усовершенствования и включает все основные элементы антивирусной программной защиты компьютера и локальной сети. Имеются версии для DOS, Windows 3.1x, Windows 95, Windows NT, Novell NetWare.

По мировым оценкам последних 5-х лет система AVP неоднократно входила в тройку наилучших в мире антивирусных продуктов поиска и удаления компьютерных вирусов в автономном компьютере. Система имеет одну из самых больших баз данных сканирования — более 14 000 тестов. В настоящее время система обнаруживает практически все полиморфные вирусы.

Говоря о достоинствах системы, следует указать, что программный продукт AVP сертифицирован Гостехкомиссией и фирмой Microsoft.

В настоящий момент “Лаборатория Касперского” выпускает следующие программные средства антивирусной защиты:

1. Сканеры-полифаги AVP с эвристическим анализатором (AVP Code Analyzer) для DOS (пакетный вариант: AVP Lite), Windows 95, Windows NT Workstation, Windows NT Server (AVP F-Secure[3]) и Novell Netware (AVPN);
2. Ревизор диска (CRC-сканер) AVP Inspector для Windows 95 и Windows NT;
3. Фильтры (резидентные мониторы) AVP Monitor для Windows 95, Windows NT Workstation, Windows NT Server (AVP F-Secure) и Novell Netware (AVPN);
4. Электронный мультимедийный справочник по вирусологии AVP Virus Encyclopedia;
5. Различные утилиты и дополнительные продукты, как-то: макро-полифаг AVP Macro Stop (AVP MacroKiller), сканер сообщений электронной почты на рабочих станциях AVP Mail Checker для Windows 95 и др.

9.2.3. Сравнительные характеристики антивирусных комплексов

Сравнительные характеристики наиболее эффективных антивирусных средств по данным Virus Bulletin представлены в таблицах 9.2 и 9.3. Наилучшие антивирусы на начало 1998 года указаны в таблице 9.4.

Таблица 9.2.

Характеристики сканеров компьютерных вирусов для DOS

Антивирус	**Время сканирования зараженного ГМД, *мин***	**Скорость передачи данных при работе с жестким диском, *Кб/с***	**Процент найденных вирусов**		
			Обычные	**Полиморфные**	**Актуальные**
Dr Web (Диалог-Наука)	1.48	86.3	98.2	95.5	86.7
Antiviral Toolkit Pro	0.57	195.6	99.8	100	96.6

[3] Совместная разработка Data Fellows (Финляндия) и Лаборатории Касперского.

Антивирус	Время сканирования зараженного ГМД, *мин*	Скорость передачи данных при работе с жестким диском, *Кб/с*	Процент найденных вирусов		
(КАМИ)					
AntiVirus (IBM)	1.09	604.8	98.2	65.2	99.7
Norton AntiVirus (Symantec)	0.46	2700.5	92.8	59.7	96.6
Dr Solomon's AVTK (S&S)	1.02	2282.6	99.5	90.7	99.4

Virus Bulletin, 06.96

Таблица 9.3.

Характеристики сканеров компьютерных вирусов для DOS

Антивирус	Бутовые актуальные		Файловые актуальные		Актуальные	Обычные		Полиморфные	
	Число	Процент	Число	Процент	Процент	Число	Процент	Число	Процент
Command F-Prot	86	100.0%	419	96.8%	98.1%	481	93.6%	6053	50.4%
Dr Solomon's AVTK	86	100.0%	418	97.7%	98.7%	530	99.6%	10997	98.8%
McAfee Scan	83	96.5%	423	97.9%	97.3%	473	93.1%	9078	77.8%
Norman Virus Control	86	100.0%	435	100.0%	100.0%	532	100.0%	11000	100.0%
Symantec Norton Antivirus	86	100.0%	434	99.6%	99.8%	441	89.8%	10500	95.5%

Virus Bulletin, 01.97

Таблица 9.4.

Лучшие антивирусные продукты на начало 1998 года

ОС (дата)	Windows NT (март 1998)	DOS (февраль 1998)	Windows 95 (январь 1998)
Антивирусы	Dr Solomon's Software AVTK v7.79	•Data Fellows F-Secure Anti-Virus 3.0.115 •Dr Solomon's Software AVTK v7.77 •IBM AntiVirus v3.0w •KAMI AVP v3.0.115 •McAfee VirusScan v3.1.2.3010 •Norman ThunderByte Virus Control v8.04 •Norman Virus Control v4.30 •Sophos SWEEP v3.03	•Command Software F-PROT Pro v3.00 •IBM AntiVirus v3.0f •Norman ThunderByte Virus Control v8.03 •Norman Virus Control v4.20 •Sophos SWEEP v3.01a

Virus Bulletin,04.98

Следует отметить, что отечественные разработки зарекомендовали себя высоко эффективными средствами антивирусной защиты на автономных ПК, главным образом работающих под управлением DOS/Windows 3.x. Несмотря на наметавшийся прогресс в области антивирусной защиты 32-х разрядных ОС и сетевой среды, они еще уступают место зарубежным программным средствам.

Поэтому имеет смысл перечислить в таблице 9.5 наиболее известные зарубежные фирмы, производящие антивирусные средства для сетевых приложений.

Таблица 9.5.

Поддержка операционной сетевой среды

Фирма	Windows NT Server	Novell Netware	OS/2	SCO UNIX	Solaris	HP-UNIX	Macintosh	Межсетевые экраны
Symantec	+	+	-	-	-	-	+	+
EliaShim	+	+	-	-	-	-	-	+ (Check Point FireWall)
Datel	+				+	+		+ (прокси - сервер)
NETA	+	+	+	-	-	-	+	+
S&S	+	+	+	+			-	

В заключении следует сказать, что международные тесты и конкурсы направлены на борьбу с компьютерными вирусами международного, преимущественно евро-американского сообщества. Это несколько искажает оценки эффективности антивирусных средств применительно к нашей стране. Отечественные разработки ориентированы на компьютерные вирусы, являющиеся актуальными (inter wild) именно в России и ближайших евроазиатских стран. Сказанное делает AVP и DSAV, весьма, предпочтительными относительно зарубежных аналогов.

ЗАКЛЮЧЕНИЕ

Мы рассмотрели законодательно-правовые и организационно-технические основы обеспечения безопасности информации в автоматизированных системах и информационно-вычислительных сетях.

Предложенный читателю материал, конечно, не может претендовать на полное и всестороннее освещение проблемы обеспечения информационной безопасности. Нашей целью было рассмотрение основных современных представлений в данной области и раскрытие некоторых тонкостей и особенностей применения действующей законодательной базы и организационно-технических мер, которые проявляются на практике при построении систем обеспечения безопасности информации.

Следует отметить, что в вопросах законодательно-правового обеспечения безопасности информации до сих пор остается много “белых пятен”, которые связаны с отсутствием ряда основополагающих законодательных актов, или “нестыковки” действующих законов и подзаконных актов. В частности, до сих пор не принят Федеральный закон “О коммерческой тайне”, неоднократно обсуждавшийся в Государственной Думе, существует целый ряд спорных положений в Федеральном законе от 20 февраля 1995 года № 24-ФЗ “Об информации, информатизации и защите информации”.

Все это порождает определенные трудности при практическом построении систем обеспечения безопасности информации предприятия или отдельной автоматизированной системы.

Однако процесс законотворчества движется вперед в положительном направлении и это вселяет оптимизм и уверенность в хорошей перспективе решения основных вопросов обеспечения безопасности информации.

ЛИТЕРАТУРА

1. Алёшенков М., Бузанова Я., Ярочкин В. Концепция комплексной безопасности предпринимательства: Учебное пособие. - М.: Паруса, 1997. - 31 с.
2. Атака через Интернет /И.Д.Медведовский, П.В.Семьянов, В.В.Платонов; Под ред. проф. П.Д.Зегжды. - СПб.: Мир и семья-95, 1997. - 296 с.
3. Банковская система России. Настольная книга банкира. Безопасность банка.- М.: Изд. ТОО Инжиниринго-консалтинговая компания “ДеКА”, 1995.- 104 с.
4. Барсуков В.С., Дворянкин С.В., Шеремет И.А. Безопасность связи в каналах телекоммуникаций. // ТЭК. - 1992. - Т. 20. - 122 с.
5. Батурин Ю.М. Право и политика в компьютерном круге.- М.: Наука, 1987.- 112 с.
6. Батурин Ю.М. Проблемы компьютерного права. - М.: Изд. юридич. лит-ры, 1991. - 271 с.
7. Батурин Ю.М., Жодзишский А.М. Компьютерная преступность и компьютерная безопасность.- М.: Юридическая литература. - 160 с.
8. Безруков Н.Н. Классификация компьютерных вирусов MS-DOS и методы защиты от них.- М.: Изд. СП “ICE”, 1990.- 48 с.
9. Безруков Н.Н. Компьютерная вирусология. - К.: Укр. советская энцикл. - 1991. - 416 с.
10. Белая книга Российских спецслужб. Изд. 2-е. - М.: Изд. Информационно-издательского агентства “Обозреватель”, 1996. - 272 с.
11. Вехов В.Б. Компьютерные преступления: Способы совершения и раскрытия. - М.: Изд-во “Право и Закон”, 1996.- 182 с.
12. Владимиров Д.Н. Критерии выбора межсетевого экрана. // Защита Информации. Конфидент. - 1998. - № 1. - С. 29-33.
13. Вычислительная техника. Терминология: Справочное пособие. - М.: Изд-во стандартов, 1989.- 168 с.
14. Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации. - М.: Яхтсмен, 1996. - 190 с.
15. Гайкович В., Першин А. Безопасность электронных банковских систем. - М.: Единая Европа, 1994. - 363 с.
16. Галатенко В., Трифаленков И. Информационная безопасность в Интранет: концепции и решения. // Jet Info. - 1996. - № 23-24. - С. 3-29.
17. Галатенко В.А. Информационная безопасность. //Открытые системы. - 1996. - № 1. - С. 38-43.
18. Галатенко В.А. Информационная безопасность. //Открытые системы. - 1996. - № 2. - С. 53-57.
19. Галатенко В.А. Информационная безопасность. //Открытые системы. - 1996. - № 3. - С. 42-45.

20. Галатенко В.А. Информационная безопасность. //Открытые системы. - 1996. - № 4. - С. 40-47.

21. Галатенко В.А. Информационная безопасность: Обзор основных положений. //Jet Info. - 1998. - Спец. выпуск. - 60 с.

22. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. В 2-х кн. - М.: Энергоатомиздат, 1994. - Кн. 1. - 400 с., кн.2. - 175 с.

23. Гудков П.Б. Компьютерные преступления в сфере экономики //В сб.: Актуальные проблемы борьбы с коррупцией и организованной преступностью в сфере экономики. - М.: Изд. МИ МВД России, 1995.- с. 136-145.

24. Демин В.В., Судов Е.В. Интегрированная система информационной безопасности. //Сети и системы связи. - 1996. - № 9. - С. 132-133.

25. Жельников В. Криптография от папируса до компьютера. - М.: ABF, 1996. - 336 с.

26. Заморин А.П., Марков А.С. Толковый словарь по вычислительной технике и программированию. Основные термины.- М.: Русский язык, 1987.- 221 с.

27. Зарубежная радиоэлектроника. 1989. N 12. Защита информации. Специальный выпуск /Под ред. В.А.Герасименко.- М.: Радио и связь, 1989.- 128 с.

28. Защита информации в персональных ЭВМ /А.В.Спесивцев, В.А.Вегнер, А.Ю.Крутяков и др.- М.: Радио и связь, 1992.- 192 с.

29. Защита информации. //Вычислительная техника и ее применение. Вып. 9.- М.: Изд-во “Знание”, 1990.- 48 с.- (Новое в жизни, науке и технике).

30. Защита информации. Сборник статей. - М.: Изд. МП “Ирбис”, 1992.- Вып. 1 - 240 с.

31. Зима В.М., Молдовян А.А. Многоуровневая защита от компьютерных вирусов. - СПб.: ВИКА им. А.Ф.Можайского, 1997. - 170 с.

32. Зима В.М., Молдовян А.А. Технология практического обеспечения информационной безопасности: Учеб.пособие. - СПб.: Изд. ВИКА им. А.Ф.Можайского, 1997. - 118 с.

33. Зима В.М., Молдовян А.А., Молдовян Н.А. Защита компьютерных ресурсов от несанкционированных действий пользователей: Учеб.пособие. - СПб.: ВИКА им. А.Ф.Можайского, 1997. - 189 с.

34. Касперский Е. Компьютерные вирусы в MS-DOS. - М.: Эдель, 1992. - 175 с.

35. Климов В.А. Положение об отделе защиты информации.// Защита Информации. Конфидент. - 1998.- № 1. - С. 13 - 20.

36. Ковалерчик И. Брандмауэры, или запирайте вашу дверь. - Сети. - 1997, № 2. - С. 88-99.

37. Крысин А.В. Безопасность предпринимательской деятельности. - М.: Финансы и статистика, 1996.- 384 с.

38. Льюс К. Как защитить сеть от “взлома”. // Сети и системы связи. - 1998. - № 2. - С. 136-142.

39. Мафтик. С. Механизмы защиты в сетях ЭВМ: Пер. с англ. - М.: Мир, 1993. - 216 с.

40. Миронос В. SecurID - технология “двухкомпонентной” аутентификации. //Computerweek Moscow. - 1997. - № 39. - С. 26, 45, 47.

41. Моисеенков И. Американская классификация и принципы оценивания безопасности компьютерных систем. // Компьютер Пресс. - 1992. - № 2. - С. 61-68; № 3. - С. 47-54.

42. Моисеенков И. Суета вокруг Роберта или Моррис-сын и все, все, все... //Компьютер Пресс. 1991. N 8. С. 45-62; N 9. С. 7-20.

43. Морриси П. Воздвигая “огненные стены”. //Сети и системы связи. - 1997. - № 6. - С. 115-123.

44. Некоторые правовые аспекты защиты и использования сведений, накапливаемых в информационных системах //Борьба с преступностью за рубежом. - М.: ВИНИТИ, 1990, № 7.- с. 63-64; 1992, № 6.- с. 13-14.

45. Никитин Ф.Н. Администратор безопасности корпоративной сети и его инструментарий. //Защита Информации. Конфидент. - 1997. - № 2. - С. 60-65.

46. Пашков Ю.Д., Казеннов В.Н. Организация защиты информации от несанкционированного доступа в автоматизированных системах. - СПб.: АОЗТ, 1995. - 76 с.

47. Право и информатика /Под ред. Е.А.Суханова.- М.: Изд-во МГУ,- 144 с.

48. Предотвращение компьютерных преступлений //Проблемы преступности в капиталистических странах. - М.: ВИНИТИ, 1986, № 4.- с. 5-9.

49. Преснухин В.В., Пискова Г.К. Некоторые аспекты моделирования воспроизведения компьютерного вируса и совершенствования программных средств защиты //Информатика и вычислительная техника за рубежом /ВИМИ. 1991. N 4. С. 52-63.

50. Расторгуев С. Программные методы защиты информации в компьютерных сетях. - М.: Яхтсмен, 1993. - 187 с.

51. РД ГТК. Автоматизированные системы. Защита от несанкционированного доступа к информации: Классификация автоматизированных систем и требования по защите информации. - М.: Военное издательство, 1992.

52. РД ГТК. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. - М.: Военное издательство, 1992.

53. РД ГТК. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации. - М.: Военное издательство, 1992.

54. РД ГТК. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Термины и определения. - М.: Военное издательство, 1992. - 13 с.

55. РД ГТК. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. // Защита Информации. Конфидент. - 1997. - № 6. - С. 26-31.

56. Ронин Р. Своя разведка. - Минск: Изд-во “Харвест”, 1998.- 368 с.

57. Руководство по информационной безопасности предприятия. // Jet Info. - 1996. - № 10-11. - С.11-

58. Селиванов Н.А. Проблемы борьбы с компьютерной преступностью //Законность, 1993, № 8.- с. 36-40.

59. Соловьев Э. Коммерческая тайна и ее защита. - М.: Изд-во ЗАО “Бизнес-школа “Интел-Синтез”, 1997.- 96 с.

60. Теория и практика обеспечения информационной безопасности. / Под ред. П.Д.Зегжды. - М.: Яхтсмен, 1996. - 192 с.

61. Уиллис Д. Игра ва-банк с сетевыми “медвежатниками”. // Сети и системы связи. - 1997. - № 9. - С. 121-129.

62. Уолкер Б.Дж., Блейк Я.Ф. Безопасность ЭВМ и организация их защиты. - М.: Связь, 1980. - 112 с.

63. Федеральный закон “Об информации, информатизации и защите информации“ (от 20.02.95 г. № 24-ФЗ). Москва. 1995. - 32 с.

64. Фролов А.В., Фролов Г.В. Осторожно: компьютерные вирусы. - М.: ДИАЛОГ-МИФИ, 1996. - 256 с.

65. Хоффман Л. Современные методы защиты информации: Пер. с англ. /Под ред. В.А.Герасименко. - М.: Советское радио, 1980. - 264 с.

66. Цуприков С. Новый этап автоматизации банков Московского региона //ComputerWorld, 1993, № 28.

67. Щербаков А. Разрушающие программные воздействия. - М.: Эдель, 1993. - 63 с.

68. Эрланджер Э. Безопасность сети. // PC Magazine/RE - 1997, № 3. - С. 56-64.

69. Юсупов Р.М., Пальчун Б.П. Безопасность компьютерных информационных систем критических приложений // Вооружение, политика и конверсия. - 1993. - № 2, 3

70. Ярочкин В.И. Безопасность информационных систем. - М.: Ось-89, 1996. - 320 с.

71. An Introduction to Computer Security: The NIST Handbook. - National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce. - NIST SP 800-12. - 1996.

72. Barker L.K., Nelson L.D. Security Standards - Govenment and Commercial //AT&T Techn. J., 1988, v. 67, N 3, P. 9-18.

73. Carroll J.M. Security and Credibility and some Fundamental Flows //Proc. 7th Int. Conf. and Exhib. Inf. Secur., Oxford,

74. Cooper J.A. Computer & Communications Security: Strategies for the 1990s. - Singapore: McGraw-Hill Book Company, 1989. - 411 p.

75. Datapro reports on Information Security.- Datapro Research Group. Delran, NJ, USA, 1991.

76. DoD 5200.28-STD. Department of Defense Trusted Computer Security Evaluation Criteria.- DoD Press, Washington, DC, USA, 1986.

77. Ford W. Computer Communications Security: Principles, Standard Protocols and Techniques. - Englewood Cliffs, New Jersey, USA: Prentice Hall PTR, 1994. - 493 p.

78. Hare C., Siyan K.. Internet Firewalls and Network Security. - New Riders Publishing, 1996. - 631 p.

79. Holbrook P., Reynolds J. Site Security Handbook. - Request for Comments: 1244, 1991.

80. Implementing Internet Security. / Cooper F.J. and etc. - Indianapolis: New Riders Publishing, 1995. - 378 p.

81. Information Security: An Integrated Collection of Essays./ By ed. M.D.Abrams, S.Jajodia, H.J.Podell. - Los Alamitos: IEEE Computer Society Press, 1994. - 752 p.

82. LANSEC-94 Conference Proceedings. - Washington DC, 1994. -Vol. 1-3, № 1-48.

83. National High-Perfomance Computer Technology Act of 1989 //US Senate Hearings. S-1067.- US Senate, Washington, DC, USA,

84. Seventh Annual Computer Security Applications Conference Proceedings. - IEEE Computer Society Press, 1991. - 255 p.

85. Site Security Handbook. / By ed. P. Holbrook, J. Reynolds - Request for Comments: 1244, 1991.

86. Sixth Annual Canadian Computer Security Symposium Proceedings. - Ottawa Congress Centre, 1994. - 644 p.

87. Siyan K., Hare C. Internet Firewalls and Network Security. - Indianapolis: New Riders Publishing, 1995. - 410 p.

88.Taber M. Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network. - Macmillan computer publishing

ПРИЛОЖЕНИЕ 1.
ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

1. Термины и определения по защите от несанкционированного доступа к информации.

Выпущенный Гостехкомиссией России в 1992 году “Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения” определяет формулировки основных понятий в области защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации.

Указанные термины обязательны для применения во всех видах документации.

Для каждого понятия установлен один термин. Применение терминов - синонимов термина не допускается.

Для отдельных терминов приведены в качестве справочных краткие формы, которые разрешается применять в случаях, исключающих возможность их различного толкования.

В качестве справочных приведены иностранные эквиваленты русских терминов на английском языке, а также алфавитные указатели содержащихся в нем терминов на русском и английском языках.

Таблица 1

ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Термин	Определение
1. Доступ к информации Доступ Access to information	Ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации
2. Правила разграничения доступа ПРД Security policy	Совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа
3. Санкционированный доступ к информации Authorized access to information	Доступ к информации, не нарушающий правила разграничения доступа
4. Несанкционированный доступ к информации НСД Unauthorized access to information	Доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами. П р и м е ч а н и е. Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения средств вычислительной техники или автоматизированных систем
5. Защита от несанкцио-	Предотвращение или существенное

Термин	Определение
нированного доступа Защита от НСД Protection from unauthorized access	затруднение несанкционированного доступа
6. Субъект доступа Субъект Access subject	Лицо или процесс, действия которых регламентируются правилами разграничения доступа
7. Объект доступа Объект Access object	Единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа
8. Матрица доступа Access matrix	Таблица, отображающая правила разграничения доступа
9. Уровень полномочий субъекта доступа Subject privilege	Совокупность прав доступа субъекта доступа
10. Нарушитель правил разграничения доступа Нарушитель ПРД Security policy violator	Субъект доступа, осуществляющий несанкционированный доступ к информации
11. Модель нарушителя правил разграничения доступа Модель нарушителя ПРД Security policy violater's model	Абстрактное (формализованное или неформализованное) описание нарушителя правил разграничения доступа
12. Комплекс средств защиты КСЗ Trusted computing base	Совокупность программных и технических средств, создаваемая и поддерживаемая для обеспечения защиты средств вычислительной техники или автоматизированных систем от несанкционированного доступа к информации
13. Система разграничения доступа СРД Security policy realization	Совокупность реализуемых правил разграничения доступа в средствах вычислительной техники или автоматизированных системах
14. Идентификатор доступа Access identifier	Уникальный признак субъекта или объекта доступа
15. Идентификация Identification	Присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов
16. Пароль Password	Идентификатор субъекта доступа, который является его (субъекта) секретом

Термин	Определение
17. Аутентификация Authentication	Проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности
18. Защищенное средство вычислительной техники (защищенная автоматизированная система) Trusted computer system	Средство вычислительной техники (автоматизированная система), в котором реализован комплекс средств защиты
19. Средство защиты от несанкционированного доступа Средство защиты от НСД Protection facility	Программное, техническое или программно-техническое средство, направленное на предотвращение или существенное затруднение несанкционированного доступа
20. Модель защиты Protection model	Абстрактное (формализованное или неформализованное) описание комплекса программно-технических средств и/или организационных мер защиты от несанкционированного доступа
21. Безопасность информации Information security	Состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы от внутренних или внешних угроз
22. Целостность информации Information integrity	Способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и (или) преднамеренного искажения (разрушения)
23. Конфиденциальная информация Sensitive information	Информация, требующая защиты
24. Дискреционное управление доступом Discretionary access control	Разграничение доступа между поименованными субъектами и поименованными объектами. Субъект с определенным правом доступа может передать это право любому другому субъекту
25. Мандатное управление доступом Mandatory access control	Разграничение доступа субъектов к объектам, основанное на характеризуемой меткой конфиденциальности информации, содержащейся в объектах, и официальном разрешении (допуске) субъектов обращаться к информации такого уровня конфиденциальности
26. Многоуровневая защита Multilevel secure	Защита, обеспечивающая разграничение доступа субъектов с различными правами доступа к объектам различных уровней конфиденциальности

Термин	Определение
27. Концепция диспетчера доступа Reference monitor concept	Концепция управления доступом, относящаяся к абстрактной машине, которая посредничает при всех обращениях субъектов к объектам
28. Диспетчер доступа Security kernel	Технические, программные и микропрограммные элементы комплекса средств защиты, реализующие концепцию диспетчера доступа; ядро защиты
29. Администратор защиты Security administrator	Субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации
30. Метка конфиденциальности Метка Sensitivity label	Элемент информации, который характеризует конфиденциальность информации, содержащейся в объекте
31. Верификация Verification	Процесс сравнения двух уровней спецификации средств вычислительной техники или автоматизированных систем на надлежащее соответствие
32. Класс защищенности средств вычислительной техники (автоматизированной системы) Protection class of computer systems	Определенная совокупность требований по защите средств вычислительной техники (автоматизированной системы) от несанкционированного доступа к информации
33. Показатель защищенности средств вычислительной техники Показатель защищенности Protection criterion of computer systems	Характеристика средств вычислительной техники, влияющая на защищенность и описываемая определенной группой требований, варьируемых по уровню, глубине в зависимости от класса защищенности средств вычислительной техники
34. Система защиты секретной информации СЗСИ Secret information security system	Комплекс организационных мер и программно-технических (в том числе криптографических) средств обеспечения безопасности информации в автоматизированных системах
35. Система защиты информации от несанкционированного доступа СЗИ НСД System of protection from unauthorized access to information	Комплекс организационных мер и программно-технических (в том числе криптографических) средств защиты от несанкционированного доступа к информации в автоматизированных системах

Термин	Определение
36. Средство криптографической защиты информации СКЗИ Cryptographic information protection facility	Средство вычислительной техники, осуществляющее криптографическое преобразование информации для обеспечения ее безопасности
37. Сертификат защиты Сертификат Protection certificate	Документ, удостоверяющий соответствие средства вычислительной техники или автоматизированной системы набору определенных требований по защите от несанкционированного доступа к информации и дающий право разработчику на использование и/или распространение их как защищенных
38. Сертификация уровня защиты Сертификация Protection level certification	Процесс установления соответствия средства вычислительной техники или автоматизированной системы набору определенных требований по защите

2. Термины и определения в области межсетевых экранов

В руководящем документе Гостехкомиссии России [55]: “Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации” определен ряд терминов в области построения межсетевых экранов (МЭ).

Руководящий документ вводит следующие основные термины и определения:

Администратор МЭ - лицо, ответственное за сопровождение МЭ.

Дистанционное управление компонентами МЭ - выполнение функций по сопровождению МЭ (компоненты) администратором МЭ с узла (рабочей станции) сети, на котором не функционирует МЭ (компонента) с использованием сетевых протоколов.

Критерии фильтрации - параметры, атрибуты, характеристики, на основе которых осуществляется разрешение или запрещение дальнейшей передачи пакета (данных) в соответствии с заданными правилами разграничения доступа (правилами фильтрации). В качестве таких параметров могут использоваться служебные поля пакетов (данных), содержащие сетевые адреса, идентификаторы, адреса интерфейсов, портов и другие значимые данные, а также внешние характеристики, например, временные, частотные характеристики, объем данных и т.п.

Локальное (местное) управление компонентами МЭ - выполнение функций по сопровождению МЭ (компоненты) администратором МЭ (компонента) с использованием интерфейса МЭ.

Межсетевой экран (МЭ) - это локальное (однокомпонентное) или функционально- распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в АС и /или выходящей из АС. МЭ обеспечивает защиту АС посредством фильтрации информации, т.е. ее анализа по совокупности критериев и принятия решения о ее распространении в (из) АС на основе заданных правил, проводя таким образом разграничение доступа субъектов из одной АС к объектам другой АС. Каждое правило запрещает или разрешает передачу информации определенного вида между субъектами и объектами. Как следствие, субъекты из одной АС получают доступ только к разрешенным информационным объектам из другой АС. Интерпретация набора правил выполняется последовательностью фильтров, которые разрешают или запрещают передачу данных (пакетов) на следующий фильтр или уровень протокола.

Правила фильтрации - перечень условий, по которым с использованием заданных критериев фильтрации осуществляется разрешение или запрещение дальнейшей передачи пакетов (данных) и перечень действий, производимых МЭ по регистрации и/или осуществлению дополнительных защитных функций.

Межсетевой экран может строиться с помощью экранирующих агентов, которые обеспечивают установление соединения между субъектом и объектом, а затем пересылают информацию, осуществляя контроль и /или регистрацию. Использование экранирующих агентов позволяет предоставить дополнительную защитную функцию - сокрытие от субъекта истинного объекта. В то же время, субъекту кажется, что он непосредственно взаимодействует с объектом. Обычно экран не является симметричным, для него определены понятия “внутри” и “снаружи”. При этом задача экранирования формулируется как защита внутренней области от неконтролируемой и потенциально враждебной внешней.

Сетевые адреса - адресные данные, идентифицирующие субъекты и объекты и используемые протоколом сетевого уровня модели международной организации по стандартизации взаимодействия открытых систем (ISO OSI). Сетевой протокол выполняет управление коммуникационными ресурсами, маршрутизацию пакетов, их компоновку для передачи в сети. В этих протоколах решается возможность доступа к подсети, определяется маршрут передачи и осуществляется трансляция сообщения. Управление доступом на сетевом уровне позволяет отклонять нежелательные вызовы и дает возможность различным подсетям управлять использованием ресурсов сетевого уровня. Поэтому в данных протоколах возможно выполнение требований по защите в части проверки подлинности сетевых ресурсов, источника и приемника данных, принимаемых сообщений, проведения контроля доступа к ресурсам сети.

Трансляция адреса - функция МЭ, скрывающая внутренние адреса объектов (субъектов) от внешних субъектов.

Транспортные адреса - адресные данные, идентифицирующие субъекты и объекты и используемые протоколом транспортного уровня модели ISO OSI. Протоколы транспортного уровня обеспечивают создание и функционирование логических каналов между программами (процессами, пользователями) в различных узлах сети, управляют потоками информации между портами, осуществляют компоновку пакетов о запросах и ответах.

Централизованное управление компонентами МЭ - выполнение с одного рабочего места (рабочей станции, узла) всех функций по сопровождению МЭ (его компонент), только со стороны санкционированного администратора, включая инициализацию, останов, восста-

новление, тестирование, установку и модификацию правил фильтрации данных, параметров регистрации, дополнительных защитных функций и анализ зарегистрированных событий.

Экранирование - функция МЭ, позволяющая поддерживать безопасность объектов внутренней области, игнорируя несанкционированные запросы из внешней области. В результате экранирования уменьшается уязвимость внутренних объектов, поскольку первоначально сторонний нарушитель должен преодолеть экран, где защитные механизмы сконфигурированы наиболее тщательно и жестко. Кроме того, экранирующая система, в отличие от универсальной, может и должна быть устроена более простым и, следовательно, более безопасным образом, на ней должны присутствовать только те компоненты, которые необходимы для выполнения функций экранирования. Экранирование дает также возможность контролировать информационные потоки, направленные во внешнюю область, что способствует поддержанию во внутренней области режима конфиденциальности. Помимо функций разграничения доступа, экраны осуществляют регистрацию информационных обмен*ов

3. Краткий глоссарий иностранных терминов по средствам защиты информации

ACL (*Access Control List*) - набор правил фильтрации пакетов на маршрутизаторах; правила доступа к данным для сервера

ActiveX - технология программирования небольших сетевых приложений, называемых апплетами; разработанна фирмой Microsoft

Authentication token - жетон (карточка) аутентификации — миниатюрное устройство, используемое для установления личности пользователя; работают по принципу запрос-отклик, на основе синхронизации по времени последовательности кодов и др. технологий

C (*Cyphertext*) - зашифрованный (закрытый) текст

CGI (*Common Gateway Interface*) - общий шлюзовой интерфейс

Challenge/response - метод аутентификации, предусматривающий, что сервер посылает пользователю произвольный запрос, а тот генерирует отклик при помощи одного из жетонов аутентификации

DES (*Data Encryption Standard*) - симметричный алгоритм шифрования с закрытым ключом, стандарт для обработки информации в государственных учреждениях США; алгоритм использует ключ длиной 56 бит и 8 битов проверки на четность и требует от злоумышленника перебора 72 квадриллионов возможных ключевых комбинаций

DNS (*Domain Name System*) - система имен доменов, представляющая распределенную базу данных, которая преобразует имена пользователей и хостов в IP-адреса и наоборот

DNS spoofing - присвоение имени домена другой системы путем либо искажения данных кэша службы имен интересующей взломщика системы, либо указания “действительного” домена серверу доменных имен.

DSA (*Digital Signature Algorithm*) - алгоритм цифровой подписи, позволяющий генерировать цифровые подписи на основе арифметических операций

Firewall - межсетевой экран (брандмауэр) — является защитным межсетевым барьером, позволяющим пропускает только авторизованные пакеты

Flame - личный выпад (“наезд”) в чей-либо адрес в сети USENET

FTP (*File Transfer Protocol*) - протокол передачи файлов по сети.

Gopher - протокол, разработанный для того, чтобы позволить пользователю передавать текстовые и двоичные файлы между компьютерами в сети

HTML - язык гипертекстовой разметки документов; используется для создания Web-страниц

HTTP - протокол передачи гипертекста; базовый протокол WWW, использующийся для передачи гипертекстовых документов

IP splicing - разновидность злонамеренного проникновения, когда взломщик вторгается в активный, уже установленный сеанс

IP spoofing - подмена адресов - разновидность вторжения, когда взломщик пытается замаскироваться под другую систему, используя ее IP-адрес

Java - технология программирования сетевых приложений, разработанная фирмой Sun Microsystems; среда для выполнения Java-апплетов должна быть безопасной, то есть апплет не должен иметь возможности модифицировать что-либо вне WWW-браузера

Kerberos - название технологии аутентификации в распределенной системе, созданной в Массачусетском технологическом институте на базе стандарта шифрования с открытым ключом DES

MD5 (*Message Digest algorithm*) - алгоритм, используемый для генерации цифровых подписей в тех случаях, когда, прежде чем подписать сообщение большого размера, его требуется сжать

NNTP - протокол передачи сетевых новостей для распространения новостей в Usenet

P (*Plaintext)* - открытый (общедоступный) текст

Plug-in - набор динамически подключаемых библиотек, используемых для увеличения функциональных возможностей основной программы, такой как WWW-браузер

Proxy - приложение-посредник, выполняемое на шлюзе, которое передает пакеты между авторизованным клиентом и внешним хостом; посредник принимает запросы от клиента на определенные сервисы Internet, а затем, действуя от имени этого клиента, устанавливает соединение для получения запрошенного сервиса

Proxy server - сервер-посредник; брандмауэр, в котором для преобразования IP-адресов всех авторизованных клиентов в IP-адреса, ассоциированные с брандмауэром, используется процесс, называемый трансляцией адресов (address translation)

RADIUS (*Remote Authentication Dial-In User Service*) - служба дистанционной аутентификации пользователей по коммутируемым линиям; стандарт Internet, обеспечивающий совместимость паролей различных систем аутентификации и систем управления учетными записями пользователей

RSA (*Rivest, Shamir, Adleman*) - ассиметричный ключ шифрования

Screening router - маршрутизатор с ограничением доступа, сконфигурированный на разрешение/запрещение трафика на основе набора правил доступа, заданных администратором

SKIP (*Simple Key management for Internet Protocol*) - простой алгоритм администрирования ключей для Internet

SMTP (*Simple Mail Transfer Protocol*) - протокол, позволяющий осуществлять почтовую транспортную службу Internet

SNS (*Secure Network Services*) - сетевая служба безопасности

Spamming - посылка большого числа одинаковых сообщений в различные группы UNENET;. используется для организации рекламной компании и пирамид

SSL (*Secure Sockets Layer*) - протокол защиты сообщений в TCP/IP-сетях, разработанный Netscape Communications; использует межконцевое шифрование трафика на прикладном уровне

SYN-overflow - метод вывода системы из строя путем посылки ей такого числа SYN-пакетов, которое не может обработать сетевой драйвер

TCP/IP (*Transmission Control Protocol/ Internet Protocol*) - коммуникационные протоколы, используемые для связи серверов Internet

Telnet - протокол, используемый для терминального (возможно удаленного) подключения к хосту

Tunneling router - маршрутизатор или система, направляющая трафик с помощью шифрования и/или инкапсуляции через предусмотренную сеть — виртуальный туннель; на месте назначения производится декапсуляция и дешифрование

UDP storm - чрезмерный поток пакетов UDP, используемый для “затопления” сервера, чтобы попытаться отразить вторжение

URL (*Uniform/Universal Resource Locator*) - универсальный локатор ресурсов

USENET - система обсуждения новостей на основе электронной почты; использует TCP/IP

VPN (*Virtual Private Networking*) - дистанционный доступ через Internet; метод использования инфраструктуры Internet для соединения различных ЛВС

ПРИЛОЖЕНИЕ 2.
СПИСОК ОСНОВНЫХ РУКОВОДЯЩИХ ДОКУМЕНТОВ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

1. Законы и Законодательные акты

1. **Конституция Российской Федерации**
   Принята 12 декабря 1992 года.
   - Статья 15. п.3. Законы подлежат официальному опубликованию. Неопубликованные законы не применяются. Любые нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина, не могут применяться, если они не опубликованы официально для всеобщего сведения.

2. **Гражданский кодекс Российской Федерации**
   Принят Государственной Думой 21 октября 1994 года.

- Глава 6. Общие положения.
  - Статья 138. Интеллектуальная собственность.
  - Статья 139. Служебная и коммерческая тайна.
    Информация составляет *служебную* или *коммерческую тайну* в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицом, к ней нет свободного доступа на законном основании и обладатель информации принимает меры к охране ее конфиденциальности.
- Глава 38. Выполнение научно-исследовательских, опытно-конструкторских и технологических работ.
  - Статья 771. Конфиденциальность сведений, составляющих предмет договора.
    Объем сведений , признаваемых конфиденциальными определяется в договоре.
- Глава 45. Банковский счет.
  - Статья 857. Банковская тайна.
  - Глава 48. Страхование
    - Статья 946. Тайна страхования.

3. **Уголовно-процессуальный кодекс Российской Федерации**

4. **Уголовный кодекс Российской Федерации**
   Принят Государственной Думой 24 мая 1996 года, одобрен Советом Федерации 5 июня 1996 года.

- Глава 19. Преступления против конституционных прав и свобод человека и гражданина
  - Статья 137. Нарушение неприкосновенности частной жизни
  - Статья 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений
  - Статья 139. Нарушение неприкосновенности жилища
  - Статья 140. Отказ в предоставлении гражданину информации
  - Статья 144. Воспрепятствование законной профессиональной деятельности журналистов
  - Статья 146. Нарушение авторских и смежных прав
  - Статья 147. Нарушение изобретательских и патентных прав
- Глава 23. Преступления против интересов службы в коммерческих и иных организациях
  - Статья 201. Злоупотребление полномочиями
  - Статья 203. Превышение полномочий служащими частных охранных или детективных служб
- Глава 22. Преступления в сфере экономической деятельности

- Статья 183. Незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну
- Статья 189. Незаконный экспорт технологий, научно-технической информации и услуг, используемых при создании оружия массового поражения, вооружения и военной техники

- Глава 25. Преступления против здоровья населения и общественной нравственности
  - Статья 237. Сокрытие информации об обстоятельствах, создающих опасность для жизни и здоровья людей
- Глава 28. Преступления в сфере компьютерной информации
  - Статья 272. Неправомерный доступ к компьютерной информации

1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, - *наказывается штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.*
2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой, либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, - *наказывается штрафом в размере от пятисот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или другого дохода осужденного за период от пяти до восьми месяцев, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.*

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

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

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

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

- Глава 29. Преступления против основ конституционного строя и безопасности государства
  - Статья 275. Государственная измена
  - Статья 276. Шпионаж
  - Статья 283. Разглашение государственной тайны
  - Статья 284. Утрата документов, содержащих государственную тайну

5. **Кодекс РСФСР об административных правонарушениях**
(по состоянию на 1 ноября 1997 года)

- Глава 10. Административные правонарушения на транспорте и в области дорожного хозяйства и связи.

- Статья 136[1]. Самовольное подключение оконечного оборудования к сетям электросвязи.
- Статья 137. Изготовление, ввоз в Российскую Федерацию, приобретение, проектирование, строительство, установка, эксплуатация, а также продажа либо передача в постоянное или во временное пользование радиоэлектронных средств или высокочастотных устройств, использование радиочастот без получения специального разрешения.
- статья 138. Нарушение правил регистрации, проектирования, строительства, установки, эксплуатации радиоэлектронных средств или высокочастотных устройств.
- Статья 139. Нарушение правил охраны линий связи и сооружений связи.
- статья 139[1]. Использование несертифицированных средств связи и предоставление несертифицированных услуг связи.
- Статья 139[2]. Несоблюдение нормативных документов. Регулирующих порядок эксплуатации электрической и почтовой связи.
- Статья 139[3]. Изготовление или эксплуатация технических средств, не соответствующих государственным стандартам или нормам на допускаемые радиопомехи.
- Статья 139[4]. Самовольное строительство или эксплуатация сооружений связи.
- Статья 139[5]. Нарушение правил проектирования или строительства сооружений связи
- Статья 139[6]. Осуществление деятельности в области связи без лицензии.
- статья 140[2]. Невыполнение предписаний органов государственного надзора за связью в Российской Федерации.
- Статья 140[3]. Воспрепятствование осуществлению должностными лицами органов государственного надзора за связью в Российской Федерации их служебных обязанностей.

- Глава 14. Административные правонарушения, посягающие на установленный порядок управления.
  - Статья 170. Нарушение обязательных требований государственных стандартов, правил обязательной сертификации, нарушение требований нормативных документов по обеспечению единства измерений.

6. Закон СССР
“О собственности”.
Вводит понятие “*интеллектуальная собственность*”.
(В связи с принятием части первой Гражданского кодекса РФ данный закон утратил силу с 1 января 1995 года).

7. Федеральный закон.
“Об основах государственной службы в Российской Федерации”.
Предусматривает возможность увольнения государственного служащего при однократном нарушении им своих обязанностей по защите государственной тайны.

8. Закон СССР от 12 июня 1990 года (25 декабря 1990 года).
“О предприятиях и предпринимательской деятельности”.
Вводит понятие “*коммерческая тайна*”.
(В связи с принятием части первой Гражданского кодекса РФ данный закон утратил силу с 1 января 1995 года (кроме статей 34 и 35).

9. Закон РСФСР от 24 декабря 1990 года.
“О собственности в РСФСР”.
(В связи с принятием части первой Гражданского кодекса РФ данный Закон утратил силу с 1 января 1995 года).

10. Закон РСФСР от 24 декабря 1990 года.
“О банках и банковской деятельности”.

11. Закон РСФСР № 1026-1 от 18 апреля 1991 года.
“О милиции”.

Редакции: Закон РФ № 4510-1 от 18 февраля 1993 года, Закон РФ № 5304-1 от 1 июля 1993 года, Федеральный закон РФ № 73-ФЗ от 15 июня 1996 года

12. Закон РСФСР от 22 марта 1991 года.
“О конкуренции и ограничении монополистической деятельности на товарных рынках”.

13. Закон РСФСР № 1253-1 от 17 мая 1991 года.
“О чрезвычайном положении”.

14. Закон РСФСР от 3 июля 1991 года.
“О приватизации государственных и муниципальных предприятий РСФСР”.

15. Закон РФ от 27 декабря 1991 года.
“О средствах массовой информации”.

16. Закон РФ № 2300-1 от 7 февраля 1992 года.
“О защите прав потребителей”.

17. Закон РФ № 2446-1 от 5 марта 1992 года.
“О безопасности”.

18. Закон РФ № 2487-1 от 11 марта 1992 года.
“О частной детективной и охранной деятельности в Российской Федерации”.

19. Закон РФ № 3526-1 от 14 мая 1992 года.
“О правовой охране топологий интегральных микросхем”.

20. Закон РФ № 3245-1 от 8 июля 1992 года.
“О внешней разведке”.

21. Закон РФ № 3246/1-1 от 8 июля 1992 года.
“О федеральных органах государственной безопасности”.
(Утратил силу в соответствии со ст. 26 Федерального закона “Об органах Федеральной службы безопасности в Российской Федерации” № 40-ФЗ от 3 апреля 1995 года).

22. Закон РФ № 3517-1 от 23 сентября 1992 года.
“Патентный закон Российской Федерации”.

23. Закон РФ № 3520-1 от 23 сентября 1992 года.
“О товарных знаках, знаках обслуживания и наименования мест происхождения товаров”.

24. Закон РФ № 3523-1 от 23 сентября 1992 года.
“О правовой охране программ для электронных вычислительных машин и баз данных”.

25. Закон РФ № 4524-1 от 19 февраля 1993 года.
“О Федеральных органах правительственной связи и информации”.

26. Закон РФ № 4992-1 от 20 мая 1993 года.
“Об оружии”.
(Отменен. С 1 июля 1997 года вступил в силу Федеральный закон РФ “Об оружии” № 150-ФЗ от 13 декабря 1996 года).

27. Закон РФ № 5151-1 от 10 июня 1993 года.
“О сертификации продукции и услуг”.

Сертификация продукции - это деятельность по подтверждению соответствия продукции установленным требованиям.

28. Закон РФ № 5154-1 от 10 июня 1993 года.
“О стандартизации”.

29. Основы законодательства РФ от 7 июля 1993 года.
“Об Архивном фонде Российской Федерации и архивах”.

30. Закон РФ № 5351-1 от 9 июля 1993 года.
“Об авторском праве и смежных правах”.

31. Закон РФ № 5485-1 от 21 июля 1993 года.
“О государственной тайне” (РГ от 21.09.93).
Введен в действие с 21 сентября 1993 года.
Внесены изменения Законом РФ № 131-ФЗ от 6 октября 1997 года “О внесении изменений и дополнений в Закон Российской Федерации “О государственной тайне” (СЗ РФ № 41-97, ст. 4673).

32. Федеральный закон № 77-ФЗ от 20 декабря 1994 года.
“Об обязательном экземпляре документов”.

33. Федеральный закон от 29 декабря 1994 года.
“О библиотечном деле”.

34. Федеральный закон № 15-ФЗ от 16 февраля 1995 года.
“О связи”.

35. Федеральный закон № 24-ФЗ от 20 февраля 1995 года.
“Об информации, информатизации и защите информации”.

36. Федеральный закон № 40-ФЗ от 3 апреля 1995 года.
“Об органах Федеральной службы безопасности в Российской Федерации”

37. Федеральный закон №108-ФЗ от 18 июля 1995 года.
“О рекламе”.

38. Федеральный закон № 144-ФЗ от 12 августа 1995 года.
“Об оперативно-розыскной деятельности”.

39. Федеральный закон № 85-ФЗ от 4 июля 1996 года.
“Об участии в международном информационном обмене”.

40. Федеральный закон от 22 августа 1996 года.
“О порядке выезда из Российской Федерации и въезда в Российскую Федерацию”.

- Статья 15.1 определяет ограничения права граждан РФ на выезд за границу в связи с их осведомленностью в государственной тайне и сроки таких ограничений.

41. Федеральный закон № 150-ФЗ от 13 декабря 1996 года.
“Об оружии”.

42. Федеральный закон.
“О государственной охране”.

43. Федеральный закон № 110-ФЗ от 19 июля 1997 года.
“О внесении изменений и дополнений в Уголовно-процессуальный кодекс РСФСР, Кодекс РСФСР об административных правонарушениях и Закон РФ “Об авторском праве и смежных правах”.

44. Федеральный закон № 131-ФЗ от 6 октября 1997 года.
“О внесении изменений и дополнений в Закон Российской Федерации “О государственной тайне” (СЗ РФ № 41-97, ст. 4673).

45. Рекомендательный законодательный акт от 23 мая 1993 года.
“О принципах регулирования информационных отношений в государствах - участниках Межпарламентской Ассамблеи СНГ”.

2. Указы и распоряжения Президента Российской Федерации

1. Указ Президента РФ № 313 от 24 декабря 1991 года.
“О создании Федерального агентства правительственной связи и информации при Президенте Российской Федерации”.

2. Указ Президента РФ № 9 от 5 января 1992 года.
“О создании Государственной технической комиссии при Президенте Российской Федерации”.

3. Указ Президента РФ № 104 от 21 января 1993 года.
“О нормативных актах центральных органов государственного управления Российской Федерации”.
п.1. Установить, что нормативные акты министерств и ведомств Российской Федерации, затрагивающие права, свободы и законные интересы граждан или носящие межведомственный характер, принятые после 1 марта 1993 года и прошедшие государственную регистрацию в Министерстве юстиции РФ, подлежат официальному опубликованию в газете “Российские вести”, если иное не предусмотрено законодательством.

4. Указ Президента РФ № 966 от 28 июня 1993 года.
О концепции правовой информатизации России”.

5. Указ Президента РФ № 209 от 12 февраля 1993 года.
“О милиции общественной безопасности (местной милиции) в Российской Федерации”.
Приложение 1. Положение о милиции общественной безопасности (местной милиции) в Российской Федерации.
Приложение 2. Перечень подразделений милиции общественной безопасности, содержащихся за счет бюджетных средств.

6. Указ Президента РФ № 2267 от 22 декабря 1993 года.
Утвердил **“Положение о Федеральной государственной службе в Российской Федерации”.**

7. Указ Президента РФ № 170 от 20 января 1994 года.
“Об основах государственной политики в сфере информатизации”.
Учредил **Комитет при Президенте РФ по политике информатизации**.

8. Указ Президента РФ № 552 от 17 марта 1994 года.
“Об утверждении Положения об Архивном фонде Российской Федерации и Положения о Государственной архивной службе России”.

9. Указ Президента РФ № 334 от 3 апреля 1995 года.
“О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации”.

10. Указ Президента РФ № 633 от 23 июня 1995 года.
“О первоочередных мерах по реализации Федерального закона “Об органах Федеральной службы безопасности в Российской Федерации”.
Внесены изменения Указом Президента РФ № 937 от 14 сентября 1995 года и Указом Президента РФ № 515 от 22 мая 1997 года.

11. Указ Президента РФ № 1390 от 1 июля 1994 года.
“О совершенствовании информационно-телекоммуникационного обеспечения органов государственной власти и порядке их взаимодействия при реализации государственной политики в сфере информатизации”.
Во исполнение Указа разработана **“Концепция формирования и развития единого информационного пространства России и соответствующих государственных информационных ресурсов”.**

> *Информационное пространство* определяется как совокупность баз и банков данных, технологий их ведения, и использования информационно-телекоммуникационных систем и сетей, функционирующих на основе единых принципов и по общим правилам, обеспечивающих информационное взаимодействие организаций и граждан, а также удовлетворения их информационных потребностей.

12. Указ Президента РФ № 1108 от 8 ноября 1995 года.
“О Межведомственной комиссии по защите государственной тайны”.

13. Указ Президента РФ № 1203 от 30 ноября 1995 года.
“Об утверждении Перечня сведений, отнесенных к государственной тайне”.
Распределены полномочия руководителей органов государственной власти и управления по распоряжению сведениями, отнесенными к государственной тайне. На них персонально возложена ответственность за принятие решений о засекречивании.
Изменен. См. Указ № 61 от 24 января 1998 года.

14. Указ Президента РФ № 21 от 9 января 1996 года.
“О мерах по упорядочению разработки, производства, реализации, приобретения в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы, а также использования специальных технических средств, предназначенных для негласного получения информации”.

15. Указ Президента РФ № 71 от 20 января 1996 года.
“Об утверждении Положения о Межведомственной комиссии по защите государственной тайны”.
Председатель - Первый заместитель Председателя Правительства РФ;
Заместители - Председатель Гостехкомиссии России и Директор ФСБ России;
Ответственный секретарь - Зам. Председателя ГТК.
Внесены изменения и дополнения Указом Президента РФ № 594 от 14 июля 1997 года.

16. Указ Президента РФ № 188 от 6 марта 1996 года.
“Об утверждении Перечня сведений конфиденциального характера”.

17. Указ Президента РФ № 346 от 9 марта 1996 года.
“Об утверждении Государственной программы обеспечения защиты государственной тайны в Российской Федерации”.

Продлена на 1998 год (Указ Президента РФ № 318 от 30 марта 1998 года).

18. Указ Президента РФ № 1013 от 2 июля 1996 года.
"**О мерах по совершенствованию деятельности федеральных органов государственной охраны".**
Включил в состав Федеральной службы охраны РФ Службу безопасности Президента РФ.

19. Указ Президента РФ № 1039 от 18 июля 1996 года.
"Об утверждении Положения о Министерстве внутренних дел Российской Федерации".

20. Указ Президента РФ № 1111 от 30 июля 1996 года.
"О мерах по созданию космической телекоммуникационной системы Российской Федерации".
Работы возложены на ОАО "Корпорация "Компомаш".

21. Указ Президента РФ № 1121 от 1 августа 1996 года.
"Об утверждении состава Совета Безопасности Российской Федерации".

22. Указ Президента РФ № 1128 от 1 августа 1996 года.
"об утверждении Положения об аппарате Совета Безопасности Российской Федерации".

23. Указ Президента РФ № 1136 от 2 августа 1996 года.
"Об утверждении Положения о Федеральной службе охраны Российской Федерации".

24. Указ Президента РФ № 1268 от 26 августа 1996 года.
Утверждает **"Список товаров и технологий двойного назначения, экспорт которых контролируется"**.

25. Указ Президента РФ № 188 от 6 марта 1997 года.
"Об утверждении Перечня сведений конфиденциального характера" (СЗ РФ № 10-97, ст. 1127).

26. Указ Президента РФ № 489 от 16 мая 1997 года.
"О приведении нормативных правовых актов Президента Российской Федерации в соответствие с Федеральным законом "Об оружии".
С 1 июля 1997 года утратили силу Указы:
- № 1341 от 8 ноября 1992 года,
- № 1342 от 8 ноября 1992 года.

27. Указ Президента РФ № 490 от 16 мая 1997 года.
"О внесении дополнения в Указ Президента Российской Федерации от 23 мая 1996 года № 763 "О порядке опубликования и вступления в силу актов Президента Российской Федерации, Правительства Российской Федерации и нормативных правовых актов федеральных органов исполнительной власти".
Нормативные правовые акты федеральных органов исполнительной власти, содержащие сведения, составляющие государственную тайну, или сведения конфиденциального характера и не подлежащие в связи с этим официальному опубликованию, прошедшие государственную регистрацию в Министерстве юстиции РФ, *вступают в силу со дня государственной регистрации и присвоения номера*, если самими актами не установлен более поздний срок их вступления в силу.

28. Указ Президента РФ № 515 от 22 мая 1997 года.

“О структуре Федеральной службы безопасности Российской Федерации”.
Структура ФСБ России:

- Департамент контрразведки
- Департамент по борьбе с терроризмом
- Департамент анализа, прогноза и стратегического планирования
- Департамент по организационно-кадровой работе
- Департамент обеспечения деятельности
- Управление разработки и пресечения деятельности преступных организаций
- Следственное управление
- Оперативно-поисковое управление
- Управление оперативно-технических мероприятий
- Управление собственной безопасности
- Управление делами
- Следственный изолятор
- Научно-исследовательский центр

29.Указ Президента РФ № 793 от 29 июля 1997 года.
“Об изменении структуры аппарата Совета Безопасности Российской Федерации” (СЗ РФ № 31-97, ст. 3673).
Утвердил структуру аппарата Совета Безопасности Российской Федерации.
Отменен Указом Президента РФ № 294 от 28 марта 1998 года.

30.Указ Президента РФ № 793 от 29 июля 1997 года.
“О научном совете при Совете Безопасности Российской Федерации” (СЗ РФ № 31-97, ст. 3675).
Утвердил Положение о научном совете при Совете Безопасности Российской Федерации и персональный состав Совета.
Отменен Указом Президента РФ № 294 от 28 марта 1998 года

31.Указ Президента РФ № 1037 от 19 сентября 1997 года.
“О межведомственных комиссиях Совета Безопасности Российской Федерации” (СЗ РФ № 32, ст.4527)**.**
Утвердил “**Положения:**

- О Межведомственной комиссии СБ РФ по проблемам оборонно-промышленного комплекса
- О Межведомственной комиссии СБ РФ по оборонной безопасности
- О Межведомственной комиссии СБ РФ по охране здоровья населения
- О Межведомственной комиссии СБ РФ по федеральной конституционной безопасности
- О Межведомственной комиссии СБ РФ по информационной безопасности
- О Межведомственной комиссии СБ РФ по пограничной политике
- О Межведомственной комиссии СБ РФ по экологической безопасности
- О Межведомственной комиссии СБ РФ по международной безопасности
- О Межведомственной комиссии СБ РФ по защите прав граждан и общественной безопасности, борьбе с преступностью и коррупцией
- О Межведомственной комиссии СБ РФ по экономической безопасности

33.Указ Президента РФ № 1300 от 17 декабря 1997 года.
Утвердил **“Концепцию национальной безопасности Российской Федерации”.**

Национальные интересы России в информационной сфере обусловливают необходимость сосредоточения усилий общества и государства на решении таких задач, как соблюдение конституционных прав и свобод граждан в области получения информации и обмена ею, защита национальных духовных ценностей, пропаганда национального культурного наследия, норм морали и общественной нравственности, обеспечение права граждан на получение достоверной информации, развитие современных телекоммуникационных технологий. Планомерная деятельность государства по реализации этих задач позволит Российской Федерации стать одним из центров мирового развития в

XXI веке. В то же время недопустимо использование информации для манипулирования массовым сознанием. Необходима защита государственного информационного ресурса от утечки важной политической, экономической, научно-технической и военной информации.

Важнейшие задачи обеспечения национальной безопасности Российской Федерации в информационной сфере:

- установление необходимого баланса между потребностью в свободном обмене информацией и допустимыми ограничениями ее распространения;
- совершенствование информационной структуры, ускорение развития новых информационных технологий и их широкое распространение, унификация средств поиска, сбора, хранения, обработки и анализа информации с учетом вхождения России в глобальную информационную структуру;
- разработка соответствующей нормативно-правовой базы и координация, при ведущей роли Федерального агентства правительственной связи и информации при Президенте Российской Федерации (ФАПСИ), деятельности федеральных органов государственной власти и других органов, решающих задачи обеспечения информационной безопасности;
- развитие отечественной индустрии телекоммуникационных и информационных средств, их приоритетное по сравнению с зарубежными аналогами распространение на внутреннем рынке;
- защита государственного информационного ресурса, прежде всего в федеральных органах государственной власти и на предприятиях оборонного комплекса.

34.Указ Президента РФ № 61 от 24 января 1998 года.

“О перечне сведений, отнесенных к государственной тайне” (СЗ РФ № 5-98, ст. 561)**.** Излагает Перечень сведений (См. Указ № 1203 от 30 ноября 1995 г. - СЗ РФ 49-95, ст. 4775) в новой редакции.

35.Указ Президента РФ № 294 от 28 марта 1998 года.

“Об аппарате Совета Безопасности Российской Федерации” (СЗ РФ 14-98, ст. 1536)**.**

Утвердил “**Положение об аппарате Совета Безопасности Российской Федерации”.**

34.Указ Президента РФ № 318 от 30 марта 1998 года.

“О продлении срока реализации Государственной программы обеспечения зашиты государственной тайны в Российской Федерации на 1996 - 1997 годы” (СЗ РФ № 14-98, ст. 1541).

Продлевает на 1998 год срок реализации Программы (Указ Президента РФ № 346 от 9 марта 1996 года).

35.Распоряжение Президента РФ № 74-рп от 11 февраля 1994 года.

“О контроле за экспортом из Российской Федерации отдельных видов сырья, материалов, оборудования, технологий и научно-технической информации, которые могут быть применены при создании вооружения и военной техники”.

36.Распоряжение Президента РФ № 226-рп от 30 мая 1997 года.

Утверждает **“Перечень должностных лиц, органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне”**.

Всего полномочиями по отнесению сведений к государственной тайне наделены на 30 мая 1997 года следующие должностные лица:

- Министр РФ по атомной энергии
- Министр внешних экономических связей и торговли РФ
- Министр РФ по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий
- Министр здравоохранения РФ
- Министр иностранных дел РФ
- Министр науки и технологий РФ
- Министр общего и профессионального образования РФ
- Министр обороны РФ
- Министр природных ресурсов РФ
- Министр путей сообщения РФ
- Министр сельского хозяйства и продовольствия РФ
- Министр топлива и энергетики РФ
- Министр транспорта РФ
- Министр финансов РФ
- Министр экономики РФ
- Председатель Госкомрезерва России
- Председатель Госстроя России

- Председатель Госкомзема России
- Председатель Гскомэкологии России
- Председатель Госкомсвязи России
- Председатель Госстандарта России
- Председатель ГТК России
- Директор ФПС России
- Директор ФСБ России
- Директор СВР России
- Руководитель Роскартографии
- Руководитель ФСНП России
- Руководитель ФСО России
- Руководитель Росгидромета
- Генеральный директор РКА
- Генеральный директор ФАПСИ
- Руководитель Администрации Президента РФ
- Начальник Главного управления специальных программ Президента РФ
- Председатель Гостехкомиссии России
- Председатель Банка России

Утратили силу Указы Президента РФ № 73-рп от 11.02.94; № 331-рп от 27.06.94; № 537-рп от 24.10.94; № 290-рп от 6.06.96; № 333-рп от 21.06.96.

3. Постановления и распоряжения государственных органов

1. Постановление Совета Министров СССР № 556-126 от 12 мая 1987 года
   Об утверждении **“Инструкции по обеспечению режима секретности в Министерствах и ведомствах, на предприятиях, в учреждениях и организациях СССР” (Инструкции № 0126-87).**
2. Постановление Верховного Совета СССР № 2195-1 от 28 мая 1991 года.
   “О видах деятельности, которыми предприятия вправе заниматься только на основании специальных разрешений (лицензий)”.
3. Постановление Правительства РСФСР № 35 от 5 декабря 1991 года.
   “О перечне сведений, которые не могут составлять коммерческую тайну”.
4. Постановление Правительства РФ № 190 от 25 марта 1992 года.
   “Об организации в Российской Федерации обмена информацией о чрезвычайных ситуациях”.
5. Постановление Правительства РФ № 305 от 8 мая 1992 года.
   “О государственной регистрации ведомственных нормативных актов”.
   Вводит **“Положение о порядке государственной регистрации ведомственных нормативных актов”.**
6. Постановление Правительства РФ № 854 от 6 ноября 1992 года.
   “О лицензировании и квотировании экспорта и импорта товаров (работ, услуг) на территории Российской Федерации”
   Внесены изменения и дополнения Постановлением Правительства РФ № 331 от 15 апреля 1994 года.
7. Постановление Правительства РФ № 959 от 10 декабря 1992 года.
   “О поставках продукции и отходов производства, свободная реализация которых запрещена”.
   Вводит соответствующее **Положение.**
   Внесены изменения и дополнения Постановлением Правительства РФ № 331 от 15 апреля 1994 года.
8. Постановление Правительства РФ № 307 от 13 апреля 1993 года.
   “О регистрации и опубликовании ведомственных нормативных актов”.
9. Постановление Совета Министров - Правительства РФ № 722 от 23 июля 1993 года.
   “Об утверждении Правил подготовки ведомственных нормативных актов”.

10. Постановление Совета Министров - Правительства РФ № 912-51 от 15 сентября 1993 года.
“О государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам”.
Вводит соответствующее **Положение.**

11. Постановление Правительства РФ № 197 от 10 марта 1994 года.
“Об утверждении Положения о порядке контроля за экспортом из Российской Федерации отдельных видов сырья, материалов, оборудования, технологий и научно-технической информации, которые могут быть применены при создании вооружения и военной техники”.

12. Постановление Правительства РФ № 331 от 15 апреля 1994 года.
“О внесении дополнений и изменений в Постановления Правительства РФ № 854 от 6 ноября 1992 года “О лицензировании и квотировании экспорта и импорта товаров (работ, услуг) на территории Российской Федерации” и № 959 от 10 декабря 1992 года “О поставках продукции и отходов производства, свободная реализация которых запрещена”.

13. Постановление Правительства РФ № 758 от 1 июля 1994 года.
“О мерах по совершенствованию государственного регулирования экспорта товаров и услуг”.

14. Постановление Правительства РФ № 870 от 4 сентября 1994 года.
О степенях секретности сведений - название условно.

15. Постановление Правительства РФ № 1161 от 14 октября 1994 года.
“О порядке и условиях выплаты процентных надбавок к должностному окладу (тарифной ставке) должностных лиц и граждан, допущенных к государственной тайне”.
Порядок выплаты надбавок разъяснен Постановлением Министерства труда РФ № 84 от 23 декабря 1994 года (в рублях) и Постановлением Министерства труда РФ № 15 от 1 марта 1996 года (в валюте).

16. Постановление Правительства РФ № 1233 от 3 ноября 1994 года.
“О порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти”.
Вводит соответствующее **Положение.**
Нормативный акт, регламентирующий порядок обращения с документами *“для служебного пользования”*.

17. Постановление Правительства РФ № 1319 от 1 декабря 1994 года.
“Об информационном обеспечении предпринимательства в Российской Федерации”.
Принято решение о создании АО “Российские информационные центры”.

18. Постановление Правительства РФ № 1418 от 24 декабря 1994 года.
“О лицензировании отдельных видов деятельности”.
Вводит соответствующее **Положение.**

19. Постановление Правительства РФ № 170 от 20 февраля 1995 года.
“О порядке рассекречивания и продления сроков засекречивания архивных документов Правительства СССР”.
Вводит соответствующее **Положение.**

20. Постановление Правительства РФ № 333 от 15 апреля 1995 года.

“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”.
Вводит соответствующее **Положение.**
Внесены дополнения Постановлением Правительства РФ № 509 от 23 апреля 1996 года и Постановлением Правительства РФ № 513 от 30 апреля 1997 года.

21. Постановление Правительства РФ № 870 от 4 сентября 1995 года.
Утвердило **“Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности”**.

22. Постановление Правительства РФ № 608 от 15 сентября 1995 года.
“О сертификации средств защиты информации”.
Вводит соответствующее **Положение.**

23. Постановление Правительства РФ № 1050 от 28 октября 1995 года.
“Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне” (СЗ РФ № 43-97, ст. 4987).
Вводит соответствующую **Инструкцию.**

24. Постановление Правительства РФ № 203 от 28 февраля 1996 года.
“О персональном составе Межведомственной комиссии по защите государственной тайны ” (СЗ РФ № 12-96, ст. 1106; № 28-96, ст. 3395; № 45-96, ст. 1997; № 20-97, ст. 2312; № 23-97, ст. 2704; № 29-97, ст. 3551; № 48-97, ст. 5566)**.**
С изменениями:
Постановление Правительства РФ № 1195 от 19.09.97 (СЗ РФ № 39-97, ст. 4547) - введен Заместитель Руководителя Администрации Президента РФ - заведующий Канцелярией Президента РФ Семенченко В.П.

25. Постановление Правительства РФ № 226 от 28 февраля 1996 года.
“О государственном учете и регистрации баз и банков данных”.

26. Постановление Правительства РФ № 758 от 1 июля 1996 года.
“О мерах по совершенствованию государственного регулирования экспорта товаров и услуг”.

27. Постановление Правительства РФ № 1299 от 31 октября 1996 года.
“О порядке лицензирования экспорта и импорта товаров (работ, услуг) в Российской Федерации”.
Вводит соответствующее **Положение.**

28. Постановление Правительства РФ № 242 от 3 марта 1997 года.
“О назначении российского органа по защите информации, которой защите информации, которой обмениваются Российская Федерация и Организация Североатлантического договора, и создании Центральной службы регистрации и контроля документов, которыми обмениваются Российская Федерация и Организация Североатлантического договора” (СЗ РФ № 10-97, ст. 1182)**.**
Функции по защите информации возложены на ФСБ России.
Центральная служба регистрации и контроля создана при МИД России.

29. Постановление Правительства РФ № 513 от 30 апреля 1997 года.
“О внесении дополнения в Положение о лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты ин-

формации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны".

В связи с созданием в Министерстве обороны РФ системы сертификации средств защиты информации, предусмотренной Постановлением Правительства РФ № 608 от 26 июня 1995 года "О сертификации средств защиты информации":

Дополнить абзац 3 пункта 2, абзацы 2 и 5 пункта 10 Положения 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, утвержденного Постановлением Правительства РФ № 333 от 15 апреля 1995 года после слов: "Служба внешней разведки РФ" словами: "Министерство обороны РФ".

30. Постановление Правительства РФ от 14 июля 1997 года № 882.

"Об утверждении Положения о Государственном комитете Российской Федерации по связи и информатизации "(СЗ РФ № 29-97, ст. 3540)**.**

ГК РФ по связи и информатизации в соответствии с возложенными на него задачами:

5) проводит мероприятия в области безопасности функционирования связи и систем информатизации РФ;
6) осуществляет в установленном порядке сертификацию технических средств и услуг связи и информатизации (за исключением радиоэлектронных средств, используемых Минобороны, ФСБ, ФПС, СВР, МВД, ФАПСИ и др.);
11) осуществляет в установленном порядке выдачу лицензий юридическим и физическим лицам лицензий на виды деятельности, связанные с предоставлением услуг связи и информатизации ...;

31. Постановление Правительства РФ от 14 июля 1997 года № 883.

"Об утверждении Положений о Государственной комиссии по радиочастотам, Государственной комиссии по электросвязи и Государственной комиссии по информатизации при Государственном комитете Российской Федерации по связи и информатизации "(СЗ РФ № 29-97, ст. 3541)**.**

Государственная комиссия по радиочастотам при Государственном комитете Российской Федерации по связи и информатизации

Комиссия в целях выполнения возложенных на нее задач:

к) согласовывает общие требования к средствам и системам активной защиты информации и средствам информатики общего назначения в части их электромагнитной совместимости с другими радиоэлектронными средствами.

Государственная комиссия по электросвязи при Государственном комитете Российской Федерации по связи и информатизации

Комиссия в целях выполнения возложенных на нее задач:

и) согласовывает выдачу лицензий на виды деятельности по связи на территории РФ;
к) координирует вопросы сопряжения технических средств взаимоувязанной сети связи РФ со средствами защиты информации.

Государственная комиссия по информатизации при Государственном комитете Российской Федерации по связи и информатизации

Комиссия в целях выполнения возложенных на нее задач:

в) разрабатывает предложения по обеспечению единой государственной политики в области сертификации средств и систем информатизации и их реализации;
и) организует учет государственных информационных ресурсов и контроль за их использованием.

32. Постановление Правительства РФ от 24 июля 1997 года № 950.

"Об утверждении Положения о государственной системе научно-технической информации "(СЗ РФ № 31-97, ст. 3696)**.**

33. Постановление Правительства РФ от 2 августа 1997 года № 973.

"Об утверждении Положения о подготовке к передаче сведений, составляющих государственную тайну, другим государствам "(СЗ РФ № 31-97, ст. 3786)**.**

34.Постановление Правительства РФ № 220 от 3 марта 1998 года.
“О некоторых мерах по совершенствованию государственного управления в области обороны и безопасности” (СЗ РФ № 10-98, ст. 1155)
Упраздняет Совет обороны Российской Федерации и объединяет Совет безопасности РФ с Государственной военной инспекцией Президента РФ.

35.Распоряжение Правительства РФ от 1994 года.
Утверждает **“План разработки первоочередных нормативных документов по защите государственной тайны с финансированием из федерального бюджета”.**

36.Постановление Конституционного суда РФ № 8-П от 27 марта 1996 года.
“О непротиворечии Закона РФ “О государственной тайне” нормам Конституции РФ и общепризнанным принципам демократического правового государства”.

37.Информационное письмо Высшего арбитражного суда РФ № С-13/ОСЗ-317 от 19 октября 1993 года.
“Об авторском праве и смежных правах”.

38.Информационное письмо Высшего арбитражного суда РФ № С1-7/03-316 от 7 июня 1995 года.
“О Федеральном законе “Об информации, информатизации и защите информации”.

4. Межведомственные документы

1. **“Положение по категорированию объектов ЭВТ на территории СССР”** от 3 апреля 1981 года.
2. **“Руководящий документ. Концепция защиты СВТ и АС от НСД к информации”**.- Гостехкомиссия России, 30 марта 1992 года.
3. **“Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации”**.- Гостехкомиссия России, 30 марта 1992 года.
4. **“Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации”**.- Гостехкомиссия России, 30 марта 1992 года.
5. **“Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД в автоматизированных системах и средствах вычислительной техники”**.- Гостехкомиссия России, 30 марта 1992 года.
6. **“Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения”**.- Гостехкомиссия России, 30 марта 1992 года.
7. **“Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации”.-** Гостехкомиссия России, 1997.

8. **“Об утверждении Правил составления, подачи и рассмотрения заявок на официальную регистрацию программирования электронных вычислительных машин и баз данных”.**
   Приказ Российского агентства по правовой охране программ для ЭВМ, баз данных и топологий интегральных микросхем № 7п от 5 марта 1993 года.
   (Рег. № 181 от 17 марта 1993 года. РВ 25.03.93 № 57/7)

9. **“Об утверждении Правил составления, подачи и рассмотрения заявок на официальную регистрацию топологий интегральных микросхем ”.**
   Приказ Российского агентства по правовой охране программ для ЭВМ, баз данных и топологий интегральных микросхем № 8п от 5 марта 1993 года.
   (Рег. № 182 от 17 марта 1993 года. РВ 1.04.93 № 62)

10. **“Об утверждении Правил регистрации договоров на программы для электронных вычислительных машин, базы данных и топологии интегральных микросхем”.**
    Приказ Российского агентства по правовой охране программ для ЭВМ, баз данных и топологий интегральных микросхем № 9п от 5 марта 1993 года.
    (Рег. № 183 от 17 марта 1993 года. РВ 3.03.93 № 64/9)

11. **“О пропуске информационных материалов”.**
    Указание Государственного таможенного комитета РФ от 27 января 1993 года.
    (Рег. № 186 от 22 марта 1993 года. БНА-6-93. РВ 1.04.93 № 62/8)

12. **“Положение о Государственном лицензировании деятельности в области защиты информации”.**
    Одобрено Решением Гостехкомиссии России от 21 сентября 1993 года № 4.

13. **“Положение о сертификации средств и систем вычислительной техники и связи по требованиям безопасности информации”.**
    Одобрено Решением Гостехкомиссии России от 21 сентября 1993 года № 4.

14. **“Основы концепции защиты информации от иностранных технических разведок и от ее утечки по техническим каналам”**.
    Одобрены Решением Гостехкомиссии России от 16 ноября 1993 года № 6.

15. **“Временные рекомендации по организации работ по защите информации в региональных органах государственной власти”**.
    Одобрены Решением Гостехкомиссии России от 16 ноября 1993 года № 6.

16. **“Правила по проведению сертификации в Российской Федерации”.**
    Утверждены Постановлением Госстандарта России № 3 от 16 февраля 1994 года.
    (Рег. № № 521 от 21 марта 1994 года. БНА-6-94. РВ 30.03.94 № 56)

17. **“О совершенствовании контроля за ввозом и вывозом лицензируемых товаров”.**
    Приказ Государственного таможенного комитета РФ № 230 от 26 мая 1994 года.
    (Рег. № 596 от 9 июня 1994 года. БНА-9-94. РВ 6.07.94 №123)

18. **“Порядок ввоза на территорию Российской Федерации товаров, подлежащих обязательной сертификации”.**
    Приказ Государственного таможенного комитета РФ № 217 от 23 мая 1994 года.
    (Рег. № 599 от 14 июня 1994 года. БНА-9-94. РВ 29.06.94 № 118)

19. **“Положение о государственном лицензировании деятельности в области защиты информации”**.
    Утверждено совместным решением Гостехкомиссии России и ФАПСИ от 27 апреля 1994 года № 10.

Приложение.

- Перечень видов деятельности предприятий в области защиты информации, подлежащих лицензированию Гостехкомиссией России.
- Перечень видов деятельности предприятий в области защиты информации, подлежащих лицензированию ФАПСИ России.

20. **“Об утверждении Порядка проведения сертификации продукции в Российской Федерации”.**
Постановление Госкомстата России № 15 от 21 сентября 1994 года.
(Рег. № 826 от 5 апреля 1995 года. БНА-7-95. РВ 1.06.95 № 100)

21. **“Справочник по подготовке и оформлению официальных документов”.**
Утвержден Распоряжением Руководителя Администрации Президента РФ № 2385 от 17 декабря 1994 года.

22. **“Об утверждении Разъяснения “О порядке выплаты процентных надбавок должностным лицам и гражданам, допущенным к государственной тайне”.**
Постановление Министерства труда РФ № 84 от 23 декабря 1994 года.
(Рег. № 766 от 28 декабря 1994 года. БНА-4-95. РВ 30.03.95 № 58)

23. **“Типовое положение о подразделении по защите информации от иностранных технических разведок и от ее утечки по техническим каналам на предприятии”.**
Одобрено Решением Гостехкомиссии России № 32 от 1 марта 1995 года.

24. **“Инструкция о порядке проведения специальных экспертиз по допуску предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну” (Инструкция № 28).**
Утверждена Директором ФСБ РФ 23 августа 1995 года, № 28. (Согласована с Гостехкомиссией РФ и ФАПСИ).

25. **“Правила проведения сертификации средств индивидуальной защиты”.**
Утверждены Госкомстатом России 31 марта 1995 года.
(Рег. № 941 от 28 августа 1995 года. РВ 12.10.95 № 194)

26. **“Положение о порядке внесения и размерах платы за оформление лицензий в области связи в Российской Федерации”.**
Утверждено Министерством связи РФ от 24 апреля 1995 года.
(Рег. № 854 от 12 мая 1995 года. БНА-8-95. РВ 22.06.95 №114)

27. **“О документах по организации и проведению государственной аттестации руководителей предприятий, учреждений и организаций, ответственных за защиту сведений, составляющих государственную тайну”**.
Решение Межведомственной комиссии по защите государственной тайны № 3 от 13 марта 1996 года.
Приложения.

- Методические рекомендации по организации и проведению государственной аттестации руководителей предприятий, учреждений и организаций, ответственных за защиту сведений, составляющих государственную тайну.
- Перечень учебных заведений, осуществляющих подготовку специалистов по вопросам защиты информации, составляющей государственную тайну, свидетельство об окончании которых дает руководителям предприятий, учреждений и организаций право на освобождение от государственной аттестации.

28. Решение Межведомственной комиссии по защите государственной тайны № 9 от 24 сентября 1996 года.

29. **“Инструкция по документационному обеспечению (делопроизводству) в Администрации Президента Российской Федерации”.**
Утверждена Распоряжением Руководителя Администрации Президента РФ № 1418 от 2 августа 1997 года.

30. **“О защите информации при вхождении России в международную информационную систему Internet”.**
Рекомендации Гостехкомиссии России от 21 октября 1997 года.
Рекомендовано:
4.“... подготовить и опубликовать в 1998 году *аналитический обзор сертифицированных средств защиты информации*, которые могут быть использованы при подключении к международным информационным системам, включая сеть Internet”.

31. **“О возможности использования зарубежных программных продуктов в автоматизированных системах информационной поддержки госучреждений с учетом требований по безопасности. Состояние работ по изучению данных продуктов и перспективы их сертификации”.**
Решение Председателя Гостехкомиссии России.

32. **“Положение об испытательном центре (лаборатории) средств криптографической защиты информации (ИЦ СКЗИ), аккредитованном ФАПСИ на испытания СКЗИ по требованиям безопасности информации”.**

33. **“Положение о лицензировании деятельности в области связи в Российской Федерации”.**

34. **“Временное положение об аттестационном центре ФАПСИ, аккредитованном на проведение работ в области защиты информации”.**

35. **“Положение о Региональном Аттестационном центре специальной экспертизы”**. Утверждено Начальником Управления Федеральной службы безопасности РФ по г. Санкт-Петербургу и Ленинградской области 27 декабря 1995 года.
Статус РАЦСЭ получило **Государственное унитарное предприятие Специальное агентство экспертизы, лицензирования, сертификации и аттестации “ОМЕГА”**
195220, г. Санкт-Петербург, ул. Обручевых, 1
тел. (812) 247-57-01

5. Основные государственные и отраслевые стандарты

1. **“Единая государственная система делопроизводства (ЕСГД)”**, 1975 года.

2. ГОСТ 6.10.4-84.
“Унифицированные системы документации. Придание юридической силы документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники. Основные положения”.

3. ГОСТ 1.5-85.
“Государственная система стандартизации и построение и изложение, оформление и содержание стандартов”.

4. ГОСТ 28147-89.
“Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования”.
Введен в действие с 1 июля 1990 года.

5. ГОСТ 6.38-90.
“Унифицированные системы документации (УСД). Система организационно-распорядительной документации. Требования к составлению и оформлению документов”.

6. ГОСТ 29339-92.
“Информационная технология. Защита информации от утечки за счет ПЭМИН при ее обработке средствами вычислительной техники. ОТТ”.

7. Система сертификации ГОСТ Р.
“Порядок проведения сертификации продукции в Российской Федерации”.
Утверждены Постановлением Госстандарта России № 15 от 21 сентября 1994 года.

Зарегистрирован в Минюсте России № 826 от 5 апреля 1995 года.
Внесены изменения № 1, принятые Постановлением Госстандарта России № 15 от 25 июля 1996 года и зарегистрированные Минюстом России № 1139 от 1 августа 1996 года.

8. Система сертификации ГОСТ Р.
“Основные положения и порядок сертификации услуг”.
Утверждены Постановлением Госстандарта России № 24 от 29 декабря 1993 года.
Зарегистрированы в Госреестре № РОСС RU.0001.010006 от 27 сентября 1994 года.
Дата введения 1 апреля 1994 года.

9. РОСС.RU.0001.01БИ00.
“Система сертификации средств защиты информации по требованиям безопасности информации”.

10. РОСС.RU.0001.030001.
“Система сертификации средств криптографической защиты информации (Система сертификации СКЗИ)”.
Зарегистрирован (ФАПСИ) в Госстандарте 15 ноября 1993 года.

11. ГОСТ 34.003-90.
“Информационная технология. Комплекс стандартов на АС. Термины и определения”.

12. ГОСТ 34.602-89.
“Информационная технология. Комплекс стандартов на АС. Техническое задание на создание автоматизированной системы”.

13. ГОСТ 34.201-89.
“Информационная технология. Комплекс стандартов на АС. Виды, комплектность и обозначение документов при создании АС”.

14. ГОСТ 23773-88.
“Машины вычислительные электронные цифровые общего назначения. Методы испытаний”.

15. ГОСТ В.15.211-78.
“СРПП ВТ. Порядок разработки программ и методик испытаний опытных образцов изделий”.

16. ГОСТ 16325-88.
“Машины вычислительные электронные цифровые общего назначения. ОТТ.”

17. ГОСТ 21552-84.
“СВТ. ОТТ, приемка, методы испытаний, маркировка, упаковка, транспортировка и хранение”.

18. ГОСТ 27201-87.
“Машины вычислительные электронные персональные. Типы, основные параметры, ОТТ”.

19. ГОСТ 28388-89.
“Системы обработки информации. Документы на магнитных носителях данных. Порядок выполнения и обращения”.

20. ГОСТ Р В 50170-92.
“Противодействие ИТР. Термины и определения”.

21.ГОСТ 28689-90.
“Радиопомехи от ПЭВМ. Нормы и методы испытаний”.

22.ГОСТ Р.34.10-94.

23.**“Системы обработки информации. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма”.**

24.ГОСТ Р.34.11-94.
“Системы обработки информации. Криптографическая защита информации. Функция хеширования”.