

МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФБГОУ ВПО «Кубанский государственный аграрный университет»

Факультет прикладной информатики
Кафедра компьютерных технологий и систем

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Справочник для бакалавров специальности
« Бизнес-информатика»

Краснодар
2013

УДК 004
ББК 32.81 я 7
И72

Рецензенты:

- доктор технических наук, профессор Атрощенко В.А. – декан факультета компьютерных технологий и автоматизированных систем ФГОУ ВПО "Кубанский государственный технологический университет";
- доктор экономических наук, профессор Луценко Е.В. – профессор кафедры компьютерных технологий и систем ФГБОУ ВПО "Кубанский государственный аграрный университет".

Лаптев В.Н.

Информационная безопасность: Справочник для бакалавров специальности «Бизнес-информатика». / В.Н. Лаптев, С.В. Лаптев – Краснодар: КубГАУ, 2013. - 142 с.

В справочнике по представлены основные термины и определения, используемые в дисциплинах «Информационная безопасность». Он подготовлен для облегчения усвоения бакалаврами ФПИ КубГАУ теоретических и прикладных аспектов этой дисциплины в соответствии с требованиями ФГОС ВПО по специальности «Бизнес-информатика». информатика студентами и бакалаврами факультета прикладной информатики ФГОУ ВПО "Кубанский государственный аграрный университет" (КубГАУ).

Он является обязательным приложением к курсу лекций и практикуму по дисциплине, так как обеспечивает качественное проведение лабораторных занятий и выполнение самостоятельной работы обучаемыми по учебному курсу.

Рассмотрены и рекомендованы к изданию на заседании кафедры компьютерных технологий и систем КубГАУ __ сентября 2013 г., протокол №1.

Рекомендованы к печати:

- Советом факультета прикладной информатики Кубанского государственного аграрного университета __ сентября 2013 г., протокол № .

© Лаптев Владимир Николаевич, Лаптев Сергей Владимирович

© Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования "Кубанский государственный аграрный университет", 2013.

Оглавление

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ	4
2. ВЫПИСКА ИЗ "КОДЕКСА РФ ОБ АДМИНИСТРАТИВНЫХ ПРАВОНАРУШЕНИЯХ"	14
3. ЗАКОН РФ ОТ 5 МАРТА 1992 Г. N 2446-1 "О БЕЗОПАСНОСТИ"	15
3. ЗАКОН РФ ОТ 21.06.1993 Г. № 5485-1 "О ГОСУДАРСТВЕННОЙ ТАЙНЕ"	23
П-06. ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ	40
П-07. ДОКТРИНА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РФ	44
П-08. ПЕРЕЧЕНЬ СВЕДЕНИЙ, ОТНЕСЕННЫХ К ГОСУДАРСТВЕННОЙ ТАЙНЕ	69
П-09. ОБ УТВЕРЖДЕНИИ ПЕРЕЧНЯ СВЕДЕНИЙ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА	79
П-10. ПОЛОЖЕНИЕ О ЛИЦЕНЗИРОВАНИИ ДЕЯТЕЛЬНОСТИ ПО ТЕХНИЧЕСКОЙ ЗИ	80
П-11. ИНСТРУКЦИЯ ПО ЗИ ПРИ РАБОТЕ С ЗАРУБЕЖНЫМИ ПАРТНЕРАМИ	83
П-12. ОБЕСПЕЧЕНИЕ СОХРАННОСТИ КОММЕРЧЕСКОЙ ТАЙНЫ ПРЕДПРИЯТИЯ	87
1. Договорное обязательство	94
2. Журнал учета документов и изданий с грифом «Коммерческая тайна» (Форма № 1)	94
3. Карточка учета входящих (исходящих) документов и изданий с грифом «КТ» (Форма № 2)	95
4. Журнал учета и распределения изданий с грифом «КТ» (Форма № 3)	95
5. Карточка учета выдаваемых дел и изданий с грифом «КТ» (Форма № 4)	96
6. Журнал учета служебных изданий с грифом «КТ» (Форма № 5)	96
7. Типовой договор на комплексное режимное обслуживание	96
8. Типовой акт приемки выполнения договорных обязательств	97
П-13. КАТАЛОГ ОБОБЩЕННЫХ МЕРОПРИЯТИЯ ПО ЗИ	98
1. Мероприятия по предупреждению разглашения конфиденциальной информации	98
2. Мероприятия по защите информации от утечки по техническим каналам	101
3. Мероприятия по пресечению НСД к конфиденциальной информации	103
П-14. СПЕЦИАЛЬНЫЕ ТРЕБОВАНИЯ ГОСТЕХКОМИССИИ ПО ТЕХНИЧЕСКОЙ ЗИ	107
1. Акт классификации автоматизированной системы обработки информации	135
2. Аттестат соответствия на АС	135
3. Аттестат соответствия на защищаемое помещение	136
4. Технический паспорт на защищаемое помещение	137
5. Технический паспорт на АС	138
6. Документальное оформление перечня сведений конфиденциального характера	139
7. Основные нормативные правовые акты и методические документы по ЗИ	139

1. Термины и определения

В настоящем справочнике приведены термины и определения понятий в области информационной безопасности (при защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации). Представленные установленные термины обязательны для применения во всех видах документации по информационной безопасности (ИБ). Для каждого понятия установлен один термин. Применение синонимов термина в ИБ не допускается. Для отдельных терминов даны (в скобках) краткие формы, которые разрешается применять в случаях, исключающих возможность их различного толкования.

Для справок приведены иностранные эквиваленты русских терминов на английском языке, а также алфавитные указатели терминов на русском и английском языках.

Администратор защиты /Security administrator/ - Субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации.

Аутентификация /Authentication/ - Проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности.

Безопасность - состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.

Безопасность информации /Information security/ - Состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз.

Верификация /Verification/ - Процесс сравнения двух уровней спецификации средств вычислительной техники или автоматизированных систем на надлежащее соответствие.

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.

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

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.

Диспетчер доступа (ядро защиты) /Security kernel/ - Технические, программные и микропрограммные элементы комплекса средств защиты, реализующие концепцию диспетчера доступа.

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 информации (Доступ) /Access to information/ - Ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации.

Доступ к сведениям, составляющим государственную тайну - санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну.

Жизненно важные интересы - совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства.

Законодательные основы обеспечения безопасности составляют

- Конституция РСФСР, - настоящий Закон, законы и другие нормативные акты Российской Федерации, регулирующие отношения в области безопасности;
- конституции, законы, иные нормативные акты республик в составе Российской Федерации и нормативные акты органов государственной власти и управления краев, областей, автономной области и автономных округов, принятые в пределах их компетенции в данной сфере;
- международные договоры и соглашения, заключенные или признанные Российской Федерацией.

Защита от несанкционированного доступа (Защита от НСД) /Protection from unauthorized access/ - Предотвращение или существенное затруднение несанкционированного доступа

Защищенное средство вычислительной техники (защищенная автоматизированная система) /Trusted computer system/ - Средство вычислительной техники (автоматизированная система), в котором реализован комплекс средств защиты.

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.

Идентификатор доступа /Access identifier/ - Уникальный признак субъекта или объекта доступа

Идентификация /Identification/ - Присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

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.

Концепция диспетчера доступа /Reference monitor concept/ - Концепция управления доступом, относящаяся к абстрактной машине, которая посредничает при всех обращениях субъектов к объектам.

Конфиденциальная информация /Sensitive information/ - Информация, требующая защиты.

Мандатное управление доступом //Mandatory access control/ - Разграничение доступа субъектов к объектам, основанное на характеризующей метке конфиденциальности информации, содержащейся в объектах, и официальном разрешении (допуске) субъектов обращаться к информации такого уровня конфиденциальности.

Матрица доступа /Access matrix/ - Таблица, отображающая правила разграничения доступа.

Метка конфиденциальности (Метка) /Sensitivity label/ - Элемент информации, который характеризует конфиденциальность информации, содержащейся в объекте.

Модель защиты /Protection model/ - Абстрактное (формализованное или неформализованное) описание комплекса программно-технических средств и (или) организационных мер защиты от несанкционированного доступа.

Модель нарушителя правил разграничения доступа (Модель нарушителя ПРД) /Security policy violator's model/ - Абстрактное (формализованное или неформализованное) описание нарушителя правил разграничения доступа.

Многоуровневая защита /Multilevel security/ - Защита, обеспечивающая разграничение доступа субъектов с различными правами доступа к объектам различных уровней конфиденциальности.

Нарушитель правил разграничения доступа (Нарушитель ПРД) /Security policy violator/ - Субъект доступа, осуществляющий несанкционированный доступ к информации.

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

Примечание. Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения средств вычислительной техники или автоматизированных систем.

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.

Обеспечение безопасности – это непрерывное поддержание состояния защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз (т.е. безопасности). Безопасность достигается проведением *единой государственной политики* в области обеспечения безопасности, системой мер экономического, политического, организационного и иного характера, адекватных угрозам жизненно важным интересам личности, общества и государства.

Для создания и поддержания необходимого уровня защищенности объектов безопасности в Российской Федерации *разрабатывается система правовых норм*, регулирующих отношения в сфере безопасности, определяются основные направления деятельности органов государственной власти и управления в данной области, формируются или преобразуются органы обеспечения безопасности и механизм контроля и надзора за их деятельностью.

Для непосредственного выполнения функций по обеспечению безопасности личности, общества и государства в системе исполнительной власти в соответствии с законом *образуются государственные органы обеспечения безопасности*.

Объекты безопасности – это в основном:

- *личность* - ее права и свободы;
- *общество* - его материальные и духовные ценности;
- *государство* - его конституционный строй, суверенитет и территориальная целостность.

Объект доступа (Объект) /Access object/ - Единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

Органы защиты государственной тайны – это:

- *межведомственная комиссия* по защите государственной тайны;
- *органы федеральной исполнительной власти* (Федеральная служба 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.

Межведомственная комиссия по защите государственной тайны является коллегиальным органом, координирующим деятельность органов государственной власти по защите государственной тайны в интересах разработки и выполнения государственных программ нормативных и методических документов, обеспечивающих реализацию законодательства Российской Федерации о государственной тайне. Функции межведомственной комиссии по защите государственной тайны и ее надведомственные полномочия реализуются в соответствии с Положением о межведомственной комиссии по защите государственной тайны, утверждаемым Президентом Российской Федерации.

Указом Президента РФ от 30 марта 1994 г. № 614 функции межведомственной комиссии по защите государственной тайны временно возложены на Государственную техническую комиссию при Президенте Российской Федерации.

Органы федеральной исполнительной власти (Федеральная служба безопасности Российской Федерации, Министерства 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 организуют и обеспечивают защиту государственной тайны в соответствии с функциями, возложенными на них законодательством Российской Федерации.

Органы государственной власти, предприятия, учреждения и организации обеспечивают защиту сведений, составляющих государственную тайну, в соответствии с возложенными на них задачами и в пределах своей компетенции. Ответственность за организацию защиты сведений, составляющих государственную тайну, в органах государственной власти, на предприятиях в учреждениях и организациях возлагается на их руководителей. В зависимости от объема работ с использованием сведений, составляющих государственную тайну, руководителями органов государственной власти предприятий, учреждений и организаций создаются структурные подразделения по защите государственной тайны, функции которых определяются указанными руководителями в соответствии с нормативными документами, утверждаемыми Правительством Российской Федерации, и с учетом специфики проводимых ими работ.

Защита государственной тайны является видом основной деятельности органа государственной власти, предприятия, учреждения или организации.

Основные функции системы безопасности:

- *выявление и прогнозирование* внутренних и внешних *угроз* жизненно важным интересам объектов безопасности, осуществление комплекса оперативных и долговременных мер по их предупреждению и нейтрализации;
- *создание и поддержание в готовности* сил и средств обеспечения безопасности;
- *управление силами и средствами* обеспечения безопасности в повседневных условиях и при чрезвычайных ситуациях;
- *осуществление системы мер по восстановлению нормального функционирования* объектов безопасности в регионах, пострадавших в результате возникновения чрезвычайной ситуации;

- *участие в мероприятиях* по обеспечению безопасности за пределами Российской Федерации в соответствии с международными договорами и соглашениями, заключенными или признанными Российской Федерацией.

Основные элементы системы безопасности образуют

- *органы законодательной, исполнительной и судебной властей*, государственные, общественные и иные *организации и объединения, граждане*, принимающие участие в обеспечении безопасности в соответствии с законом, а также

- законодательство, регламентирующее отношения в сфере безопасности.

Создание органов обеспечения безопасности, не установленных законом Российской Федерации, не допускается.

Пароль /Password/ - Идентификатор субъекта доступа, который является его (субъекта) секретом.

Перечень сведений, составляющих государственную тайну - совокупность категорий сведений, в соответствии с которыми сведения относятся к государственной тайне и засекречиваются на основаниях и в порядке, установленных федеральным законодательством. К таким относятся сведения

в военной области:

- *о содержании стратегических и оперативных планов, документов боевого управления* по подготовке и проведению операций, стратегическому, оперативному и мобилизационному развертыванию Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов, предусмотренных Федеральным законом "Об обороне", об их боевой и мобилизационной готовности, о создании и об использовании мобилизационных ресурсов;

- *о планах строительства* Вооруженных Сил Российской Федерации, других войск Российской Федерации, о направлениях развития вооружения и военной техники, о содержании и результатах выполнения целевых программ, научно-исследовательских и опытно-конструкторских работ по созданию и модернизации образцов вооружения и военной техники;

- *о разработке, технологии, производстве*, об объемах производства, о хранении, об утилизации ядерных боеприпасов, их составных частей, делящихся ядерных материалов, используемых в ядерных боеприпасах, о технических средствах и (или) методах защиты ядерных боеприпасов от несанкционированного применения, а также о ядерных энергетических и специальных физических установках оборонного значения;

- *о тактико-технических характеристиках и возможностях* боевого применения образцов вооружения и военной техники, о свойствах, рецептурах или технологиях производства новых видов ракетного топлива или взрывчатых веществ военного назначения;

- *о дислокации, назначении, степени готовности, защищенности* режимных и особо важных объектов, об их проектировании, строительстве и эксплуатации, а также об отводе земель, недр и акваторий для этих объектов; о дислокации, действительных наименованиях, об организационной структуре, о вооружении, численности войск и состоянии их боевого обеспечения, а также о военно-политической и (или) оперативной обстановке;

в области экономики, науки и техники:

- *о содержании планов подготовки* Российской Федерации и ее отдельных регионов к возможным военным действиям, о мобилизационных мощностях промышленности по изготовлению и ремонту вооружения и военной техники, об объемах производства, поставок, о запасах стратегических видов сырья и материалов, а также о размещении, фактических размерах и об использовании государственных материальных резервов;

- *об использовании инфраструктуры* Российской Федерации в целях обеспечения обороноспособности и безопасности государства;

- *о силах и средствах гражданской обороны*, о дислокации, предназначении и степени защищенности объектов административного управления, о степени обеспечения безопасности

населения, о функционировании транспорта и связи в Российской Федерации в целях обеспечения безопасности государства;

- *об объемах, о планах (заданиях) государственного оборонного заказа, о выпуске и поставках (в денежном или натуральном выражении) вооружения, военной техники и другой оборонной продукции, о наличии и наращивании мощностей по их выпуску, о связях предприятий по кооперации, о разработчиках или об изготовителях указанных вооружения, военной техники и другой оборонной продукции; о достижениях науки и техники, о научно-исследовательских, об опытно-конструкторских, о проектных работах и технологиях, имеющих важное оборонное или экономическое значение, влияющих на безопасность государства;*

- *об объемах запасов, добычи, передачи и потребления платины, металлов платиновой группы, природных алмазов, а также об объемах других стратегических видов полезных ископаемых Российской Федерации (по списку, определяемому Правительством Российской Федерации);*

в области внешней политики и экономики:

- *о внешнеполитической, внешнеэкономической деятельности Российской Федерации, преждевременное распространение которых может нанести ущерб безопасности государства;*

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

в области разведывательной, контрразведывательной и оперативно-розыскной деятельности:

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

- *о лицах, сотрудничающих или сотрудничавших на конфиденциальной основе с органами, осуществляющими разведывательную, контрразведывательную и оперативно-розыскную деятельность;*

- *об организации, о силах, средствах и методах обеспечения безопасности объектов государственной охраны, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения; о системе президентской, правительственной, шифрованной, в том числе кодированной и засекреченной связи, о шифрах, о разработке, об изготовлении шифров и обеспечении ими, о методах и средствах анализа шифровальных средств и средств специальной защиты, об информационно-аналитических системах специального назначения;*

о методах и средствах защиты секретной информации:

- *об организации и о фактическом состоянии защиты государственной тайны; о защите Государственной границы Российской Федерации, исключительной экономической зоны и континентального шельфа Российской Федерации;*

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

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

Порядок отнесения сведений к государственной тайне – представляет собой следующие действия:

1) отнесение сведений к государственной тайне в соответствии с их отраслевой, ведомственной или программно-целевой принадлежностью, а также в соответствии с Законом РФ «О государственной тайне», составляющих государственную тайну, определяемых этим Законом.

2) обоснование необходимости отнесения сведений к государственной тайне в соответствии с принципами засекречивания сведений.

Первое действие выполняется *руководителями органов государственной власти в соответствии с Перечнем должностных лиц*, наделенных полномочиями по отнесению сведений к государственной тайне, утверждаемым Президентом Российской Федерации, а второе - *возлагается на органы государственной власти, предприятия, учреждения и организации, которыми эти сведения получены (разработаны)*.

Правила разграничения доступа (ПРД) /Security policy/ - Совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

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/

Принципы обеспечения безопасности – это:

- законность;
- соблюдение баланса жизненно важных интересов личности, общества и государства;
- взаимная ответственность личности, общества и государства по обеспечению безопасности;
- интеграция с международными системами безопасности.

Принципы отнесения сведений к государственной тайне и их засекречивания – это принципы:

- законности;
- обоснованности и
- своевременности

Отнесение сведений к государственной тайне и их засекречивание представляет собой введение в предусмотренном Законом порядке для сведений, составляющих государственную тайну, ограничений на их распространение и на доступ к их носителям.

Законность отнесения сведений к государственной тайне и их засекречивание заключается в соответствии засекречиваемых сведений положениям [статей 5 и 7](#) Закона «О государственной тайны» Российской Федерации.

Обоснованность отнесения сведений к государственной тайне и их засекречивание 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 отнесения сведений к государственной тайне и их засекречивание заключается в установлении ограничений на распространение этих сведений с момента их получения (разработки) или заблаговременно.

Санкционированный доступ к информации /Authorized access to information/ - Доступ к информации, не нарушающий правила разграничения доступа.

Сведения, не подлежащие отнесению к государственной тайне и засекречиванию – это сведения:

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

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

Сертификация уровня защиты (Сертификация) /Protection level certification/ - Процесс установления соответствия средства вычислительной техники или автоматизированной системы набору определенных требований по защите

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.

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

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

Система разграничения доступа (СРД) /Security policy realization/ - Совокупность реализуемых правил разграничения доступа в средствах вычислительной техники или автоматизированных системах.

Соблюдение прав и свобод граждан при обеспечении безопасности состоит в обеспечении безопасности и не допущении ограничения прав и свобод граждан (за исключением случаев, прямо предусмотренных законом). Граждане, общественные и иные организации и объединения имеют право получать разъяснения по поводу ограничения их прав и свобод от органов, обеспечивающих безопасность. По их требованию такие разъяснения даются в письменной форме в установленные законодательством сроки.

Должностные лица, превысившие свои полномочия в процессе деятельности по обеспечению безопасности, несут ответственность в соответствии с законодательством.

Средство защиты от несанкционированного доступа (Средство защиты от НСД) /Protection facility/ - Программное, техническое или программно-техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа.

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;

Средство криптографической защиты информации (СКЗИ) /Cryptographic information protection facility/ - Средство вычислительной техники, осуществляющее криптографическое преобразование информации для обеспечения ее безопасности

Субъект доступа (Субъект) /Access subject/ - Лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Субъекты обеспечения безопасности – это:

- *государство*, осуществляющее функции в этой области через органы законодательной, исполнительной и судебной властей;

- *граждане*, общественные и иные *организации и объединения*, обладающие правами и обязанностями по участию в обеспечении безопасности в соответствии с законодательством РФ, законодательством республик в составе Российской Федерации, нормативными актами органов государственной власти и управления краев, областей, автономной области и автономных округов, принятыми в пределах их компетенции в данной сфере.

Государство, как основной субъект обеспечения безопасности, в соответствии с действующим законодательством обеспечивает:

- *безопасность* каждого гражданина на территории Российской Федерации;

- гарантированную *защиту и покровительство* для граждан России, находящимся за ее пределами.

- правовую и социальную *защиту* гражданам, общественным и иным *организациям и объединениям*, оказывающим содействие в обеспечении безопасности в соответствии с законом.

Степени секретности сведений и грифы секретности носителей этих сведений.

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

Устанавливаются три степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведений:

- "особой важности",
- "совершенно секретно" и
- "секретно".

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

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

Угроза безопасности - совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства. Реальная и потенциальная угроза объектам безопасности, исходящая от внутренних и внешних источников опасности, *определяет содержание деятельности по обеспечению* внутренней и внешней безопасности.

Уровень полномочий субъекта доступа /Subject privilege/ - Совокупность прав доступа субъекта доступа.

Целостность информации /Information integrity/ - Способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и (или) преднамеренного искажения (разрушения).

Аутентификация	17
Безопасность информации	21
Верификация	31
Дискреционное управление доступом	24
Диспетчер доступа (ядро защиты)	28
Доступ к информации	1
Защита от несанкционированного доступа	5
Защищенное средство вычислительной техники (защищенная автоматизированная система)	18
Идентификатор доступа	14
Идентификация	15
Класс защищенности средств вычислительной техники автоматизированной системы	32
Комплекс средств защиты	12
Конфиденциальная информация	23
Концепция диспетчера доступа	27
Мандатное управление доступом	25
Матрица доступа	8
Метка конфиденциальности	30
Многоуровневая защита	26
Модель защиты	20
Модель нарушителя правил разграничения доступа	11
Нарушитель правил разграничения доступа	10
Несанкционированный доступ к информации	4
Объект доступа	7
Пароль	16
Показатель защищенности средств вычислительной техники	33
Правила разграничения доступа	2
Санкционированный доступ к информации	3
Сертификат защиты	37
Сертификация уровня защиты	38
Система защиты информации от несанкционированного доступа	35
Система защиты секретной информации	34
Система разграничения доступа	13
Средство защиты от несанкционированного доступа	19
Средство криптографической защиты информации	36
Субъект доступа	6
Уровень полномочий субъекта доступа	9
Целостность информации	22

3. Алфавитный указатель терминов на английском языке

№ страницы

Access identifier	4
Access matrix	8
Access object	7
Access subject	6
Access to information	1
Authorized access to information	3
Authentication	17
Cryptographic information protection facility	36
Discretionary access control	24
Identification	15
Information integrity	22
Information security	21
Mandatory access control	25
Multilevel security	26
Password	16
Protection certificate	37
Protection class of computer systems	32
Protection criterion of computer systems	33
Protection facility	19
Protection from unauthorized access -	5
Protection level certification	38
Protection model	20
Reference monitor concept	27
Secret information security system	34
Security administrator	29

Security kernel	28
Security policy	2
Security policy realization	13
Security policy violator :	10
Security policy violator's model	11
Sensitive information	23
Sensitivity label	30
Subject privilege	9
System of protection from unauthorized access to information	35
Trusted computing base	12
Trusted computer system	18
Unauthorized access to information	4
Verification	31

2. Выписка из "Кодекса РФ об административных правонарушениях"

Выписка из "Кодекса РФ об административных правонарушениях" 30.12 2001 г. № 195-ФЗ

"Кодекс Российской Федерации об административных правонарушениях"

Принят Государственной Думой 20 декабря 2001 года

Одобен Советом Федерации 26 декабря 2001 года

См. Федеральный закон от 30 декабря 2001 г. N 196-ФЗ "О введении в действие Кодекса Российской Федерации об административных правонарушениях"

Вводится в действие с 1 июля 2002 года

Статья 13.11. Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных).

Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) - влечет предупреждение или наложение административного штрафа на граждан в размере от трех до пяти минимальных размеров оплаты труда; на должностных лиц - от пяти до десяти минимальных размеров оплаты труда; на юридических лиц - от пятидесяти до ста минимальных размеров оплаты труда.

Статья 13.12. Нарушение правил защиты информации.

Нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну), - влечет наложение административного штрафа на граждан в размере от трех до пяти минимальных размеров оплаты труда; на должностных лиц - от пяти до десяти минимальных размеров оплаты труда; на юридических лиц - от пятидесяти до ста минимальных размеров оплаты труда.

Использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну), - влечет наложение административного штрафа на граждан в размере от пяти до десяти минимальных размеров оплаты труда с конфискацией несертифицированных средств защиты информации или без таковой; на должностных лиц - от десяти до двадцати минимальных размеров оплаты труда; на юридических лиц - от ста до двухсот минимальных размеров оплаты труда с конфискацией несертифицированных средств защиты информации или без таковой.

Нарушение условий, предусмотренных лицензией на проведение работ, связанных с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну, - влечет наложение административного штрафа на должностных лиц в

размере от двадцати до тридцати минимальных размеров оплаты труда; на юридических лиц - от ста пятидесяти до двухсот минимальных размеров оплаты труда.

Использование несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну, - влечет наложение административного штрафа на должностных лиц в размере от тридцати до сорока минимальных размеров оплаты труда; на юридических лиц - от двухсот до трехсот минимальных размеров оплаты труда с конфискацией несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну, или без таковой.

Статья 13.13. Незаконная деятельность в области защиты информации.

Занятие видами деятельности в области защиты информации (за исключением информации, составляющей государственную тайну) без получения в установленном порядке специального разрешения (лицензии), если такое разрешение (такая лицензия) в соответствии с федеральным законом обязательно (обязательна), - влечет наложение административного штрафа на граждан в размере от пяти до десяти минимальных размеров оплаты труда с конфискацией средств защиты информации или без таковой; на должностных лиц - от двадцати до тридцати минимальных размеров оплаты труда с конфискацией средств защиты информации или без таковой; на юридических лиц - от ста до двухсот минимальных размеров оплаты труда с конфискацией средств защиты информации или без таковой.

Занятие видами деятельности, связанной с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну без лицензии, - влечет наложение административного штрафа на должностных лиц в размере от сорока до пятидесяти минимальных размеров оплаты труда; на юридических лиц - от трехсот до четырехсот минимальных размеров оплаты труда с конфискацией созданных без лицензии средств защиты информации, составляющей государственную тайну, или без таковой.

Статья 13.14. Разглашение информации с ограниченным доступом.

Разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, - влечет наложение административного штрафа на граждан в размере от пяти до десяти минимальных размеров оплаты труда; на должностных лиц - от сорока до пятидесяти минимальных размеров оплаты труда.

Президент Российской Федерации В.Путин
Москва, Кремль
30 декабря 2001 г.

3. Закон РФ от 5 марта 1992 г. N 2446-1 "О безопасности"

Закон РФ от 5 марта 1992 г. N 2446-1 "О безопасности" (с изменениями от 25.12.1992 г.)

Постановление ВС РФ от 5 марта 1992 г. N 2446/1-1 "О введении в действие Закона Российской Федерации "О безопасности"

Настоящий Закон закрепляет правовые основы обеспечения безопасности личности, общества и государства, определяет систему безопасности и ее функции, устанавливает порядок организации и финансирования органов обеспечения безопасности, а также контроля и надзора за законностью их деятельности.

ГЛАВА I. ОБЩИЕ ПОЛОЖЕНИЯ

Статья 1. Понятие безопасности и ее объекты

Безопасность - состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.

Жизненно важные интересы - совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства.

К основным объектам безопасности относятся:

- *личность* - ее права и свободы;
- *общество* - его материальные и духовные ценности;
- *государство* - его конституционный строй, суверенитет и территориальная целостность.

Статья 2. Субъекты обеспечения безопасности

Основным субъектом обеспечения безопасности является *государство*, осуществляющее функции в этой области через органы законодательной, исполнительной и судебной властей.

Государство в соответствии с действующим законодательством обеспечивает безопасность каждого *гражданина* на территории Российской Федерации. Гражданам Российской Федерации, находящимся за ее пределами, государством гарантируется защита и покровительство.

Граждане, общественные и иные организации и объединения являются субъектами безопасности, обладают правами и обязанностями по участию в обеспечении безопасности в соответствии с законодательством Российской Федерации, законодательством республик в составе Российской Федерации, нормативными актами органов государственной власти и управления краев, областей, автономной области и автономных округов, принятыми в пределах их компетенции в данной сфере. Государство обеспечивает правовую и социальную защиту гражданам, общественным и иным организациям и объединениям, оказывающим содействие в обеспечении безопасности в соответствии с законом.

Статья 3. Угроза безопасности

Угроза безопасности - совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства.

Реальная и потенциальная угроза объектам безопасности, исходящая от внутренних и внешних источников опасности, *определяет содержание деятельности по обеспечению внутренней и внешней безопасности.*

Статья 4. Обеспечение безопасности

Безопасность достигается проведением *единой государственной политики* в области обеспечения безопасности, системой мер экономического, политического, организационного и иного характера, адекватных угрозам жизненно важным интересам личности, общества и государства.

Для создания и поддержания необходимого уровня защищенности объектов безопасности в Российской Федерации *разрабатывается система правовых норм*, регулирующих отношения в сфере безопасности, определяются основные направления деятельности органов государственной власти и управления в данной области, формируются или преобразуются органы обеспечения безопасности и механизм контроля и надзора за их деятельностью.

Для непосредственного выполнения функций по обеспечению безопасности личности, общества и государства в системе исполнительной власти в соответствии с законом *образуются государственные органы обеспечения безопасности.*

Статья 5. Принципы обеспечения безопасности

Основными принципами обеспечения безопасности являются:

- *законность*;
- *соблюдение баланса* жизненно важных интересов личности, общества и государства;
- *взаимная ответственность* личности, общества и государства по обеспечению безопасности;
- *интеграция* с международными системами безопасности.

Статья 6. Законодательные основы обеспечения безопасности

Законодательные основы обеспечения безопасности составляют

- *Конституция РСФСР, - настоящий Закон, законы и другие нормативные акты Российской Федерации, регулирующие отношения в области безопасности;*
- *конституции, законы, иные нормативные акты республик в составе Российской Федерации и нормативные акты органов государственной власти и управления краев, областей, автономной области и автономных округов, принятые в пределах их компетенции в данной сфере;*
- *международные договоры и соглашения, заключенные или признанные Российской Федерацией.*

Статья 7. Соблюдение прав и свобод граждан при обеспечении безопасности

При обеспечении безопасности не допускается ограничение прав и свобод граждан, за исключением случаев, прямо предусмотренных законом.

Граждане, общественные и иные организации и объединения имеют право получать разъяснения по поводу ограничения их прав и свобод от органов, обеспечивающих безопасность. По их требованию такие разъяснения даются в письменной форме в установленные законодательством сроки.

Должностные лица, превысившие свои полномочия в процессе деятельности по обеспечению безопасности, несут ответственность в соответствии с законодательством.

ГЛАВА II. СИСТЕМА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Статья 8. Основные элементы системы безопасности

Систему безопасности образуют органы законодательной, исполнительной и судебной властей, государственные, общественные и иные организации и объединения, граждане, принимающие участие в обеспечении безопасности в соответствии с законом, а также законодательство, регламентирующее отношения в сфере безопасности.

Создание органов обеспечения безопасности, не установленных законом Российской Федерации, не допускается.

Статья 9. Основные функции системы безопасности

Основными функциями системы безопасности являются:

- *выявление и прогнозирование внутренних и внешних угроз* жизненно важным интересам объектов безопасности, осуществление комплекса оперативных и долговременных мер по их предупреждению и нейтрализации;
- *создание и поддержание в готовности сил и средств обеспечения безопасности;*
- *управление силами и средствами обеспечения безопасности в повседневных условиях и при чрезвычайных ситуациях;*
- *осуществление системы мер по восстановлению нормального функционирования объектов безопасности в регионах, пострадавших в результате возникновения чрезвычайной ситуации;*
- *участие в мероприятиях по обеспечению безопасности за пределами Российской Федерации в соответствии с международными договорами и соглашениями, заключенными или признанными Российской Федерацией.*

Статья 10. Разграничение полномочий органов власти в системе безопасности

Обеспечение безопасности личности, общества и государства осуществляется на основе разграничения полномочий органов законодательной, исполнительной и судебной властей в данной сфере.

Указом Президента РФ от 24 декабря 1993 г. N 2288 часть вторая статьи 10 настоящего Закона признана недействующей.

Верховный Совет Российской Федерации:

- *определяет приоритеты в защите жизненно важных интересов объектов безопасности;*

- *разрабатывает* систему правового регулирования отношений в сфере безопасности;
- *устанавливает* порядок организации и деятельности органов обеспечения безопасности;
- *осуществляет контроль* за кадровой политикой государственных органов обеспечения безопасности;
- не реже одного раза в год *заслушивает доклад* Президента Российской Федерации об обеспечении безопасности Российской Федерации;
- *определяет бюджетные ассигнования* на финансирование органов обеспечения безопасности и федеральных программ в сфере безопасности;
- *ратифицирует и денонсирует* международные договоры и соглашения Российской Федерации по вопросам обеспечения безопасности.

Органы исполнительной власти:

- *обеспечивают исполнение законов* и иных нормативных актов, регламентирующих отношения в сфере безопасности;
- *организуют разработку и реализацию* государственных программ обеспечения безопасности;
- *осуществляют систему мероприятий по обеспечению безопасности* личности, общества и государства в пределах своей компетенции;
- в соответствии с законом *формируют, реорганизуют и ликвидируют* государственные органы обеспечения безопасности.

Судебные органы:

- *обеспечивают защиту* конституционного строя в Российской Федерации, руководствуясь Конституцией РСФСР и законами Российской Федерации, конституциями и законами республик в составе Российской Федерации;
- *осуществляют правосудие* по делам о преступлениях, посягающих на безопасность личности, общества и государства;
- обеспечивают судебную защиту граждан, общественных и иных организаций и объединений, чьи права были нарушены в связи с деятельностью по обеспечению безопасности.

Статья 11. Руководство государственными органами обеспечения безопасности

Общее руководство государственными органами обеспечения безопасности осуществляет Президент Российской Федерации.

Президент Российской Федерации:

- *возглавляет* Совет безопасности Российской Федерации;
- Указом Президента РФ от 24 декабря 1993 г. № 2288 абзацы третий и шестой части второй статьи 11 настоящего Закона признаны недействующими
- совместно с Верховным Советом Российской Федерации *определяет стратегию* обеспечения внутренней и внешней безопасности;
 - *контролирует и координирует деятельность* государственных органов обеспечения безопасности;
 - в пределах определенной законом компетенции *принимает оперативные решения* по обеспечению безопасности;
 - не реже одного раза в год *представляет* Верховному Совету Российской Федерации доклад об обеспечении безопасности Российской Федерации.

Совет Министров Российской Федерации (Правительство Российской Федерации):

- в пределах определенной законом компетенции *обеспечивает руководство* государственными органами обеспечения безопасности Российской Федерации;
- *организует и контролирует разработку и реализацию мероприятий* по обеспечению безопасности министерствами и государственными комитетами Российской Федерации, другими подведомственными ему органами Российской Федерации, республик в составе Российской Федерации, краев, областей, автономной области, автономных округов.

Министерства и государственные комитеты Российской Федерации:

- в пределах своей компетенции, на основе действующего законодательства, в соответствии с решениями Президента Российской Федерации и постановлениями Правительства Российской Федерации *обеспечивают реализацию федеральных программ* защиты жизненно важных интересов объектов безопасности;

- на основании настоящего Закона в пределах своей компетенции *разрабатывают* внутриведомственные *инструкции (положения)* по обеспечению безопасности и представляют их на рассмотрение Совета безопасности.

Статья 12. Силы и средства обеспечения безопасности

Силы и средства обеспечения безопасности создаются и развиваются в Российской Федерации в соответствии с решениями Верховного Совета Российской Федерации, указами Президента Российской Федерации, краткосрочными и долгосрочными федеральными программами обеспечения безопасности.

Силы обеспечения безопасности включают в себя:

- Вооруженные Силы, федеральные органы безопасности, органы внутренних дел, внешней разведки, обеспечения безопасности органов законодательной, исполнительной, судебной властей и их высших должностных лиц, налоговой службы;

- службы ликвидации последствий чрезвычайных ситуаций, формирования гражданской обороны;

- пограничные войска, внутренние войска;

- органы, обеспечивающие безопасное ведение работ в промышленности, энергетике, на транспорте и в сельском хозяйстве;

- службы обеспечения безопасности средств связи и информации, таможни, природоохранные органы, органы охраны здоровья населения и другие государственные органы обеспечения безопасности, действующие на основании законодательства.

Службы Министерства безопасности Российской Федерации, Министерства внутренних дел Российской Федерации, иных органов исполнительной власти, использующие в своей деятельности специальные силы и средства, действуют только в пределах своей компетенции и в соответствии с законодательством.

Руководители органов обеспечения безопасности в соответствии с законодательством *несут ответственность* за нарушение установленного порядка их деятельности.

ГЛАВА III. СОВЕТ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

См. также Положение о Совете Безопасности Российской Федерации, утвержденное Указом Президента РФ от 10 июля 1996 г. № 1024

Статья 13. Статус Совета безопасности Российской Федерации

Совет безопасности Российской Федерации является конституционным органом, осуществляющим подготовку решений Президента Российской Федерации в области обеспечения безопасности.

Совет безопасности Российской Федерации рассматривает вопросы внутренней и внешней политики Российской Федерации в области обеспечения безопасности, стратегические проблемы государственной, экономической, общественной, оборонной, информационной, экологической и иных видов безопасности, охраны здоровья населения, прогнозирования, предотвращения чрезвычайных ситуаций и преодоления их последствий, обеспечения стабильности и правопорядка и ответствен перед Верховным Советом Российской Федерации за состояние защищенности жизненно важных интересов личности, общества и государства от внешних и внутренних угроз.

Статья 14. Состав Совета безопасности Российской Федерации и порядок его формирования

Совет безопасности Российской Федерации *формируется на основании Конституции РСФСР, Закона РСФСР "О Президенте РСФСР" и настоящего Закона.*

Указом Президента РФ от 24 декабря 1993 г. № 2288 Закон РСФСР "О Президенте РСФСР" признан недействующим

В состав Совета безопасности Российской Федерации входят:

- председатель,
- секретарь,
- постоянные члены и
- члены Совета безопасности.

Председателем Совета безопасности *является по должности Президент Российской Федерации.*

Состав Совета Безопасности РФ утвержден Указом Президента РФ от 31 июля 1996 г. № 1121

Указом Президента РФ от 24 декабря 1993 г. № 2288 части четвертая - шестая статьи 14 настоящего Закона признаны недействующими

В число постоянных членов Совета безопасности Российской Федерации входят по должности:

- вице-президент Российской Федерации,
- Первый заместитель Председателя Верховного Совета Российской Федерации,
- Председатель Совета Министров Российской Федерации (Председатель Правительства Российской Федерации).

Секретарь Совета безопасности *входит в число постоянных членов* Совета безопасности, назначается Президентом Российской Федерации и утверждается в должности Верховным Советом Российской Федерации.

Членами Совета безопасности *могут являться руководители* федеральных министерств и ведомств:

- экономики и финансов,
- иностранных дел,
- юстиции,
- обороны,
- безопасности,
- внутренних дел,
- экологии и природных ресурсов,
- здравоохранения,
- службы внешней разведки, а также
- иные должностные лица, назначенные Президентом Российской Федерации с согласия Верховного Совета Российской Федерации.

Законом РФ от 25 декабря 1992 г. N 4235-1 статья 14 настоящего Закона дополнена частью седьмой. Части седьмая и восьмая считаются соответственно частями восьмой и девятой

В заседаниях Совета безопасности принимает участие Председатель Верховного Совета Российской Федерации или по его поручению заместитель Председателя.

В зависимости от содержания рассматриваемого вопроса Совет безопасности Российской Федерации может привлекать к участию в заседаниях на правах консультантов и других лиц.

При рассмотрении вопросов обеспечения безопасности на территориях республик в составе Российской Федерации, краев, областей, автономной области и автономных округов для участия в работе Совета безопасности привлекаются их полномочные представители, а также председатель Государственного комитета Российской Федерации по национальной политике.

Статья 15. Основные задачи Совета безопасности Российской Федерации

Основными задачами Совета безопасности Российской Федерации являются:

- определение жизненно важных интересов личности, общества и государства и выявление внутренних и внешних угроз объектам безопасности;
- разработка основных направлений стратегии обеспечения безопасности Российской Федерации и организация подготовки федеральных программ ее обеспечения;

- подготовка рекомендаций *Президенту* Российской Федерации для принятия решений по вопросам внутренней и внешней политики в области обеспечения безопасности личности, общества и государства;
- подготовка оперативных решений по предотвращению чрезвычайных ситуаций, которые могут повлечь существенные социально-политические, экономические, военные, экологические и иные последствия, и по организации их ликвидации;
- подготовка предложений Президенту Российской Федерации о введении, продлении или отмене чрезвычайного положения;
- разработка предложений по координации деятельности органов исполнительной власти в процессе реализации принятых решений в области обеспечения безопасности и оценка их эффективности;
- совершенствование системы обеспечения безопасности путем разработки предложений по реформированию существующих либо созданию новых органов, обеспечивающих безопасность личности, общества и государства.

Статья 16. Порядок принятия решений Советом безопасности Российской Федерации

Заседания Совета безопасности Российской Федерации *проводятся* не реже одного *раза в месяц*. В случае необходимости могут проводиться внеочередные заседания Совета.

Постоянные члены Совета безопасности Российской Федерации обладают равными правами при принятии решений. Члены Совета безопасности принимают участие в его работе с правом совещательного голоса.

Решения Совета безопасности Российской Федерации *принимаются* на его заседании постоянными членами Совета безопасности *простым большинством* голосов от их общего количества и вступают в силу после утверждения председателем Совета безопасности.

Решения Совета безопасности по вопросам обеспечения безопасности оформляются указами Президента Российской Федерации.

Статья 17. Межведомственные комиссии Совета безопасности Российской Федерации

Совет безопасности Российской Федерации в соответствии с основными задачами его деятельности образует постоянные межведомственные комиссии, которые могут создаваться на функциональной или региональной основе.

В случае необходимости выработки предложений по предотвращению чрезвычайных ситуаций и ликвидации их последствий, отдельным проблемам обеспечения стабильности и правопорядка в обществе и государстве, защите конституционного строя, суверенитета и территориальной целостности Российской Федерации Советом безопасности Российской Федерации могут создаваться временные межведомственные комиссии.

Порядок формирования постоянных и временных межведомственных комиссий регламентируется Положением о Совете безопасности Российской Федерации, утверждаемым Президентом Российской Федерации по согласованию с Верховным Советом Российской Федерации.

По решению Совета безопасности Российской Федерации постоянные и временные межведомственные комиссии могут возглавляться членами Совета безопасности, а также руководителями соответствующих министерств и ведомств Российской Федерации, их заместителями либо лицами, уполномоченными на то Президентом Российской Федерации.

Статья 18. Аппарат Совета безопасности Российской Федерации

Организационно-техническое и информационное обеспечение деятельности Совета безопасности Российской Федерации осуществляет его *аппарат*, возглавляемый секретарем *Совета безопасности* Российской Федерации.

Структура и штатное расписание аппарата Совета безопасности Российской Федерации, а также положения о его подразделениях утверждаются председателем Совета безопасности.

См. Положение об аппарате Совета Безопасности Российской Федерации, утвержденное Указом Президента РФ от 1 августа 1996 г. N 1128

Статья 19. Основные задачи межведомственных комиссий и аппарата Совета безопасности Российской Федерации

На межведомственные комиссии и аппарат Совета безопасности Российской Федерации возлагаются:

- оценка внутренних и внешних угроз жизненно важным интересам объектов безопасности, выявление источников опасности;
- подготовка научно обоснованных прогнозов изменения внутренних и внешних условий и факторов, влияющих на состояние безопасности Российской Федерации;
- разработка и координация федеральных программ по обеспечению безопасности Российской Федерации и оценка их эффективности;
- накопление, анализ и обработка информации о функционировании системы обеспечения безопасности Российской Федерации, выработка рекомендаций по ее совершенствованию;
- информирование Совета безопасности Российской Федерации о ходе исполнения его решений;
- организация научных исследований в области обеспечения безопасности;
- подготовка проектов решений Совета безопасности Российской Федерации, а также проектов указов Президента Российской Федерации по вопросам безопасности;
- подготовка материалов для доклада Президента Российской Федерации Верховному Совету Российской Федерации об обеспечении безопасности Российской Федерации.

ГЛАВА IV. ФИНАНСИРОВАНИЕ ДЕЯТЕЛЬНОСТИ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ

Статья 20. Финансирование деятельности по обеспечению безопасности

Финансирование деятельности по обеспечению безопасности в зависимости от содержания и масштабов программ, характера чрезвычайных ситуаций и их последствий *осуществляется за счет* средств республиканского *бюджета* Российской Федерации, бюджетов республик в составе Российской Федерации, краев и областей, автономной области, автономных округов, городов Москвы и Санкт-Петербурга, а также внебюджетных средств.

ГЛАВА V. КОНТРОЛЬ И НАДЗОР ЗА ДЕЯТЕЛЬНОСТЬЮ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ

Статья 21. Контроль за деятельностью по обеспечению безопасности

Указом Президента РФ от 24 декабря 1993 г. № 2288 часть первая статьи 21 настоящего Закона признана недействующей

Контроль за деятельностью по обеспечению безопасности *осуществляет* Верховный Совет Российской Федерации через Совет Республики и Совет Национальностей Верховного Совета Российской Федерации, соответствующие постоянные комиссии палат и комитеты Верховного Совета Российской Федерации в соответствии с действующим законодательством.

Органы государственной власти и управления Российской Федерации в пределах своей компетенции *осуществляют контроль за деятельностью министерств и ведомств, предприятий, учреждений и организаций* по обеспечению безопасности.

Общественные и иные объединения и организации, граждане Российской Федерации *имеют право на получение* ими в соответствии с действующим законодательством *информации* о деятельности органов обеспечения безопасности.

Статья 22. Надзор за законностью деятельности органов обеспечения безопасности.

Надзор за законностью деятельности органов обеспечения безопасности *осуществляет* Генеральный прокурор Российской Федерации и подчиненные ему прокуроры.

Президент Российской Федерации Б.Ельцин

Москва, Дом Советов России
5 марта 1992 года N 2446-1

3. Закон РФ от 21.06.1993 г. № 5485-1 "О государственной тайне"

Закон РФ от 21 июля 1993 г. № 5485-1 "О государственной тайне"
(с изменениями от 6 октября 1997 г.)

Постановление ВС РФ от 21 июля 1993 г. № 5486-1 "О порядке введения в действие Закона Российской Федерации "О государственной тайне"

Федеральным законом от 6 октября 1997 г. № 131-ФЗ в тексте настоящего Закона слова "Министерство безопасности Российской Федерации" заменены словами "Федеральная служба безопасности Российской Федерации" в соответствующих падежах, преамбула Закона после слова "их" дополнена словами "засекречиванием или"

Настоящий Закон регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации.

ГЛАВА I. ОБЩИЕ ПОЛОЖЕНИЯ

О соответствии Конституции статьи 1 настоящего Закона см. постановление Конституционного Суда РФ от 27 марта 1996 г. N 8-П

Федеральным законом от 6 октября 1997 г. N 131-ФЗ в статье 1 настоящего Закона слово "представительной" заменено словом "законодательной"

Статья 1. Сфера действия настоящего Закона

Положения настоящего Закона обязательны для исполнения на территории Российской Федерации и за ее пределами

- органами законодательной, 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 2. Основные понятия, используемые в настоящем Законе

В настоящем 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;

Федеральным законом от 6 октября 1997 г. N 131-ФЗ [статья 2](#) настоящего Закона дополнена абзацем девятым следующего содержания:

перечень сведений, составляющих государственную тайну, - совокупность категорий сведений, в соответствии с которыми сведения относятся к государственной тайне и засекречиваются на основаниях и в порядке, установленных федеральным законодательством.

Статья 3. Законодательство Российской Федерации о государственной тайне

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.

Федеральным законом от 6 октября 1997 г. N 131-ФЗ в статью 4 настоящего Закона внесены изменения См. текст статьи в предыдущей редакции

Статья 4. Полномочия органов государственной власти и должностных лиц в области отнесения сведений к государственной тайне и их защиты

1. Палаты Федерального Собрания:

- осуществляют законодательное *регулирование отношений* в области государственной тайны;
- рассматривают *статьи* федерального бюджета в части средств, направляемых на реализацию государственных программ в области защиты государственной тайны;
- *определяют полномочия* должностных лиц в аппаратах палат Федерального Собрания по обеспечению защиты государственной тайны в палатах Федерального Собрания.

2. Президент Российской Федерации:

- *утверждает государственные программы* в области защиты государственной тайны;
- Государственная программа обеспечения защиты государственной тайны в Российской Федерации на 1996 - 1997 годы утверждена Указом Президента РФ от 9 марта 1996 г. N 346
- *утверждает* по представлению Правительства Российской Федерации *состав, структуру* межведомственной комиссии по защите государственной тайны и положение о ней;
- Межведомственная комиссия по защите государственной тайны образована Указом Президента РФ от 8 ноября 1995 г. № 1108
- Положение о Межведомственной комиссии по защите государственной тайны утверждено Указом Президента РФ от 20 января 1996 г. № 71
- Персональный состав Межведомственной комиссии по защите государственной тайны утвержден постановлением Правительства РФ от 28 февраля 1996 г. № 203
- *утверждает* по представлению Правительства Российской Федерации *Перечень должностных лиц* органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне, а также Перечень сведений, отнесенных к государственной тайне;
- Перечень должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне, утвержден распоряжением Президента РФ от 30 мая 1997 г. N 226-рп
- *заключает* международные *договоры* Российской Федерации о совместном использовании и защите сведений, составляющих государственную тайну;
- *определяет полномочия* должностных лиц по обеспечению защиты государственной тайны в Администрации Президента Российской Федерации;
- в пределах своих полномочий решает иные вопросы, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и их защитой.

3. Правительство Российской Федерации:

- *организует исполнение* Закона Российской Федерации "О государственной тайне";
- представляет на утверждение Президенту Российской Федерации *состав, структуру* межведомственной комиссии по защите государственной тайны и положение о ней;

- *представляет* на утверждение Президенту Российской Федерации Перечень *должностных лиц* органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне;

- *устанавливает порядок разработки Перечня* сведений, отнесенных к государственной тайне;

- *организует разработку и выполнение государственных программ* в области защиты государственной тайны;

- *определяет полномочия должностных лиц* по обеспечению защиты государственной тайны в аппарате Правительства Российской Федерации;

- *устанавливает размеры и порядок предоставления льгот* гражданам, допущенным к государственной тайне на постоянной основе, и сотрудникам структурных подразделений по защите государственной тайны;

Порядок и условия выплаты процентных надбавок к должностному окладу (тарифной ставке) должностных лиц и граждан, допущенных к государственной тайне утверждены постановлением Правительства РФ от 14 октября 1994 г. № 1161 устанавливает порядок определения размеров ущерба, наступившего в результате несанкционированного распространения сведений, составляющих государственную тайну, а также ущерба, наносимого собственнику информации в результате ее засекречивания;

- *заключает межправительственные соглашения*, принимает меры по выполнению международных договоров Российской Федерации о совместном использовании и защите сведений, составляющих государственную тайну, принимает решения о возможности передачи их носителей другим государствам;

- в пределах своих полномочий решает иные вопросы, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и их защитой.

4. Органы государственной власти Российской Федерации, органы государственной власти субъектов Российской Федерации и органы местного самоуправления во взаимодействии с органами защиты государственной тайны, расположенными в пределах соответствующих территорий:

- обеспечивают защиту переданных им другими органами государственной власти, предприятиями, учреждениями и организациями сведений, составляющих государственную тайну, а также сведений, засекречиваемых ими;

- обеспечивают защиту государственной тайны на подведомственных им предприятиях, в учреждениях и организациях в соответствии с требованиями актов законодательства Российской Федерации;

- обеспечивают в пределах своей компетенции проведение проверочных мероприятий в отношении граждан, допускаемых к государственной тайне;

- реализуют предусмотренные законодательством меры по ограничению прав граждан и предоставлению льгот лицам, имеющим либо имевшим доступ к сведениям, составляющим государственную тайну;

- вносят в полномочные органы государственной власти предложения по совершенствованию системы защиты государственной тайны.

5. Органы судебной власти:

- рассматривают уголовные и гражданские дела о нарушениях законодательства Российской Федерации о государственной тайне;

- обеспечивают судебную защиту граждан, органов государственной власти, предприятий, учреждений и организаций в связи с их деятельностью по защите государственной тайны;

- обеспечивают в ходе рассмотрения указанных дел защиту государственной тайны;

- определяют полномочия должностных лиц по обеспечению защиты государственной тайны в органах судебной власти.

Федеральным законом от 6 октября 1997 г. N 131-ФЗ название раздела II изложено в новой редакции. См. текст названия в предыдущей редакции

ГЛАВА II. ПЕРЕЧЕНЬ СВЕДЕНИЙ, СОСТАВЛЯЮЩИХ ГОСУДАРСТВЕННУЮ ТАЙНУ

Федеральным законом от 6 октября 1997 г. N 131-ФЗ статья 5 настоящего Закона изложена в новой редакции. См. текст статьи в предыдущей редакции

Статья 5. Перечень сведений, составляющих государственную тайну

Государственную тайну составляют:

- сведения в военной области:

- *о содержании стратегических и оперативных планов, документов боевого управления* по подготовке и проведению операций, стратегическому, оперативному и мобилизационному развертыванию Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов, предусмотренных Федеральным законом "Об обороне", об их боевой и мобилизационной готовности, о создании и об использовании мобилизационных ресурсов;

- *о планах строительства* Вооруженных Сил Российской Федерации, других войск Российской Федерации, о направлениях развития вооружения и военной техники, о содержании и результатах выполнения целевых программ, научно-исследовательских и опытно-конструкторских работ по созданию и модернизации образцов вооружения и военной техники;

- *о разработке, технологии, производстве*, об объемах производства, о хранении, об утилизации ядерных боеприпасов, их составных частей, делящихся ядерных материалов, используемых в ядерных боеприпасах, о технических средствах и (или) методах защиты ядерных боеприпасов от несанкционированного применения, а также о ядерных энергетических и специальных физических установках оборонного значения;

- *о тактико-технических характеристиках и возможностях* боевого применения образцов вооружения и военной техники, о свойствах, рецептурах или технологиях производства новых видов ракетного топлива или взрывчатых веществ военного назначения;

- *о дислокации, назначении, степени готовности, защищенности* режимных и особо важных объектов, об их проектировании, строительстве и эксплуатации, а также об отводе земель, недр и акваторий для этих объектов; о дислокации, действительных наименованиях, об организационной структуре, о вооружении, численности войск и состоянии их боевого обеспечения, а также о военно-политической и (или) оперативной обстановке;

- сведения в области экономики, науки и техники:

- *о содержании планов подготовки* Российской Федерации и ее отдельных регионов к возможным военным действиям, о мобилизационных мощностях промышленности по изготовлению и ремонту вооружения и военной техники, об объемах производства, поставок, о запасах стратегических видов сырья и материалов, а также о размещении, фактических размерах и об использовании государственных материальных резервов;

- *об использовании инфраструктуры* Российской Федерации в целях обеспечения обороноспособности и безопасности государства;

- *о силах и средствах* гражданской обороны, о дислокации, предназначении и степени защищенности объектов административного управления, о степени обеспечения безопасности населения, о функционировании транспорта и связи в Российской Федерации в целях обеспечения безопасности государства;

- *об объемах, о планах (заданиях) государственного оборонного заказа*, о выпуске и поставках (в денежном или натуральном выражении) вооружения, военной техники и другой оборонной продукции, о наличии и наращивании мощностей по их выпуску, о связях предприятий по кооперации, о разработчиках или об изготовителях указанных вооружения, военной техники и другой оборонной продукции; о достижениях науки и техники, о научно-исследовательских, об опытно-конструкторских, о проектных работах и технологиях, имеющих важное оборонное или экономическое значение, влияющих на безопасность государства;

- *об объемах запасов, добычи, передачи и потребления* платины, металлов платиновой группы, природных алмазов, а также об объемах других стратегических видов полезных ископаемых Российской Федерации (по списку, определяемому Правительством Российской Федерации);

- сведения в области внешней политики и экономики:

- *о внешнеполитической, внешнеэкономической деятельности* Российской Федерации, преждевременное распространение которых может нанести ущерб безопасности государства;

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

- в области разведывательной, контрразведывательной и оперативно-розыскной деятельности:

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

- *о лицах*, сотрудничающих или сотрудничавших на конфиденциальной основе с органами, осуществляющими разведывательную, контрразведывательную и оперативно-розыскную деятельность;

- *об организации, о силах, средствах и методах* обеспечения безопасности объектов государственной охраны, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения; о системе президентской, правительственной, шифрованной, в том числе кодированной и засекреченной связи, о шифрах, о разработке, об изготовлении шифров и обеспечении ими, о методах и средствах анализа шифровальных средств и средств специальной защиты, об информационно-аналитических системах специального назначения;

- *о методах и средствах защиты* секретной информации;

- *об организации* и о фактическом состоянии защиты государственной тайны; о защите Государственной границы Российской Федерации, исключительной экономической зоны и континентального шельфа Российской Федерации;

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

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

Федеральным законом от 6 октября 1997 г. № 131-ФЗ название раздела III изложено в новой редакции. См. текст названия в предыдущей редакции.

ГЛАВА III. ОТНЕСЕНИЕ СВЕДЕНИЙ К ГОСУДАРСТВЕННОЙ ТАЙНЕ И ИХ ЗАСЕКРЕЧИВАНИЕ

Федеральным законом от 6 октября 1997 г. N 131-ФЗ в статью 6 настоящего Закона внесены изменения. См. текст статьи в предыдущей редакции.

Статья 6. Принципы отнесения сведений к государственной тайне и засекречивания этих сведений

Отнесение сведений к государственной тайне и их засекречивание - введение в предусмотренном настоящим Законом порядке для сведений, составляющих государственную тайну, ограничений на их распространение и на доступ к их носителям.

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

Законность отнесения сведений к государственной тайне и их засекречивание заключается в соответствии засекречиваемых сведений положениям [статей 5](#) и [7](#) настоящего Закона и законодательству Российской Федерации о государственной тайне.

Обоснованность отнесения сведений к государственной тайне и их засекречивание 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 отнесения сведений к государственной тайне и их засекречивание заключается в установлении ограничений на распространение этих сведений с момента их получения (разработки) или заблаговременно.

Федеральным законом от 6 октября 1997 г. N 131-ФЗ в статью 7 настоящего Закона внесены изменения. См. текст статьи в предыдущей редакции.

Статья 7. Сведения, не подлежащие отнесению к государственной тайне и засекречиванию

Не подлежат отнесению к государственной тайне и засекречиванию сведения:

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

О сведениях, не подлежащих засекречиванию, см. также постановление Правительства РФ от 7 августа 1995 г. № 798.

Статья 8. Степени секретности сведений и грифы секретности носителей этих сведений

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

Устанавливаются три степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведений:

- "особой важности",
- "совершенно секретно" и
- "секретно".

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

Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности утверждены постановлением Правительства РФ от 4 сентября 1995 г. № 870

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

Федеральным законом от 6 октября 1997 г. N 131-ФЗ в статью 9 настоящего Закона внесены изменения. См. текст статьи в предыдущей редакции.

Статья 9. Порядок отнесения сведений к государственной тайне

Отнесение сведений к государственной тайне *осуществляется* в соответствии с их отраслевой, ведомственной или программно-целевой *принадлежностью*, а также в соответствии с настоящим Законом.

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 в соответствии с Перечнем* сведений, составляющих государственную тайну, определяемым настоящим Законом, руководителями органов государственной власти в соответствии с Перечнем должностных лиц, наделенных полномочиями по отнесению сведений к государственной тайне, утверждаемым Президентом Российской Федерации. Указанные лица несут персональную ответственность за принятые ими решения о целесообразности отнесения конкретных сведений к государственной тайне.

Для осуществления единой государственной политики в области засекречивания сведений *межведомственная комиссия* по защите государственной тайны *формирует* по предложениям органов государственной власти и в соответствии с Перечнем сведений, составляющих государственную тайну, *Перечень* сведений, отнесенных к государственной тайне. В этом Перечне указываются органы государственной власти, наделяемые полномочиями по распоряжению данными сведениями. Указанный Перечень утверждается Президентом Российской Федерации, подлежит открытому опубликованию и пересматривается по мере необходимости.

Органами государственной власти, руководители которых наделены полномочиями по отнесению сведений к государственной тайне, в соответствии с Перечнем сведений, отнесенных к государственной тайне, *разрабатываются развернутые перечни* сведений, подлежащих засекречиванию. В эти перечни включаются сведения, полномочиями по распоряжению которыми наделены указанные органы, и устанавливается степень их секретности. В рамках целевых программ по разработке и модернизации образцов вооружения и военной техники, опытно-конструкторских и научно-исследовательских работ по решению заказчиков указанных образцов и работ могут разрабатываться отдельные перечни сведений, подлежащих засекречиванию. Эти перечни утверждаются соответствующими руководителями органов государственной власти. Целесообразность засекречивания таких перечней определяется их содержанием.

Статья 10. Ограничение прав собственности предприятий, учреждений организаций и граждан Российской Федерации на информацию в связи с ее засекречиванием

Должностные лица, наделенные в порядке, предусмотренном [статьей 9](#) настоящего Закона, полномочиями по отнесению сведений к государственной тайне, *вправе принимать решения* о засекречивании информации, находящейся в собственности предприятий, учреждений, организаций и граждан (далее - собственник информации), если эта информация включает сведения, перечисленные в Перечне сведений, отнесенных к государственной тайне. Засекречивание указанной информации осуществляется по представлению собственников информации или соответствующих органов государственной власти.

Материальный ущерб, наносимый собственнику информации в связи с ее засекречиванием, *возмещается государством* в размерах, определяемых в договоре между органом государственной власти, в распоряжение которого переходит эта информация, и ее собственником. В договоре также предусматриваются обязательства собственника информации по ее нераспространению. При отказе собственника информации от подписания договора он предупреждается об ответственности за несанкционированное распространение сведений, составляющих государственную тайну в соответствии с действующим законодательством.

Собственник информации *вправе обжаловать в суде* действия должностных лиц, ущемляющие, по мнению собственника информации, его права. В случае признания судом действий должностных лиц незаконными порядок возмещения ущерба, нанесенного собственнику информации, определяется решением суда в соответствии с действующим законодательством.

Не может быть ограничено право собственности на информацию иностранных организаций и иностранных граждан, если эта информация получена (разработана) ими без нарушения законодательства Российской Федерации.

Статья 11. Порядок засекречивания сведений и их носителей

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

При невозможности идентификации полученных (разработанных) сведений со сведениями, содержащимися в действующем перечне, должностные лица органов государственной власти, предприятий, учреждений и организаций обязаны обеспечить предварительное засекречивание полученных (разработанных) сведений в соответствии с предполагаемой степенью секретности и в месячный срок направить в адрес должностного лица, утвердившего указанный перечень, предложения по его дополнению (изменению).

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

Статья 12. Реквизиты носителей сведений, составляющих государственную тайну

На носители сведений, составляющих государственную тайну, вносятся 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.

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

Помимо перечисленных в настоящей статье реквизитов на носителе и (или) в сопроводительной документации к нему могут проставляться дополнительные отметки, определяющие полномочия должностных лиц по ознакомлению с содержащимися в этом носителе сведениями. Вид и порядок проставления дополнительных отметок и других реквизитов определяются нормативными документами, утверждаемыми Правительством Российской Федерации.

ГЛАВА IV. РАССЕКРЕЧИВАНИЕ СВЕДЕНИЙ И ИХ НОСИТЕЛЕЙ

О порядке рассекречивания архивных документов см. постановление Правительства РФ от 20 февраля 1995 г. № 170

Статья 13. Порядок рассекречивания сведений

Рассекречивание сведений и их носителей - снятие ранее введенных в предусмотренном настоящим Законом порядке ограничений на распространение сведений, составляющих государственную тайну, и на доступ к их носителям.

Основаниями для рассекречивания сведений являются:

- взятие на себя Российской Федерацией международных обязательств по открытому обмену сведениями, составляющими в Российской Федерации государственную тайну;
- *изменение объективных обстоятельств*, вследствие которого дальнейшая защита сведений, составляющих государственную тайну, является нецелесообразной.

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

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

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

Статья 14. Порядок рассекречивания носителей сведений, составляющих государственную тайну.

Носители сведений, составляющих государственную тайну, *рассекречиваются не позднее сроков, установленных при их засекречивании*. До истечения этих сроков носители подлежат рассекречиванию, если изменены положения действующего в данном органе государственной власти, на предприятии, в учреждении и организации перечня, на основании которых они были засекречены.

В исключительных случаях право продления первоначально установленных сроков засекречивания носителей сведений, составляющих государственную тайну, *предоставляется руководителям* государственных органов, наделенным полномочиями по отнесению соответствующих сведений к государственной тайне, на основании заключения назначенной ими в установленном порядке экспертной комиссии.

Руководители органов государственной власти, предприятий, учреждений и организаций *наделяются полномочиями по рассекречиванию* носителей сведений, необоснованно засекреченных подчиненными им должностными лицами.

Руководители государственных архивов Российской Федерации *наделяются полномочиями по рассекречиванию* носителей сведений, составляющих государственную тайну, находящихся на хранении в закрытых фондах этих архивов, в случае делегирования им таких полномочий организацией - фондообразователем или ее правопреемником. В случае ликвидации организации - фондообразователя и отсутствия ее правопреемника вопрос о порядке рассекречивания носителей сведений, составляющих государственную тайну, рассматривается межведомственной комиссией по защите государственной тайны.

Статья 15. Исполнение запросов граждан, предприятий, учреждений, организаций и органов государственной власти Российской Федерации о рассекречивании сведений

Граждане, предприятия, учреждения, организации и органы государственной власти Российской Федерации *вправе обратиться* в органы государственной власти, на предприятия, в учреждения, организации в том числе в государственные архивы, *с запросом о рассекречивании сведений*, отнесенных к государственной тайне.

Органы государственной власти, предприятия, учреждения, организации, в том числе государственные архивы, получившие такой запрос, *обязаны в течение трех месяцев рассмот-*

реть его и дать мотивированный ответ по существу запроса. Если они не правомочны решить вопрос о рассекречивании запрашиваемых сведений, то запрос в месячный срок с момента его поступления передается в орган государственной власти, наделенный такими полномочиями либо в межведомственную комиссию по защите государственной тайны о чем уведомляются граждане предприятия, учреждения, организации и органы государственной власти Российской Федерации, подавшие запрос.

Уклонение должностных лиц от рассмотрения запроса по существу влечет за собой административную (дисциплинарную) ответственность в соответствии с действующим законодательством.

Обоснованность отнесения сведений к государственной тайне может быть обжалована в суд. При признании судом необоснованности засекречивания сведений эти сведения подлежат рассекречиванию в установленном настоящим Законом порядке.

ГЛАВА V. РАСПОРЯЖЕНИЕ СВЕДЕНИЯМИ, СОСТАВЛЯЮЩИМИ ГОСУДАРСТВЕННУЮ ТАЙНУ

Статья 16. Взаимная передача сведений, составляющих государственную тайну, органами государственной власти, предприятиями, учреждениями и организациями

Взаимная передача сведений, составляющих государственную тайну, осуществляется органами государственной власти, предприятиями, учреждениями и организациями, не состоящими в отношениях подчиненности и не выполняющими совместных работ с санкции органа государственной власти, в распоряжении которого в соответствии со [статьей 9](#) настоящего Закона находятся эти сведения.

Органы государственной власти, предприятия, учреждения и организации, запрашивающие сведения, составляющие государственную тайну, обязаны создать условия, обеспечивающие защиту этих сведений. Их руководители несут персональную ответственность за несоблюдение установленных ограничений по ознакомлению со сведениями, составляющими государственную тайну.

Обязательным условием для передачи сведений, составляющих государственную тайну, органам государственной власти, предприятиям, учреждениям и организациям является выполнение ими требований, предусмотренных в [статье 27](#) настоящего Закона.

Постановлением ВС РФ от 21 июля 1993 г. N 5486-1 установлено, что часть первая статьи 17 настоящего Закона вводится в действие не позднее 1 января 1995 года

Статья 17. Передача сведений, составляющих государственную тайну, в связи с выполнением совместных и других работ

Передача сведений, составляющих государственную тайну, предприятиям, учреждениям, организациям или гражданам в связи с выполнением совместных и других работ осуществляется заказчиком этих работ с разрешения органа государственной власти, в распоряжении которого в соответствии со [статьей 9](#) настоящего Закона находятся соответствующие сведения, и только в объеме, необходимом для выполнения этих работ. При этом до передачи сведений, составляющих государственную тайну, заказчик обязан убедиться в наличии у предприятия, учреждения или организации лицензии на проведение работ с использованием сведений соответствующей степени секретности, а у граждан - соответствующего допуска.

Предприятия, учреждения или организации, в том числе и негосударственных форм собственности, при проведении совместных и других работ (получении государственных заказов) и возникновении в связи с этим необходимости в использовании сведений, составляющих государственную тайну, могут заключать с государственными предприятиями, учреждениями или организациями договоры об использовании услуг их структурных подразделений по защите государственной тайны, о чем делается соответствующая отметка в лицензиях на проведение работ с использованием сведений, составляющих государственную тайну, обеих договаривающихся сторон.

В договоре на проведение совместных и других работ, заключаемом в установленном законом порядке, предусматриваются взаимные обязательства сторон по обеспечению сохранно-

сти сведений, составляющих государственную тайну, как в процессе проведения работ, так и по их завершении, а также условия финансирования работ (услуг) по защите сведений, составляющих государственную тайну.

Организация контроля за эффективностью защиты государственной тайны при проведении совместных и других работ возлагается на заказчика этих работ в соответствии с положениями заключенного сторонами договора.

При нарушении исполнителем в ходе совместных и других работ взятых на себя обязательств по защите государственной тайны заказчик вправе приостановить выполнение заказа до устранения нарушений, а при повторных нарушениях - поставить вопрос об аннулировании заказа и лицензии на проведение работ с использованием сведений, составляющих государственную тайну, и о привлечении виновных лиц к ответственности. При этом материальный ущерб, нанесенный исполнителем государству в лице заказчика, подлежит взысканию в соответствии с действующим законодательством.

Статья 18. Передача сведений, составляющих государственную тайну, другим государствам

Решение о передаче сведений, составляющих государственную тайну, другим государствам принимается Правительством Российской Федерации при наличии экспертного заключения межведомственной комиссии по защите государственной тайны о возможности передачи этих сведений.

См. Положение о подготовке к передаче сведений, составляющих государственную тайну, другим государствам, утвержденное постановлением Правительства РФ от 2 августа 1997 г. № 973

Обязательства принимающей стороны по защите передаваемых ей сведений предусматриваются заключаемым с ней договором (соглашением).

Статья 19. Защита сведений, составляющих государственную тайну, при изменении функций субъектов правоотношений

Органы государственной власти, предприятия, учреждения и организации, располагающие сведениями, составляющими государственную тайну, в случаях изменения их функций, форм собственности, ликвидации или прекращения работ с использованием сведений, составляющих государственную тайну, обязаны принять меры по обеспечению защиты этих сведений и их носителей. При этом носители сведений, составляющих государственную тайну, в установленном порядке уничтожаются, сдаются на архивное хранение либо передаются:

- правопреемнику органа государственной власти, предприятия, учреждения или организации, располагающих сведениями, составляющими государственную тайну, если этот правопреемник имеет полномочия по проведению работ с использованием указанных сведений;
- органу государственной власти, в распоряжении которого в соответствии со [статьей 9](#) настоящего Закона находятся соответствующие сведения;
- другому органу государственной власти, предприятию, учреждению или организации по указанию межведомственной комиссии по защите государственной тайны.

Глава VI. Защита государственной тайны

Статья 20. Органы защиты государственной тайны

К органам защиты государственной тайны относятся:

- *межведомственная комиссия* по защите государственной тайны;
- *органы федеральной исполнительной власти* (Федеральная служба 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.

Межведомственная комиссия по защите государственной тайны является коллегиальным органом, координирующим деятельность органов государственной власти по защите государственной тайны в интересах разработки и выполнения государственных программ нормативных и методических документов, обеспечивающих реализацию законодательства Российской Федерации о государственной тайне. Функции межведомственной комиссии по защите государственной тайны и ее надведомственные полномочия реализуются в соответствии с Положением о межведомственной комиссии по защите государственной тайны, утвержденным Президентом Российской Федерации.

Указом Президента РФ от 30 марта 1994 г. № 614 функции межведомственной комиссии по защите государственной тайны временно возложены на Государственную техническую комиссию при Президенте Российской Федерации.

Органы федеральной исполнительной власти (Федеральная служба безопасности Российской Федерации, Министерства 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 организуют и обеспечивают защиту государственной тайны в соответствии с функциями, возложенными на них законодательством Российской Федерации.

Органы государственной власти, предприятия, учреждения и организации обеспечивают защиту сведений, составляющих государственную тайну, в соответствии с возложенными на них задачами и в пределах своей компетенции. Ответственность за организацию защиты сведений, составляющих государственную тайну, в органах государственной власти, на предприятиях в учреждениях и организациях возлагается на их руководителей. В зависимости от объема работ с использованием сведений, составляющих государственную тайну, руководителями органов государственной власти предприятий, учреждений и организаций создаются структурные подразделения по защите государственной тайны, функции которых определяются указанными руководителями в соответствии с нормативными документами, утвержденными Правительством Российской Федерации, и с учетом специфики проводимых ими работ.

Защита государственной тайны является видом основной деятельности органа государственной власти, предприятия, учреждения или организации.

Постановлением Правительства РФ от 3 марта 1997 г. N 242 на Федеральную службу безопасности Российской Федерации возложено выполнение функций органа Российской Федерации, ответственного за осуществление мероприятий и процедур в области защиты информации и обеспечение надзора в целях защиты информации, имеющей гриф секретности, которой обмениваются Российская Федерация и НАТО

О соответствии Конституции [статьи 21](#) настоящего Закона см. постановление Конституционного Суда РФ от 27 марта 1996 г. № 8-П.

Статья 21. Допуск должностных лиц и граждан к государственной тайне

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;
- *согласия 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. Проверочные мероприятия осуществляются в соответствии с законодательством Российской Федерации. Целью проведения проверочных мероприятий является выявление оснований, предусмотренных [статьей 22](#) настоящего Закона.

Для должностных лиц и граждан, допущенных к государственной тайне на постоянной основе, устанавливаются следующие льготы:

- процентные надбавки к заработной плате в зависимости от степени секретности сведений, к которым они имеют доступ;

Порядок и условия выплаты процентных надбавок к должностному окладу (тарифной ставке) должностных лиц и граждан, допущенных к государственной тайне утверждены постановлением Правительства РФ от 14 октября 1994 г. № 1161 преимущественное право при прочих равных условиях на оставление на работе при проведении органами государственной власти, предприятиями, учреждениями и организациями организационных и (или) штатных мероприятий.

Для сотрудников структурных подразделений по защите государственной тайны дополнительно к льготам, установленным для должностных лиц и граждан, допущенных к государственной тайне на постоянной основе, устанавливается процентная надбавка к заработной плате за стаж работы в указанных структурных подразделениях.

Взаимные обязательства администрации и оформляемого лица *отражаются в трудовом договоре (контракте)*. Заключение трудового договора (контракта) до окончания проверки компетентными органами не допускается.

Устанавливается три формы допуска к государственной тайне должностных лиц и граждан, соответствующие трем степеням секретности сведений, составляющих государственную тайну: к сведениям особой важности, совершенно секретным или секретным. Наличие у должностных лиц и граждан допуска к сведениям более высокой степени секретности является основанием для доступа их к сведениям более низкой степени секретности.

Сроки, обстоятельства и порядок переоформления допуска граждан к государственной тайне *устанавливаются нормативными документами*, утверждаемыми *Правительством Российской Федерации*.

См. Инструкцию о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне, утвержденную постановлением Правительства РФ от 28 октября 1995 г. № 1050.

Порядок допуска должностных лиц и граждан к государственной тайне в условиях объявленного чрезвычайного положения *может быть изменен Президентом Российской Федерации*.

Федеральным законом от 6 октября 1997 г. N 131-ФЗ настоящий Закон дополнен статьей 21(1).

Статья 21(1). Особый порядок допуска к государственной тайне

Члены Совета Федерации, депутаты Государственной Думы, судьи на период исполнения ими своих полномочий, а также адвокаты, участвующие в качестве защитников в уголовном судопроизводстве по делам, связанным со сведениями, составляющими государственную тайну, допускаются к сведениям, составляющим государственную тайну, без проведения проверочных мероприятий, предусмотренных [статьей 21](#) настоящего Закона.

Указанные лица предупреждаются о неразглашении государственной тайны, ставшей им известной в связи с исполнением ими своих полномочий, и о привлечении их к ответственности в случае ее разглашения, о чем у них отбирается соответствующая расписка.

Сохранность государственной тайны в таких случаях гарантируется путем установления ответственности указанных лиц федеральным законом.

Статья 22. Основания для отказа должностному лицу или гражданину в допуске к государственной тайне

Федеральным законом от 6 октября 1997 г. N 131-ФЗ в абзаце втором части первой статьи 22 настоящего Закона слова "особо опасным" исключены.

Основаниями для отказа должностному лицу или гражданину в допуске к государственной тайне могут являться:

- признание его судом недееспособным, ограниченно дееспособным или особо опасным рецидивистом, нахождение его под судом или следствием за государственные и иные тяжкие преступления, наличие у него неснятой судимости за эти преступления;
- наличие у него медицинских противопоказаний для работы с использованием сведений, составляющих государственную тайну, согласно перечню, утверждаемому Министерством здравоохранения Российской Федерации;
- постоянное проживание его самого и (или) его близких родственников за границей и (или) оформление указанными лицами документов для выезда на постоянное жительство в другие государства;
- выявление в результате проверочных мероприятий действий оформляемого лица, создающих угрозу безопасности Российской Федерации;
- уклонение его от проверочных мероприятий и (или) сообщение им заведомо ложных анкетных данных.

Решение об отказе должностному лицу или гражданину в допуске к государственной тайне принимается руководителем органа государственной власти, предприятия, учреждения или организации в индивидуальном порядке с учетом результатов проверочных мероприятий. Гражданин имеет право обжаловать это решение в вышестоящую организацию или в суд.

Статья 23. Условия прекращения допуска должностного лица или гражданина к государственной тайне

Допуск должностного лица или гражданина к государственной тайне может быть прекращен по решению руководителя органа государственной власти, предприятия, учреждения или организации в случаях:

- *расторжения с ним трудового договора (контракта) в связи с проведением организационных и (или) штатных мероприятий;*
- *однократного нарушения им взятых на себя предусмотренных трудовым договором (контрактом) обязательств, связанных с защитой государственной тайны;*
- *возникновения обстоятельств, являющихся согласно [статье 22](#) настоящего Закона основанием для отказа должностному лицу или гражданину в допуске к государственной тайне.*

Прекращение допуска должностного лица или гражданина к государственной тайне *является дополнительным основанием для расторжения с ним трудового договора (контракта), если такие условия предусмотрены в трудовом договоре (контракте).*

Прекращение допуска к государственной тайне *не освобождает* должностное лицо или гражданина *от взятых ими обязательств* по неразглашению сведений, составляющих государственную тайну.

Решение администрации о прекращении допуска должностного лица или гражданина к государственной тайне и расторжении на основании этого с ним трудового договора (контракта) *может быть обжаловано* в вышестоящую организацию или в суд.

Статья 24. Ограничения прав должностного лица или гражданина, допущенных или ранее допускавшихся к государственной тайне

Должностное лицо или гражданин, допущенные или ранее допускавшиеся к государственной тайне, могут быть временно ограничены в своих правах. Ограничения могут касаться:

- *права выезда за границу на срок, оговоренный в трудовом договоре (контракте) при оформлении допуска гражданина к государственной тайне;*
- *права на распространение сведений, составляющих государственную тайну, и на использование открытий и изобретений, содержащих такие сведения;*
- *права на неприкосновенность частной жизни при проведении проверочных мероприятий в период оформления допуска к государственной тайне.*

Статья 25. Организация доступа должностного лица или гражданина к сведениям, составляющим государственную тайну

Организация доступа должностного лица или гражданина к сведениям, составляющим государственную тайну, возлагается на руководителя соответствующего органа государственной власти, предприятия, учреждения или организации, а также на их структурные подразделения по защите государственной тайны. Порядок доступа должностного лица или гражданина к сведениям, составляющим государственную тайну, устанавливается нормативными документами, утверждаемыми Правительством Российской Федерации.

Руководители органов государственной власти, предприятий, учреждений и организаций несут персональную ответственность за создание таких условий, при которых должностное лицо или гражданин знакомятся только с теми сведениями, составляющими государственную тайну, и в таких объемах, которые необходимы ему для выполнения его должностных (функциональных) обязанностей.

Статья 26. Ответственность за нарушение законодательства Российской Федерации о государственной тайне

Должностные лица и граждане, виновные в нарушении законодательства Российской Федерации о государственной тайне, несут уголовную, административную, гражданско-правовую или дисциплинарную *ответственность* в соответствии с действующим законодательством.

Федеральным законом от 6 октября 1997 г. № 131-ФЗ статья 26 настоящего Закона дополнена новой частью второй, часть вторая считается частью третьей.

Соответствующие органы государственной власти и их должностные лица основываются на подготовленных в установленном порядке экспертных заключениях об отнесении незаконно распространенных сведений к сведениям, составляющим государственную тайну.

Защита прав и законных интересов граждан, органов государственной власти, предприятий, учреждений и организаций в сфере действия настоящего Закона *осуществляется в судебном или ином порядке*, предусмотренном настоящим Законом.

Постановлением ВС РФ от 21 июля 1993 г. N 5486-1 установлено, что часть первая статьи 27 настоящего Закона вводится в действие не позднее 1 января 1995 года.

Статья 27. Допуск предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну

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.

Положение о лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны утверждено постановлением Правительства РФ от 15 апреля 1995 г. № 333.

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.*

Статья 28. Порядок сертификации 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, Федеральная служба безопасности Российской Федерации, Федеральное агентство правительственной связи и информации при Президенте 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.

Положение о сертификации средств защиты информации утверждено постановлением Правительства РФ от 26 июня 1995 г. № 608.

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

ГЛАВА VII. ФИНАНСИРОВАНИЕ МЕРОПРИЯТИЙ ПО ЗАЩИТЕ ГОСУДАРСТВЕННОЙ ТАЙНЫ

Статья 29. Финансирование мероприятий по защите государственной тайны

Финансирование деятельности органов государственной власти, бюджетных предприятий, учреждений и организаций и их структурных подразделений по защите государственной тайны осуществляется за счет средств соответствующих *бюджетов*, а остальных предприятий, учреждений и организаций - за счет *средств*, получаемых от их основной деятельности при выполнении работ, связанных с использованием сведений, составляющих государственную тайну.

Средства на финансирование государственных программ в области защиты государственной тайны предусматриваются в федеральном бюджете Российской Федерации отдельной строкой.

Контроль за расходованием финансовых средств, выделяемых на проведение мероприятий по защите государственной тайны, осуществляется руководителями органов государственной власти, предприятий, учреждений и организаций, заказчиками работ, а также специально уполномоченными на то представителями Министерства финансов Российской Федерации. Если осуществление этого контроля связано с доступом к сведениям, составляющим государственную тайну, то перечисленные лица должны иметь допуск к сведениям соответствующей степени секретности.

ГЛАВА VIII. КОНТРОЛЬ И НАДЗОР ЗА ОБЕСПЕЧЕНИЕМ ЗАЩИТЫ ГОСУДАРСТВЕННОЙ ТАЙНЫ

Федеральным законом от 6 октября 1997 г. № 131-ФЗ статья 30 настоящего Закона изложена в новой редакции. См. текст статьи в предыдущей редакции

Статья 30. Контроль за обеспечением защиты государственной тайны

Контроль за обеспечением защиты государственной тайны *осуществляют Президент Российской Федерации, Правительство Российской Федерации в пределах полномочий, опре-*

деляемых Конституцией Российской Федерации, федеральными конституционными законами и федеральными законами.

Статья 31. Межведомственный и ведомственный контроль

Межведомственный контроль за обеспечением защиты государственной тайны в органах государственной власти, на предприятиях, в учреждениях и организациях осуществляют органы федеральной исполнительной *власти* (Федеральная служба 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, на которые эта функция возложена законодательством Российской Федерации.

Органы государственной власти, наделенные в соответствии с настоящим Законом полномочиями по распоряжению сведениями, составляющими государственную тайну, *обязаны контролировать эффективность защиты* этих сведений во всех подчиненных и подведомственных им органах государственной власти, на предприятиях, в учреждениях и организациях, осуществляющих работу с ними.

Федеральным законом от 6 октября 1997 г. N 131-ФЗ часть третья [статьи 31](#) настоящего Закона изложена в новой редакции. См. текст части третьей в предыдущей редакции.

Контроль за обеспечением защиты государственной тайны в Администрации Президента Российской Федерации, в аппаратах палат Федерального Собрания, Правительства Российской Федерации организуется их руководителями.

Контроль за обеспечением защиты государственной тайны в судебных органах и органах прокуратуры организуется руководителями этих органов.

Статья 32. Прокурорский надзор

Надзор за соблюдением законодательства при обеспечении защиты государственной тайны и законностью принимаемых при этом решений *осуществляют Генеральный прокурор* Российской Федерации и подчиненные ему прокуроры.

Доступ лиц, осуществляющих прокурорский надзор, к сведениям, составляющим государственную тайну, осуществляется в соответствии со [статьей 25](#) настоящего Закона.

Президент Российской Федерации Б.Ельцин
Москва, Дом Советов России
21 июля 1993 года № 5485-1

П-06. Защита от несанкционированного доступа к информации. Термины и определения**ГОСТЕХКОМИССИЯ РОССИИ****Руководящий документ****ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ.****ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ**

Настоящий руководящий документ устанавливает термины и определения понятий в области защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации.

Установленные термины обязательны для применения во всех видах документации.

Для каждого понятия установлен один термин. Применение синонимов термина не допускается.

Для отдельных терминов даны (в скобках) краткие формы, которые разрешается применять в случаях, исключающих возможность их различного толкования.

Для справок приведены иностранные эквиваленты русских терминов на английском языке, а также алфавитные указатели терминов на русском и английском языках.

1. 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 Примечание. Под штатными средствами понимается совокупность программного, микропрограммного и технического обес-
5. Защита от несанкционированного доступа (Защита от НСД) Protection from unauthorized Access	Предотвращение или существенное затруднение несанкционированного доступа
6. Субъект доступа (Субъект) Access subject	Лицо или процесс, действия которого 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 violator'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

Термин	Определение
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
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, предназначенное для предотвращения или существенного затруднения 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)
26. Многоуровневая защита Multilevel security	Защита, обеспечивающая разграничение доступа субъектов с различными правами доступа к объектам различных уровней конфиденциальности
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 (ядро защиты) Security kernel	Технические, программные и микропрограммные элементы комплекса средств защиты, реализующие концепцию диспетчера доступа
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

Термин	Определение
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
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. Алфавитный указатель терминов на русском языке

№ страницы

Администратор защиты	29
Аутентификация	17
Безопасность информации	21
Верификация	31
Дискреционное управление доступом	24
Диспетчер доступа (ядро защиты)	28
Доступ к информации	1
Защита от несанкционированного доступа	5
Защищенное средство вычислительной техники (защищенная автоматизированная система)	18
Идентификатор доступа	14
Идентификация	15
Класс защищенности средств вычислительной техники автоматизированной системы	32
Комплекс средств защиты	12
Конфиденциальная информация	23
Концепция диспетчера доступа	27
Мандатное управление доступом	25
Матрица доступа	8
Метка конфиденциальности	30
Многоуровневая защита	26
Модель защиты	20
Модель нарушителя правил разграничения доступа	11
Нарушитель правил разграничения доступа	10
Несанкционированный доступ к информации	4
Объект доступа	7
Пароль	16
Показатель защищенности средств вычислительной техники	33
Правила разграничения доступа	2
Санкционированный доступ к информации	3
Сертификат защиты	37
Сертификация уровня защиты	38
Система защиты информации от несанкционированного доступа	35
Система защиты секретной информации	34
Система разграничения доступа	13
Средство защиты от несанкционированного доступа	19
Средство криптографической защиты информации	36
Субъект доступа	6
Уровень полномочий субъекта доступа	9
Целостность информации	22

3. Алфавитный указатель терминов на английском языке

№ страницы

Access identifier	4
Access matrix	8
Access object	7
Access subject	6
Access to information	1
Authorized access to information	3
Authentication	17
Cryptographic information protection facility	36
Discretionary access control	24
Identification	15
Information integrity	22
Information security	21
Mandatory access control	25
Multilevel security	26
Password	16
Protection certificate	37
Protection class of computer systems	32
Protection criterion of computer systems	33
Protection facility	19
Protection from unauthorized access -	5
Protection level certification	38
Protection model	20
Reference monitor concept	27
Secret information security system	34
Security administrator	29
Security kernel	28
Security policy	2
Security policy realization	13
Security policy violator :	10
Security policy violator's model	11
Sensitive information	23
Sensitivity label	30
Subject privilege	9
System of protection from unauthorized access to information	35
Trusted computing base	12
Trusted computer system	18
Unauthorized access to information	4
Verification	31

П-07. Доктрина информационной безопасности РФ**ДОКТРИНА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ**

19.09.2000

Доктрина информационной безопасности Российской Федерации представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации.

Настоящая Доктрина служит основой для:

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

Настоящая Доктрина развивает концепцию национальной безопасности Российской Федерации применительно к информационной сфере.

Глава 1. Информационная безопасность Российской Федерации**Статья 1. Национальные интересы Российской Федерации в информационной сфере и их обеспечение**

Современный этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений. Информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации. Национальная безопасность Российской Федерации существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать.

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

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

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

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

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

Выделяются четыре основные составляющие национальных интересов Российской Федерации в информационной сфере.

Первая составляющая национальных интересов Российской Федерации в информационной сфере включает в себя соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.

Для достижения этого требуется:

- повысить эффективность использования информационной инфраструктуры в интересах общественного развития, консолидации российского общества, духовного возрождения многонационального народа Российской Федерации;

- усовершенствовать систему формирования, сохранения и рационального использования информационных ресурсов, составляющих основу научно-технического и духовного потенциала Российской Федерации;

- обеспечить конституционные права и свободы человека и гражданина свободно искать, получать, передавать, производить и распространять информацию любым законным способом, получать достоверную информацию о состоянии окружающей среды;

- обеспечить конституционные права и свободы человека и гражданина на личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, на защиту своей чести и своего доброго имени;

- укрепить механизмы правового регулирования отношений в области охраны интеллектуальной собственности, создать условия для соблюдения установленных федеральным законодательством ограничений на доступ к конфиденциальной информации;

- гарантировать свободу массовой информации и запрет цензуры;

- не допускать пропаганду и агитацию, которые способствуют разжиганию социальной, расовой, национальной или религиозной ненависти и вражды;

- обеспечить запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия и другой информации, доступ к которой ограничен федеральным законодательством.

Вторая составляющая национальных интересов Российской Федерации в информационной сфере включает в себя информационное обеспечение государственной политики Российской Федерации, связанное с доведением до российской и международной общественности достоверной информации о государственной политике Российской Федерации, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам.

Для достижения этого требуется:

- укреплять государственные средства массовой информации, расширять их возможности по своевременному доведению достоверной информации до российских и иностранных граждан;

- интенсифицировать формирование открытых государственных информационных ресурсов, повысить эффективность их хозяйственного использования.

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

Для достижения этого требуется:

- развивать и совершенствовать инфраструктуру единого информационного пространства Российской Федерации;
- развивать отечественную индустрию информационных услуг и повышать эффективность использования государственных информационных ресурсов;
- развивать производство в Российской Федерации конкурентоспособных средств и систем информатизации, телекоммуникации и связи, расширять участие России в международной кооперации производителей этих средств и систем;
- обеспечить государственную поддержку отечественных фундаментальных и прикладных исследований, разработок в сферах информатизации, телекоммуникации и связи.

Четвертая составляющая национальных интересов Российской Федерации в информационной сфере включает в себя защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России.

В этих целях необходимо:

- повысить безопасность информационных систем, включая сети связи, прежде всего безопасность первичных сетей связи и информационных систем федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, финансово-кредитной и банковской сфер, сферы хозяйственной деятельности, а техники, систем управления войсками и оружием, экологически опасными и экономически важными производствами;
- интенсифицировать развитие отечественного производства аппаратных и программных средств государственную тайну;
- расширять международное сотрудничество Российской Федерации в области развития и безопасного использования информационных ресурсов, противодействия угрозе развязывания противоборства в информационной сфере.

Статья 2. Виды угроз информационной безопасности Российской Федерации

По своей общей направленности угрозы информационной безопасности Российской Федерации подразделяются на следующие виды:

- угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;
- угрозы информационному обеспечению государственной политики Российской Федерации;
- угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и иных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.

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

- принятие федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации нормативных правовых актов, ущемляющих конституционные права и свободы граждан в области духовной жизни и информационной деятельности; создание монополий на формирование, получение и распространение информации в Российской Федерации, в том числе с использованием телекоммуникационных систем;
- противодействие, в том числе со стороны криминальных структур, реализации гражданами своих конституционных прав на личную и семейную тайну, тайну переписки, телефонных переговоров и иных сообщений;
- нерациональное, чрезмерное ограничение доступа к общественно необходимой информации; противоправное применение специальных средств воздействия на индивидуальное, групповое и общественное сознание;

- неисполнение федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, органами местного самоуправления, организациями и гражданами требований федерального законодательства, регулирующего отношения в информационной сфере;

- неправомерное ограничение доступа граждан к открытым информационным ресурсам федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, к открытым архивным материалам, к другой открытой социально значимой информации;

- дезорганизация и разрушение системы накопления и сохранения культурных ценностей, включая архивы;

- нарушение конституционных прав и свобод человека и гражданина в области массовой информации;

- вытеснение российских информационных агентств, средств массовой информации с внутреннего информационного рынка и усиление зависимости духовной, экономической и политической сфер общественной жизни России от зарубежных информационных структур;

- девальвация духовных ценностей, пропаганда образцов массовой культуры, основанных на культе насилия, на духовных и нравственных ценностях, противоречащих ценностям, принятым в российском обществе;

- снижение духовного, нравственного и творческого потенциала населения России, что существенно осложнит подготовку трудовых ресурсов для внедрения и использования новейших технологий, в том числе информационных;

- манипулирование информацией (дезинформация, сокрытие или искажение информации).

Угрозами информационному обеспечению государственной политики Российской Федерации могут являться:

- монополизация информационного рынка России, его отдельных секторов отечественными и зарубежными информационными структурами;

- блокирование деятельности государственных средств массовой информации по информированию российской и зарубежной аудитории;

- низкая эффективность информационного обеспечения государственной политики Российской Федерации вследствие дефицита квалифицированных кадров, отсутствия системы формирования и реализации государственной информационной политики.

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

- противодействие доступу Российской Федерации к новейшим информационным технологиям, взаимовыгодному и равноправному участию российских производителей в мировом разделении труда в индустрии информационных услуг, средств информатизации, телекоммуникации и связи, информационных продуктов, а также создание условий для

- усиления технологической зависимости России в области современных информационных технологий;

- закупка органами государственной власти импортных средств информатизации, телекоммуникации и связи при наличии отечественных аналогов, не уступающих по своим характеристикам зарубежным образцам;

- вытеснение с отечественного рынка российских производителей средств информатизации, телекоммуникации и связи;

- увеличение оттока за рубеж специалистов и правообладателей интеллектуальной собственности.

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

- противоправные сбор и использование информации;
- нарушения технологии обработки информации;
- внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;
- разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;
- уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;
- воздействие на пароль и о-ключевые системы защиты автоматизированных систем обработки и передачи информации;
- компрометация ключей и средств криптографической защиты информации;
- утечка информации по техническим каналам;
- внедрение электронных устройств для перехвата средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти, предприятий, учреждений и организаций независимо от формы собственности;
- уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;
- перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации;
- использование сертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии российской информационной инфраструктуры;
- несанкционированный доступ к информации, находящейся в банках и базах данных;
- нарушение законных ограничений на распространение информации.

Статья 3. Источники угроз информационной безопасности Российской Федерации

Источники угроз информационной безопасности Российской Федерации подразделяются на внешние и внутренние.

К внешним источникам относятся:

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

К внутренним источникам относятся:

- критическое состояние отечественных отраслей промышленности;

- неблагоприятная криминогенная обстановка, сопровождающаяся тенденциями сращивания государственных и криминальных структур в информационной сфере, получения криминальными структурами доступа к конфиденциальной информации, усиления влияния организованной преступности на жизнь общества, снижения степени защищенности законных интересов граждан, общества и государства в информационной сфере; недостаточная координация деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации по формированию и реализации единой государственной политики в области обеспечения информационной безопасности Российской Федерации;

- недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика;

- неразвитость институтов гражданского общества и недостаточный государственный контроль за развитием информационного рынка России; недостаточное финансирование мероприятий по обеспечению информационной безопасности Российской Федерации;

- недостаточная экономическая мощь государства; снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности;

- недостаточная активность федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации в информировании общества о своей деятельности, в разъяснении принимаемых решений, в формировании открытых государственных ресурсов и развитии системы доступа к ним граждан;

- отставание России от ведущих стран мира по уровню информатизации федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления, кредитно-финансовой сферы, промышленности, сельского хозяйства, образования, здравоохранения, сферы услуг и быта граждан.

Статья 4. Состояние информационной безопасности Российской Федерации и основные задачи по ее обеспечению

За последние годы в Российской Федерации реализован комплекс мер по совершенствованию обеспечения ее информационной безопасности.

Начато формирование базы правового обеспечения информационной безопасности. Приняты Закон Российской Федерации «О государственной тайне», Основы законодательства Российской Федерации об Архивном фонде Российской Федерации и архивах, федеральные законы «Об информации, информатизации и защите информации», «Об участии в международном информационном обмене», ряд других законов, развернута работа по созданию механизмов их реализации, подготовке законопроектов, регламентирующих общественные отношения в информационной сфере.

Осуществлены мероприятия по обеспечению информационной безопасности в федеральных органах государственной власти, органах государственной власти субъектов Российской Федерации, на предприятиях, в учреждениях и организациях независимо от формы собственности. Развернуты работы по созданию защищенной информационно-телекоммуникационной системы специального назначения в интересах органов власти.

Успешному решению вопросов обеспечения информационной безопасности Российской Федерации способствуют государственная система защиты информации, система защиты государственной тайны, системы лицензирования деятельности в области защиты государственной тайны и системы сертификации средств защиты информации.

Вместе с тем анализ состояния информационной безопасности Российской Федерации показывает, что ее уровень не в полной мере соответствует потребностям общества и государства.

Современные условия политического и социально-экономического развития страны вызывают обострение противоречий между потребностями общества в расширении свободного обмена информацией и необходимостью сохранения отдельных регламентированных ограничений на ее распространение.

Противоречивость и неразвитость правового регулирования общественных отношений в информационной сфере приводят к серьезным негативным последствиям. Так, недостаточность нормативного правового регулирования отношений в области реализации возможностей конституционных ограничений свободы массовой информации в интересах защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороноспособности страны и безопасности государства существенно затрудняет поддержание необходимого баланса интересов личности, общества и государства в информационной сфере. Несовершенное нормативное правовое регулирование отношений в области массовой информации затрудняет формирование на территории Российской Федерации конкурентоспособных российских информационных агентств и средств массовой информации.

Необеспеченность прав граждан на доступ к информации, манипулирование информацией вызывают негативную реакцию населения, что в ряде случаев ведет к дестабилизации социально-политической обстановки в обществе.

Закрепленные в Конституции Российской Федерации права граждан на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки практически не имеют достаточного правового, организационного и технического обеспечения. Неудовлетворительно организована защита собираемых федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, органами местного самоуправления данных о физических лицах (персональных данных).

Нет четкости при проведении государственной политики в области формирования российского информационного пространства, развития системы массовой информации, организации международного информационного обмена и интеграции информационного пространства России в мировое информационное пространство, что создает условия для вытеснения российских информационных агентств, средств массовой информации с внутреннего информационного рынка и деформации структуры международного информационного обмена.

Недостаточна государственная поддержка деятельности российских информационных агентств по продвижению их продукции на зарубежный информационный рынок.

Ухудшается ситуация с обеспечением сохранности сведений, составляющих государственную тайну.

Серьезный урон нанесен кадровому потенциалу научных и производственных коллективов, действующих в области создания средств информатизации, телекоммуникации и связи, в результате массового ухода из этих коллективов наиболее квалифицированных специалистов.

Отставание отечественных информационных технологий вынуждает федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации и органы местного самоуправления при создании информационных систем идти по пути закупок импортной техники и привлечения иностранных фирм, из-за чего повышается вероятность несанкционированного доступа к обрабатываемой информации и возрастает зависимость российских производителей компьютерной и телекоммуникационной техники, а также программного обеспечения.

В связи с интенсивным внедрением зарубежных информационных технологий в сферы деятельности личности, общества и государства, а также с широким применением открытых информационно-телекоммуникационных систем, интеграцией отечественных информационных систем и международных информационных систем возросли угрозы применения «информационного оружия» против информационной инфраструктуры России. Работы по адекватному комплексному противодействию этим угрозам ведутся при недостаточной координации и слабом бюджетном финансировании. Недостаточное внимание уделяется развитию средств космической разведки и радиоэлектронной борьбы.

Сложившееся положение дел в области обеспечения информационной безопасности Российской Федерации требует безотлагательного решения таких задач, как:

- разработка основных направлений государственной политики в области обеспечения информационной безопасности Российской Федерации, а также мероприятий и механизмов, связанных с реализацией этой политики;

- развитие и совершенствование системы обеспечения информационной безопасности Российской Федерации, реализующей единую государственную политику в этой области, включая совершенствование форм, методов и средств выявления, оценки и прогнозирования угроз информационной безопасности Российской Федерации, а так же системы противодействия этим угрозам;
- разработка федеральных целевых программ обеспечения информационной безопасности Российской Федерации;
- разработка критериев и методов оценки эффективности систем и средств обеспечения информационной безопасности Российской Федерации, а также сертификации этих систем и средств;
- совершенствование нормативной правовой базы обеспечения информационной безопасности Российской Федерации, включая механизмы реализации прав граждан на получение информации и доступ к ней, формы и способы реализации правовых норм, касающихся взаимодействия государства со средствами массовой информации;
- установление ответственности должностных лиц федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, юридических лиц и граждан за соблюдение требований информационной безопасности; координация деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, предприятий, учреждений и организаций независимо от формы собственности в области обеспечения безопасности Российской Федерации с учетом современной геополитической ситуации, условий политического и социально-экономического развития России и реальности угроз применения «информационного оружия»;
- разработка и создание механизмов формирования и реализации государственной информационной политики России;
- разработка методов повышения эффективности участия государства в формировании информационной политики государственных телерадиовещательных организаций, других государственных средств массовой информации;
- обеспечение технологической независимости Российской Федерации в важнейших областях информатизации, телекоммуникации и связи, определяющих ее безопасность, и в первую очередь в области создания специализированной вычислительной техники для образцов вооружения и военной техники;
- разработка современных методов и средств защитных технологий, и прежде всего используемых в системах управления войсками и оружием, экологически опасными и экономически важными производствами;
- развитие и совершенствование государственной системы защиты информации и системы защиты государственной тайны;
- создание и развитие современной защищенной технологической основы управления государством в мирное время, в чрезвычайных ситуациях и в военное время;
- расширение взаимодействия с международными и зарубежными органами и организациями при решении научно-технических и правовых вопросов обеспечения безопасности информации, передаваемой с помощью международных телекоммуникационных систем и систем связи; обеспечение условий для активного развития российской информационной инфраструктур и систем; создание единой системы подготовки кадров в области информационной безопасности и информационных технологий.

ГЛАВА 2. Методы обеспечения информационной безопасности Российской Федерации

Статья 5. Общие методы обеспечения информационной безопасности Российской Федерации

Общие методы обеспечения информационной безопасности Российской Федерации разделяются на правовые, организационно-технические и экономические.

К правовым методам обеспечения информационной безопасности Российской Федерации относится разработка нормативных правовых актов, регламентирующих отношения в информационной сфере, и нормативных методических документов по вопросам обеспечения информационной безопасности Российской Федерации.

Наиболее важными направлениями этой деятельности являются:

Внесение изменений и дополнений в законодательство РФ, регулирующее отношения в области обеспечения информационной безопасности, в целях создания и совершенствования системы обеспечения информационной безопасности Российской Федерации, устранения внутренних противоречий в федеральном законодательстве, противоречий, связанных с международными соглашениями, к которым присоединилась Российская Федерация, и противоречий между федеральными законодательными актами и законодательными актами субъектов Российской Федерации, а также в целях конкретизации правовых норм, устанавливающих ответственность за правонарушения в области обеспечения информационной безопасности Российской Федерации;

- законодательное разграничение полномочий в области обеспечения информационной безопасности Российской Федерации между федеральными органами государственной власти и органами государственной власти субъектов Российской Федерации, определение целей, задач и механизмов участия в этой деятельности общественных объединений, организаций и граждан;

- разработка и принятие нормативных правовых актов Российской Федерации, устанавливающих ответственность юридических и физических лиц за несанкционированный доступ к информации, ее противоправное копирование, искажение и противоправное использование, преднамеренное распространение недостоверной информации, противоправное раскрытие конфиденциальной информации, использование в преступных и корыстных целях служебной информации или информации, содержащей коммерческую тайну;

- уточнение статуса иностранных информационных агентств, средств массовой информации и журналистов, а также инвесторов при привлечении иностранных инвестиций для развития информационной инфраструктуры России;

- законодательное закрепление приоритета развития национальных сетей связи и отечественного производства космических спутников связи;

- определение статуса организаций, предоставляющих услуги глобальных информационно-телекоммуникационных сетей на территории Российской Федерации, и правовое регулирование деятельности этих организаций;

- создание правовой базы для формирования в Российской Федерации региональных структур обеспечения информационной безопасности.

Организационно-техническими методами обеспечения информационной безопасности Российской Федерации являются:

- создание и совершенствование системы обеспечения информационной безопасности Российской Федерации;

- усиление правоприменительной деятельности федеральных органов исполнительной власти, органы субъектов Российской Федерации, включая предупреждение и пресечение правонарушений в информационной сфере, а также выявление, изобличение и привлечение к ответственности лиц, совершивших преступления и другие правонарушения в этой сфере;

- разработка, использование и совершенствование средств защиты информации и методов контроля эффективности этих средств, развитие защищенных телекоммуникационных систем, повышение надежности специального программного обеспечения;

- создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи;

- выявление технических устройств и программ, представляющих опасность для нормального функционирования информационно-телекоммуникационных систем, предотвращение

перехвата информации по техническим каналам, применение криптографических средств защиты информации при ее хранении, обработке и передаче по каналам связи, контроль за выполнением специальных требований по защите информации;

- сертификация средств защиты информации, лицензирование деятельности в области защиты государственной тайны, стандартизация способов и средств защиты информации;
- совершенствование системы сертификации телекоммуникационного оборудования и программного обеспечения автоматизированных систем обработки информации по требованиям информационной безопасности;
- контроль за действиями персонала в защищенных безопасности;
- формирование системы мониторинга показателей и характеристик информационной безопасности Российской Федерации в наиболее важных сферах жизни и деятельности общества и государства.

Экономические методы обеспечения информационной безопасности Российской Федерации включают в себя:

- разработку программ обеспечения информационной безопасности Российской Федерации и определение порядка их финансирования;
- совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-технических методов защиты информации, создание системы страхования информационных рисков физических и юридических лиц.

Статья 6. Особенности обеспечения информационной безопасности Российской Федерации в различных сферах общественной жизни

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

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

В сфере экономики

Обеспечение информационной безопасности Российской Федерации в сфере экономики играет ключевую роль в обеспечении национальной безопасности Российской Федерации.

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

- система государственной статистики;
- кредитно-финансовая система;
- информационные и учетные автоматизированные системы подразделений федеральных органов исполнительной власти, обеспечивающих деятельность общества и государства в сфере экономики;
- системы бухгалтерского учета предприятий, учреждений и организаций независимо от формы собственности;
- системы сбора, обработки, хранения и передачи финансовой, биржевой, налоговой, таможенной информации и информации о внешнеэкономической деятельности государства, а также предприятий, учреждений и организаций независимо от формы собственности.

Переход к рыночным отношениям в экономике вызвал появление на внутреннем российском рынке товаров и услуг множества отечественных и зарубежных коммерческих структур - производителей и потребителей информации, средств информатизации и защиты информации.

Бесконтрольная деятельность этих структур по созданию и защите систем сбора, обработки, хранения и передачи статистической, финансовой, биржевой, налоговой, таможенной информации создает реальную угрозу безопасности России в экономической сфере. Аналогичные угрозы возникают при бесконтрольном привлечении иностранных фирм к созданию подобных систем, поскольку при этом складываются благоприятные условия для несанкционированного доступа к конфиденциальной экономической информации и для контроля за процессами ее передачи и обработки со стороны иностранных спецслужб.

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

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

Недостаточность нормативной правовой базы, определяющей ответственность хозяйствующих субъектов за недостоверность или сокрытие сведений об их коммерческой деятельности, о потребительских свойствах производимых ими товаров и услуг, о результатах их хозяйственной деятельности, об инвестициях и тому подобном препятствует нормальному функционированию хозяйствующих субъектов. В то же время существенный экономический ущерб хозяйствующим субъектам может быть нанесен вследствие разглашения информации, содержащей коммерческую тайну. В системах сбора, обработки, хранения и передачи финансовой, биржевой, налоговой, таможенной информации наиболее опасны противоправное копирование информации и ее искажение вследствие преднамеренных или случайных нарушений технологии работы с информацией, несанкционированного доступа к ней. Это касается и федеральных органов исполнительной власти, занятых формированием и распространением информации о внешнеэкономической деятельности Российской Федерации.

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

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

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

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

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

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

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

В сфере внутренней политики

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

- конституционные права и свободы человека и гражданина;

- конституционный строй, национальное согласие, стабильность государственной власти, суверенитет и территориальная целостность Российской Федерации;
- открытые информационные ресурсы федеральных органов исполнительной власти и средств массовой информации.

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

- нарушение конституционных прав и свобод граждан, реализуемых в информационной сфере;
- недостаточное правовое регулирование отношений в области прав различных политических сил на использование средств массовой информации для пропаганды своих идей;
- распространение дезинформации о политике Российской Федерации, деятельности федеральных органов государственной власти, событиях, происходящих в стране и за рубежом;
- деятельность общественных объединений, направленная на насильственное изменение основ конституционного строя и нарушение целостности Российской Федерации, разжигание социальной, расовой, национальной и религиозной вражды, на распространение этих идей в средствах массовой информации.

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

- создание системы противодействия монополизации отечественными и зарубежными структурами;
- активизация контрпропагандистской деятельности, направленной на предотвращение негативных последствий распространения дезинформации о внутренней политике России.

В сфере внешней политики

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

- информационные ресурсы федеральных органов исполнительной власти, реализующих внешнюю политику Российской Федерации, российских представительств и организаций за рубежом, представительств Российской Федерации при международных организациях;
- информационные ресурсы представительств федеральных органов исполнительной власти, реализующих внешнюю политику Российской Федерации, на территориях субъектов Российской Федерации;
- информационные ресурсы российских предприятий, учреждений и организаций, подведомственных федеральным органам исполнительной власти, реализующим внешнюю политику Российской Федерации;
- блокирование деятельности российских средств массовой информации по разъяснению зарубежной аудитории целей и основных направлений государственной политики Российской Федерации, ее мнения по социально значимым событиям российской и международной жизни.

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

- информационное воздействие иностранных политических, экономических, военных и информационных структур на разработку и реализацию стратегии внешней политики Российской Федерации;
- распространение за рубежом дезинформации о внешней политике Российской Федерации;
- нарушение прав российских граждан и юридических в информационной сфере за рубежом;
- попытки несанкционированного доступа к информации и воздействия на информационные ресурсы, информационную инфраструктуру федеральных органов исполнительной власти, реализующих внешнюю политику Российской Федерации, российских представительств и организаций за рубежом, представительств Российской Федерации при международных организациях.

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

- нарушение установленного порядка сбора, обработки, хранения и передачи информации в федеральных органах исполнительной власти, реализующих внешнюю политику Российской Федерации, и на подведомственных им предприятиях, в учреждениях и организациях;
- информационно-пропагандистская деятельность политических сил, общественных объединений, средств массовой информации и отдельных лиц искажающая стратегию и тактику внешнеполитической деятельности Российской Федерации;
- недостаточная информированность населения о внешнеполитической деятельности Российской Федерации.

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

- разработка основных направлений государственной политики в области совершенствования информационного обеспечения внешнеполитического курса Российской Федерации;
- разработка и реализация комплекса мер по усилению информационной безопасности информационной инфраструктуры федеральных органов исполнительной власти, реализующих внешнюю политику Российской Федерации, российских представительств и организаций за рубежом, представительств Российской Федерации при международных организациях;
- создание российским представительством и организациям за рубежом условий для работы по нейтрализации распространяемой там дезинформации о внешней политике Российской Федерации;
- в совершенствование информационного обеспечения работы по противодействию нарушениям прав и свобод российских граждан и юридических лиц за рубежом;
- совершенствование информационного обеспечения субъектов Российской Федерации по вопросам внешнеполитической деятельности, которые входят в их компетенцию.

В области науки и техники

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

- результаты фундаментальных, поисковых и прикладных научных исследований, потенциально важные для научно-технического, технологического и социально-экономического развития страны, включая сведения, утрата которых может нанести ущерб национальным интересам и престижу Российской Федерации;
- открытия, незапатентованные технологии, промышленные образцы, полезные модели и экспериментальное оборудование;
- научно-технические кадры и система их подготовки;
- системы управления сложными исследовательскими комплексами (ядерными реакторами, ускорителями элементарных частиц, плазменными генераторами и другими).

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

- стремление развитых иностранных государств получить противоправный доступ к научно-техническим ресурсам России для использования полученных российскими учеными результатов в собственных интересах;
- создание льготных условий на российском рынке для иностранной научно-технической продукции и стремление развитых стран в то же время ограничить развитие научно-технического потенциала России (скупка акций передовых предприятий с их последующим репродуцированием, сохранение экспортно-импортных ограничений и тому подобное);
- политику западных стран, направленную на дальнейшее разрушение унаследованного от СССР единого научно-технического пространства государств-участников Содружества Независимых Государств за счет переориентации на западные страны их научно-технических связей, а также отдельных, наиболее перспективных научных коллективов;

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

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

- сохраняющуюся сложную экономическую ситуацию в России, ведущую к резкому снижению финансирования научно-технической деятельности, временному падению престижа научно-технической сферы, утечке за рубеж идей и передовых разработок;
- неспособность предприятий национальных отраслей электронной промышленности производить на базе новейших достижений микроэлектроники, передовых информационных технологий конкурентоспособную наукоемкую продукцию, позволяющую обеспечить достаточный уровень технологической независимости России от зарубежных стран, что приводит к вынужденному широкому использованию импортных программно-аппаратных средств при создании и развитии в России информационной инфраструктуры;
- серьезные проблемы в области патентной защиты результатов научно-технической деятельности российских ученых;
- сложности реализации мероприятий по защите информации, особенно на акционированных предприятиях, в научно-технических учреждениях и организациях.

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

В сфере духовной жизни

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

- достоинство личности, свобода совести, включая право свободно выбирать, иметь и распространять религиозные и иные убеждения и действовать в соответствии с ними, свобода мысли и слова (за исключением пропаганды или агитации, возбуждающих социальную, расовую, национальную или религиозную ненависть и вражду), а также свобода литературного, художественного, научного, технического и других видов творчества, преподавания;
- свобода массовой информации;
- неприкосновенность частной жизни, личная и семейная тайна;
- русский язык как фактор духовного единения народов многонациональной России, язык межгосударственного общения народов государств-участников Содружества Независимых Государств;
- языки, нравственные ценности и культурное наследие народов и народностей Российской Федерации;
- объекты интеллектуальной собственности.

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

- деформация системы массового информирования как за счет монополизации средств массовой информации, так и за счет неконтролируемого расширения сектора зарубежных средств массовой информации в отечественном информационном пространстве;
- ухудшение состояния и постепенный упадок объектов российского культурного наследия, включая архивы, музейные фонды, библиотеки, памятники архитектуры, ввиду недостаточного финансирования соответствующих программ и мероприятий;
- возможность нарушения общественной стабильности, нанесение вреда здоровью и жизни граждан вследствие деятельности религиозных объединений, проповедующих религиозный фундаментализм, а также тоталитарных религиозных сект;
- использование зарубежными специальными службами средств массовой информации, действующих на территории Российской Федерации, для нанесения ущерба обороноспособности страны и безопасности государства, распространения дезинформации;
- неспособность современного гражданского общества России обеспечить формирование у подрастающего поколения и поддержание в обществе общественно необходимых нравственных ценностей, патриотизма и гражданской ответственности за судьбу страны.

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

- развитие в России основ гражданского общества;
- создание социально-экономических условий для осуществления творческой деятельности и функционирования учреждений культуры;
- выработка цивилизованных форм и способов общественного контроля за формированием в обществе духовных ценностей, отвечающих национальным интересам страны, воспитанием патриотизма и гражданской ответственности за ее судьбу;
- совершенствование законодательства Российской Федерации, регулирующего отношения в области конституционных ограничений прав и свобод человека и гражданина;
- государственная поддержка мероприятий по сохранению и возрождению культурного наследия народов и народностей Российской Федерации;
- формирование правовых и организационных механизмов обеспечения конституционных прав и свобод граждан, повышения их правовой культуры в интересах противодействия сознательному или непреднамеренному нарушению этих конституционных прав и свобод в сфере духовной жизни;
- разработка действенных организационно-правовых механизмов доступа средств массовой информации и граждан к открытой информации о деятельности федеральных органов государственной власти и общественных объединений, обеспечение достоверности сведений о социально значимых событиях общественной жизни, распространяемых через средства массовой информации;
- разработка специальных правовых и организационных механизмов недопущения противоправных информационно-психологических воздействий на массовое сознание общества, неконтролируемой коммерциализации культуры и науки, а также обеспечивающих сохранение культурных и исторических ценностей народов и народностей Российской Федерации, рациональное использование накопленных обществом информационных ресурсов, составляющих национальное достояние;
- введение запрета на использование эфирного времени в электронных средствах массовой информации для проката программ, пропагандирующих насилие и жестокость, антиобщественное поведение;
- противодействие негативному влиянию иностранных религиозных организаций и миссионеров.

В общегосударственных информационных и телекоммуникационных системах

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

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

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

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

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

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

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

- вынужденное в силу объективного отставания отечественной промышленности использование при создании и развитии информационных и телекоммуникационных систем импортных программно-аппаратных средств;

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

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

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

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

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

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

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

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

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

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

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

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

- лицензирование деятельности организаций в области защиты информации;
- аттестация объектов информатизации по выполнению требований обеспечения защиты информации при проведении работ, связанных с использованием сведений, составляющих государственную тайну;
- сертификация средств защиты информации и контроля эффективности их использования, а также защищенности информации от утечки по техническим каналам систем и средств информатизации и связи;
- введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите;
- создание и применение информационных и автоматизированных систем управления в защищенном исполнении.

В сфере обороны

К объектам обеспечения информационной безопасности Российской Федерации в сфере обороны относятся:

- информационная инфраструктура центральных органов военного управления и органов военного управления видов Вооруженных Сил Российской Федерации и родов войск, объединений, соединений, воинских частей и организаций, входящих в Вооруженные Силы Российской Федерации, научно-исследовательских учреждений Министерства обороны Российской Федерации;
- информационные ресурсы предприятий оборонного комплекса и научно-исследовательских учреждений, выполняющих государственные оборонные заказы либо занимающихся оборонной проблематикой;
- программно-технические средства автоматизированных и автоматических систем управления войсками и оружием, вооружения и военной техники, оснащенных средствами информатизации;
- информационные ресурсы, системы связи и информационная инфраструктура других войск, воинских формирований и органов.

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

- все виды разведывательной деятельности зарубежных государств;
- информационно-технические воздействия (в том числе радиоэлектронная борьба, проникновение в компьютерные сети) со стороны вероятных противников;
- диверсионно-подрывная деятельность специальных служб иностранных государств, осуществляемая методами информационно-психологического воздействия;
- деятельность иностранных политических, экономических и военных структур, направленная против интересов Российской Федерации в сфере обороны.

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

- нарушение установленного регламента сбора, обработки, хранения и передачи информации, находящейся в штабах и учреждениях Министерства обороны Российской Федерации, на предприятиях оборонного комплекса;
- преднамеренные действия, а также ошибки персонала информационных и телекоммуникационных систем специального назначения;
- ненадежное функционирование информационных и телекоммуникационных систем специального назначения;
- возможная информационно-пропагандистская деятельность, подрывающая престиж Вооруженных Сил Российской Федерации и их боеготовность;
- нерешенность вопросов защиты интеллектуальной собственности предприятий оборонного комплекса, приводящая к утечке за рубеж ценнейших государственных информационных ресурсов;
- нерешенность вопросов социальной защиты военнослужащих и членов их семей.

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

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

- систематическое выявление угроз и их источник, структуризация целей обеспечения информационной безопасности в сфере обороны и определение соответствующих практических задач;
- проведение сертификации общего и специального программного обеспечения, пакетов прикладных программ и средств защиты информации в существующих и создаваемых автоматизированных системах управления военного назначения и системах связи, имеющих в своем составе элементы вычислительной техники;
- постоянное совершенствование средств защиты информации от несанкционированного доступа, развитие защищенных систем связи и управления войсками и оружием, повышение надежности специального программного обеспечения;
- совершенствование структуры функциональных органов системы обеспечения информационной безопасности в сфере обороны и координация их взаимодействия;
- совершенствование приемов и способов стратегической и оперативной маскировки, разведки и радиоэлектронной борьбы, методов и средств активного противодействия информационно-пропагандистским и психологическим операциям вероятного противника;
- подготовка специалистов в области обеспечения информационной безопасности в сфере обороны.

В правоохранительной и судебной сферах

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

- информационные ресурсы федеральных органов исполнительной власти, реализующих правоохранительные функции, судебных органов, их информационно-вычислительных центров, научно-исследовательских учреждений и учебных заведений, содержащие специальные сведения и оперативные данные служебного характера;
- информационно-вычислительные центры, их информационное, техническое, программное и нормативное обеспечение;
- тура (информационно-вычислительные сети, пункты управления, узлы и линии связи).

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

- разведывательная деятельность специальных служб иностранных государств, международных преступных сообществ, организаций и групп, связанная со сбором сведений, раскрывающих задачи, планы деятельности, техническое оснащение, методы работы и места дислокации специальных подразделений и органов внутренних дел Российской Федерации;
- деятельность иностранных государственных и частных коммерческих структур, стремящихся получить несанкционированный доступ к информационным ресурсам правоохранительных и судебных органов.

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

- нарушение установленного регламента сбора, обработки, хранения и передачи информации, содержащейся в картотеках и автоматизированных банках данных и используемой для расследования преступлений;
- недостаточность законодательного и нормативного регулирования информационного обмена в правоохранительной и судебной сферах;
- отсутствие единой методологии сбора, обработки и хранения информации оперативно-разыскного, справочного, криминалистического и статистического характера;
- отказ технических средств и сбой программного обеспечения в информационных и телекоммуникационных системах;

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

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

Главными из них являются:

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

- повышение уровня профессиональной и специальной подготовки пользователей информационных систем.

В условиях чрезвычайных ситуаций

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

Особое значение для нормального функционирования указанных объектов имеет обеспечение безопасности информационной инфраструктуры страны при авариях, катастрофах и стихийных бедствиях. Соккрытие, задержка поступления, искажение и разрушение оперативной информации, несанкционированный доступ к ней отдельных лиц или групп лиц могут привести как к человеческим жертвам, так и к возникновению разного рода ложностей при ликвидации последствий чрезвычайной ситуации, связанных с особенностями информационного воздействия в экстремальных условиях: к приведению в движение больших масс людей, испытывающих психический стресс; к быстрому возникновению и распространению среди них паники и беспорядков на основе слухов, ложной или недостоверной информации.

К специфическим для данных условий направлениям обеспечения информационной безопасности относятся:

- разработка эффективной системы мониторинга объектов повышенной опасности, нарушение функционирования которых может привести к возникновению чрезвычайных ситуаций, и прогнозирования чрезвычайных ситуаций;

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

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

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

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

Статья 7. Международное сотрудничество Российской Федерации в области обеспечения информационной безопасности

Международное сотрудничество Российской Федерации в области обеспечения информационной безопасности - неотъемлемая составляющая политического, военного, экономического, культурного и других видов взаимодействия стран, входящих в мировое сообщество. Такое сотрудничество должно способствовать повышению информационной безопасности всех членов мирового сообщества, включая Российскую Федерацию.

Особенность международного сотрудничества Российской Федерации в области обеспечения информационной безопасности состоит в том, что оно осуществляется в условиях обострения международной конкуренции за обладание технологическими и информационными ресурсами, за доминирование на рынках сбыта, в условиях продолжения попыток создания

структуры международных отношений, основанной на односторонних решениях ключевых проблем мировой политики, противодействия укреплению роли России как одного из влиятельных центров формирующегося многополярного мира, усиления технологического отрыва ведущих держав мира и наращивания их возможностей для создания «информационного оружия». Все это может привести к новому этапу развертывания гонки вооружений в информационной сфере, нарастанию угрозы агентурного и оперативно-технического проникновения в Россию иностранных разведок, в том числе с использованием глобальной информационной инфраструктуры.

Основными направлениями международного сотрудничества Российской Федерации в области обеспечения информационной безопасности являются:

- запрещение разработки, распространения и применения «информационного оружия»;
- обеспечение безопасности международного информационного обмена, в том числе сохранности информации при ее передаче по национальным телекоммуникационным каналам и каналам связи;
- координация деятельности правоохранительных органов стран, входящих в мировое сообщество, по предотвращению компьютерных преступлений;
- предотвращение несанкционированного доступа к конфиденциальной информации в международных банковских телекоммуникационных сетях и системах информационного обеспечения мировой торговли, к информации международных правоохранительных организаций, ведущих борьбу с транснациональной организованной преступностью, международным терроризмом, распространением наркотиков и психотропных веществ, незаконной торговлей оружием и расщепляющимися материалами, а также торговлей людьми.

При осуществлении международного сотрудничества Российской Федерации в области обеспечения информационной безопасности особое внимание должно уделяться проблемам взаимодействия с государствами-участниками Содружества Независимых Государств.

Для осуществления этого сотрудничества по указанным основным направлениям необходимо обеспечить активное участие России во всех международных организациях, осуществляющих деятельность в области информационной безопасности, в том числе в сфере стандартизации и сертификации средств информатизации и защиты информации.

ГЛАВА 3. Основные положения государственной политики обеспечения информационной безопасности Российской Федерации и первоочередные мероприятия по ее реализации

Статья 8. Основные положения государственной политики обеспечения информационной безопасности Российской Федерации

Государственная политика обеспечения информационной безопасности Российской Федерации определяет основные направления деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации в этой области, порядок закрепления их обязанностей по защите интересов Российской Федерации в информационной сфере в рамках направлений их деятельности и базируется на соблюдении баланса интересов личности, общества и государства в информационной сфере.

Государственная политика обеспечения информационной безопасности Российской Федерации основывается на следующих основных принципах:

- соблюдение Конституции Российской Федерации, законодательства Российской Федерации, общепризнанных принципов и норм международного права при осуществлении деятельности по обеспечению информационной безопасности российской федерации;
- открытость в реализации функций федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и общественных объединений, предусматривающая информирование общества об их деятельности с учетом ограничений, установленных законодательством Российской Федерации;
- правовое равенство всех участников процесса информационного взаимодействия вне зависимости от их политического, социального и экономического статуса, основывающееся на

конституционном праве граждан на свободный поиск, получение, передачу, производство и распространение информации любым законным способом;

- приоритетное развитие отечественных современных информационных и телекоммуникационных технологий, производство технических и программных средств, способных обеспечить совершенствование национальных телекоммуникационных сетей, их подключение к глобальным информационным сетям в целях соблюдения жизненно важных интересов Российской Федерации.

Государство в процессе реализации своих функций по обеспечению информационной безопасности Российской Федерации:

- проводит объективный и всесторонний анализ и прогнозирование угроз информационной безопасности Российской Федерации, разрабатывает меры по ее обеспечению;

- организует работу законодательных (представительных) и исполнительных органов государственной власти Российской Федерации по реализации комплекса мер, направленных на предотвращение, отражение и нейтрализацию угроз информационной безопасности Российской Федерации;

- поддерживает деятельность общественных объединений, направленную на объективное информирование населения о социально значимых явлениях общественной жизни, защиту общества от искаженной и недостоверной информации;

- осуществляет контроль за разработкой, созданием, развитием, использованием, экспортом и импортом средств защиты информации посредством их сертификации и лицензирования деятельности в области защиты информации;

- проводит необходимую протекционистскую политику в отношении производителей средств информатизации и защиты информации на территории Российской Федерации и принимает меры по защите внутреннего рынка от проникновения на него некачественных средств информатизации и информационных продуктов;

- способствует предоставлению физическим и юридическим лицам доступа к мировым информационным ресурсам, глобальным информационным сетям;

- формулирует и реализует государственную информационную политику России;

- организует разработку федеральной программы обеспечения информационной безопасности Российской Федерации, объединяющей усилия государственных и негосударственных организаций в данной области;

- способствует интернационализации глобальных информационных сетей и систем, а также вхождению России в мировое информационное сообщество на условиях равноправного партнерства.

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

Это предполагает:

- оценку эффективности применения действующих законодательных и иных нормативных правовых актов в информационной сфере и выработку программы их совершенствования;

- создание организационно-правовых механизмов обеспечения информационной безопасности;

- определение правового статуса всех субъектов отношений в информационной сфере, включая пользователей информационных и телекоммуникационных систем, и установление их ответственности за соблюдение законодательства Российской Федерации в данной сфере;

- создание системы сбора и анализа данных об источниках угроз информационной безопасности Российской Федерации, а также о последствиях их осуществления;

- разработку нормативных правовых актов, определяющих организацию следствия и процедуру судебного разбирательства по фактам противоправных действий в информационной сфере, а также порядок ликвидации последствий этих противоправных действий;

- разработку составов правонарушений с учетом специфики уголовной, гражданской, административной, дисциплинарной ответственности и включение соответствующих правовых

норм в уголовный, гражданский, административный и трудовой кодексы, в законодательство Российской Федерации о государственной службе;

- совершенствование системы подготовки кадров, используемых в области обеспечения информационной безопасности Российской Федерации.

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

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

Соблюдение принципа баланса интересов граждан, общества и государства в информационной сфере предполагает законодательное закрепление приоритета этих интересов в различных областях жизнедеятельности общества, а также использование форм общественного контроля деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации. Реализация гарантий конституционных прав и свобод человека и гражданина, касающихся деятельности в информационной сфере, является важнейшей задачей государства в области информационной безопасности.

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

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

Статья 9. Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности Российской Федерации

Первоочередными мероприятиями по реализации государственной политики обеспечения информационной безопасности Российской Федерации являются:

- разработка и внедрение механизмов реализации правовых норм, регулирующих отношения в информационной сфере, а также подготовка концепции правового обеспечения информационной безопасности Российской Федерации;

- разработка и реализация механизмов повышения эффективности государственного руководства деятельностью государственных средств массовой информации, осуществления государственной информационной политики;

- принятие и реализация федеральных программ, предусматривающих формирование общедоступных архивов информационных ресурсов федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, повышение правовой культуры и компьютерной грамотности граждан, развитие инфраструктуры единого информационного пространства России, комплексное противодействие угрозам информационной войны, создание безопасных информационных технологий для систем, используемых в процессе реализации жизненно важных функций общества и государства, пресечение компьютерной преступности, создание информационно-телекоммуникационной системы специального назначения в интересах федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, обеспечение технологической независимости страны в области создания и эксплуатации информационно-телекоммуникационных систем оборонного назначения;

- развитие системы подготовки кадров, используемых в области обеспечения информационной безопасности Российской Федерации; гармонизация отечественных стандартов в области информатизации и обеспечения информационной безопасности автоматизированных систем

управления, информационных и телекоммуникационных систем общего и специального назначения.

ГЛАВА 4. Организационная основа системы обеспечения информационной безопасности Российской Федерации

Статья 10. Основные функции системы обеспечения информационной безопасности Российской Федерации

Система обеспечения информационной безопасности Российской Федерации предназначена для реализации государственной политики в данной сфере.

Основными функциями системы обеспечения информационной безопасности Российской Федерации являются:

- разработка нормативной правовой базы в области обеспечения информационной безопасности Российской Федерации;
- создание условий для реализации прав граждан и общественных объединений на разрешенную законом деятельность в информационной сфере;
- определение и поддержание баланса между потребностью, граждан, общества и государства в свободном обмене информацией и необходимыми ограничениями на распространение информации;
- оценка состояния информационной безопасности Российской Федерации, выявление источников
 - внутренних и внешних угроз информационной безопасности, определение приоритетных направлений предотвращения, отражения и нейтрализации этих угроз;
 - координация деятельности федеральных органов государственной власти и других государственных органов, решающих задачи обеспечения информационной безопасности Российской Федерации; контроль деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, государственных и межведомственных комиссий, участвующих в решении задач обеспечения информационной безопасности Российской Федерации; предупреждение, выявление и пресечение правонарушений, связанных с посягательствами на законные интересы граждан, общества и государства в информационной сфере, на осуществление судопроизводства по делам о преступлениях в этой области;
- развитие отечественной информационной инфраструктуры, а также индустрии телекоммуникационных и информационных средств, повышение их конкурентоспособности на внутреннем и внешнем рынке;
- организация разработки федеральной и региональных программ обеспечения информационной безопасности и координация деятельности по их реализации;
- проведение единой технической политики в области обеспечения информационной безопасности Российской Федерации;
- организация фундаментальных и прикладных научных исследований в области обеспечения информационной безопасности Российской Федерации;
- защита государственных информационных ресурсов, прежде всего в федеральных органах государственной власти и органах государственной власти субъектов Российской Федерации, на предприятиях оборонного комплекса;
- обеспечение контроля за созданием и использованием средств защиты информации посредством обязательного лицензирования деятельности в данной сфере и сертификации средств защиты информации;
- совершенствование и развитие единой системы подготовки кадров, используемых в области информационной безопасности Российской Федерации;
- осуществление международного сотрудничества в сфере обеспечения информационной безопасности, представление интересов Российской Федерации в соответствующих международных организациях.

Компетенция федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, других государственных органов, входящих в состав

системы обеспечения информационной безопасности Российской Федерации и ее подсистем, определяется федеральными законами, нормативными правовыми актами Президента Российской Федерации и Правительства Российской Федерации.

Функции органов, координирующих деятельность федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, других государственных органов, входящих в состав системы обеспечения информационной безопасности Российской Федерации и ее подсистем, определяются отдельными нормативными правовыми актами Российской Федерации.

Статья 11. Основные элементы организационной основы системы обеспечения информационной безопасности Российской Федерации

Система обеспечения информационной безопасности Российской Федерации является частью системы обеспечения национальной безопасности страны.

Система обеспечения информационной безопасности Российской Федерации строится на основе разграничения полномочий органов законодательной, исполнительной и судебной власти в данной сфере, а также предметов ведения федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации.

Основными элементами организационной основы системы обеспечения информационной безопасности Российской Федерации являются: Президент Российской Федерации, Совет Федерации Федерального Собрания Российской Федерации, Государственная Дума Федерального Собрания Российской Федерации, Правительство Российской Федерации, Совет Безопасности Российской Федерации, федеральные органы исполнительной власти, межведомственные и государственные комиссии, создаваемые Президентом Российской Федерации и Правительством Российской Федерации, органы исполнительной власти субъектов Российской Федерации, органы местного самоуправления, органы судебной власти, общественные объединения, граждане, принимающие в соответствии с законодательством Российской Федерации участие в решении задач обеспечения информационной безопасности Российской Федерации.

Президент Российской Федерации руководит в пределах своих конституционных полномочий органами и силами по обеспечению информационной безопасности Российской Федерации; санкционирует действия по обеспечению информационной безопасности Российской Федерации; в соответствии с законодательством Российской Федерации формирует, реорганизует и упраздняет подчиненные ему органы и силы по обеспечению информационной безопасности Российской Федерации; определяет в своих ежегодных посланиях Федеральному Собранию приоритетные направления государственной политики в области обеспечения информационной безопасности Российской Федерации, а также меры по реализации настоящей Доктрины.

Палаты Федерального Собрания Российской Федерации на основе Конституции Российской Федерации по представлению Президента Российской Федерации и Правительства Российской Федерации формируют законодательную базу в области обеспечения информационной безопасности Российской Федерации.

Правительство Российской Федерации в пределах своих полномочий и с учетом сформулированных в ежегодных посланиях Президента Российской Федерации Федеральному Собранию приоритетных направлений в области обеспечения информационной безопасности Российской Федерации координирует деятельность федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации, а также при формировании в установленном порядке проектов федерального бюджета на соответствующие годы предусматривает выделение средств, необходимых для реализации федеральных программ в этой области.

Совет Безопасности Российской Федерации проводит работу по выявлению и оценке угроз информационной безопасности Российской Федерации, оперативно подготавливает проекты решений Президента Российской Федерации по предотвращению таких угроз, разрабатывает предложения в области обеспечения информационной безопасности Российской Федерации, а также предложения по уточнению отдельных положений настоящей Доктрины, координирует

нирует деятельность органов и сил по обеспечению информационной безопасности Российской Федерации, контролирует реализацию федеральными органами исполнительной власти и органами исполнительной власти субъектов Российской Федерации решений Президента Российской Федерации в этой области.

Федеральные органы исполнительной власти обеспечивают исполнение законодательства Российской Федерации, решений Президента Российской Федерации и Правительства Российской Федерации в области обеспечения информационной безопасности Российской Федерации; в пределах своей компетенции разрабатывают нормативные правовые акты в этой области и представляют их в установленном порядке Президенту Российской Федерации и в Правительство Российской Федерации.

Межведомственные и государственные комиссии, создаваемые Президентом Российской Федерации и Правительством Российской Федерации, решают в соответствии с предоставленными им полномочиями задачи обеспечения информационной безопасности Российской Федерации.

Органы исполнительной власти субъектов Российской Федерации взаимодействуют с федеральными органами исполнительной власти по вопросам исполнения законодательства Российской Федерации, решений Президента Российской Федерации и Правительства Российской Федерации в области обеспечения информационной безопасности Российской Федерации, а также по вопросам реализации федеральных программ в этой области; совместно с органами местного самоуправления осуществляют мероприятия по привлечению граждан, организаций и общественных объединений к оказанию содействия в решении проблем обеспечения информационной безопасности Российской Федерации; вносят в федеральные органы исполнительной власти предложения по совершенствованию системы обеспечения информационной безопасности Российской Федерации.

Органы местного самоуправления обеспечивают соблюдение законодательства Российской Федерации в области обеспечения информационной безопасности Российской Федерации.

Органы судебной власти осуществляют правосудие по делам о преступлениях, связанных с посягательствами на законные интересы личности, общества и государства в информационной сфере, и обеспечивают судебную защиту граждан и общественных объединений, чьи права были нарушены в связи с деятельностью по обеспечению информационной безопасности Российской Федерации.

В состав системы обеспечения информационной безопасности Российской Федерации могут входить подсистемы (системы), ориентированные на решение локальных задач в данной сфере.

Реализация первоочередных мероприятий по обеспечению информационной безопасности Российской Федерации, перечисленных в настоящей Доктрине, предполагает разработку соответствующей федеральной программы. Конкретизация некоторых положений настоящей Доктрины применительно к отдельным сферам деятельности общества и государства может быть осуществлена в соответствующих документах, утверждаемых Президентом Российской Федерации.

П-08. Перечень сведений, отнесенных к государственной тайне**УКАЗ ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ****О перечне сведений, отнесенных к государственной тайне**

В связи с совершенствованием структуры федеральных органов исполнительной власти постановляю:

Изложить перечень сведений, отнесенных к государственной тайне, утвержденный Указом Президента Российской Федерации от 30 ноября 1995 г. № 1203 (Собрание законодательства Российской Федерации, 1995, № 49, ст. 4775), в новой редакции (прилагается).

Президент Российской Федерации

Б. ЕЛЬЦИН

Москва, Кремль

24 января 1998 года

№61

1. Общие положения

1. Перечень сведений, отнесенных к государственной тайне, содержит сведения в области военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности государства, распространение которых может нанести ущерб безопасности Российской Федерации, а также наименования федеральных органов исполнительной власти и других организаций (далее именуются -государственные органы), Наделенных полномочиями по распоряжению этими сведениями.

Каждый из указанных в настоящем перечне государственных органов наделяется полномочиями по распоряжению сведениями отраслевой (ведомственной) принадлежности в рамках его компетенции, определенной положением о конкретном государственном органе, а также сведениями других собственников информации соответствующей тематической направленности по их представлению.

Настоящий перечень пересматривается по мере необходимости.

2. В настоящем перечне применяются следующие понятия:

- «специальные объекты» - пункты управления государством и Вооруженными Силами Российской Федерации, а также другие объекты, обеспечивающие функционирование федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации в военное время;

- «военные объекты» - боевые позиции войск, пункты управления, полигоны, узлы связи, базы, склады и другие сооружения военного назначения;

- «режимные объекты» - военные и специальные объекты, воинские части, предприятия, организации, учреждения, для функционирования которых установлены дополнительные меры безопасности;

- «предприятия и организации» - юридические лица независимо от форм собственности, создаваемые в соответствии с законодательством Российской Федерации, а также их филиалы и представительства;

- «войска» - Вооруженные Силы Российской Федерации, другие войска, воинские формирования, органы и создаваемые на военное время специальные формирования, предусмотренные Федеральным законом «Об обороне»;

- «вооружение» - средства, предназначенные для поражения живой силы, техники, сооружений и других объектов противника, составные части этих средств и комплектующие изделия;

- «военная техника» - технические средства, предназначенные для боевого, технического и тылового обеспечения деятельности войск, а также оборудование и аппаратура для контроля и испытаний этих средств, составные части этих средств и комплектующие изделия;

- «объекты оборонной промышленности» - предприятия по разработке, производству и ремонту вооружения, военной техники или снаряжения;

- «оружие массового поражения» - ядерное, химическое, биологическое или иное оружие большой поражающей способности, применение которого вызывает массовые потери и (или) разрушения.

3. В настоящем перечне применяется сокращение: ГУСП - Главное управление специальных программ Президента Российской Федерации.

4. В позициях 59, 60, 68 и 69 настоящего перечня указаны государственные органы, руководители которых наделены полномочиями по отнесению сведений к государственной тайне.

2. Сведения в военной области

1. Сведения, раскрывающие стратегические планы применения войск, оперативные планы, документы боевого управления, документы по приведению войск в различные степени боевой готовности.

МВД России, Минобороны России, МЧС России, ФАПСИ, ФПС России * /Подчеркиванием выделены государственные органы, наделенные полномочиями по распоряжению сведениями, отнесенными к государственной тайне. – Ред./.

2. Сведения о стратегическом и оперативном развертывании войск

МВД России, Минобороны России, МЧС России, ФАПСИ, ФПС России, Администрация Президента Российской Федерации.

3. Сведения о планах строительства, развитии, численности, боевом составе или количестве войск, их боевой готовности, а также о военно-политической и (или) оперативной обстановке

МВД России, Минобороны России, МЧС России, ФАПСИ, ФПС России, Администрация Президента Российской Федерации.

4. Сведения, раскрывающие состояние оперативной (боевой) подготовки войск, обеспеченность их деятельности, состав и (или) состояние систем управления войсками

МВД России, Минобороны России, ФАПСИ, ФПС России, МЧС России.

5. Сведения о мобилизационном развертывании войск, их мобилизационной готовности, о создании и использовании мобилизационных ресурсов, системе управления мобилизационным развертыванием и (или) о возможностях комплектования войск личным составом, обеспечения вооружением, военной техникой и другими материальными, финансовыми средствами, а также воинскими перевозками

МВД России, Минобороны России, МЧС России, ФАПСИ, ФПС России, Администрация Президента Российской Федерации.

6. Сведения, раскрывающие направления, долгосрочные прогнозы или планы развития вооружения и военной техники, содержание или результаты выполнения целевых программ, научно-исследовательских, опытно-конструкторских работ по созданию или модернизации образцов вооружения и военной техники, их тактико-технические характеристики

Минатом России, МВД России Минздрав России, Минобороны России, Минобрнауки России, ФПС России, Минтопэнерго России, Минтранс России, МЧС России, Минэкономики России, Росгидромет, ФПС России, ФСБ России, ФСО России, РККА.

7. Сведения, раскрывающие направления разработки, конструкцию, технологию изготовления, изотопный состав, боевые, физические, химические или ядерные свойства, порядок применения или эксплуатации вооружения и военной техники

Минатом России, МВД России, Минздрав России, Минобороны России, Минобрнауки России, Минтопэнерго России, Минтранс России, МЧС России, Минэкономики России, Росгидромет, ФПС России, ФСБ России, РККА.

8. Сведения, раскрывающие производственные мощности, плановые или фактические данные о выпуске и (или) поставках (в натуральном выражении) средств бактериальной или медицинской защиты

Минздрав России, Минобороны России, Минобрнауки России, Минэкономики России.

9. Сведения о разработке, технологии, производстве, об объемах производства, о хранении и (или) утилизации ядерных боеприпасов и (или) их составных частей, делящихся материалов

ядерных энергетических установок, специальных физических установок оборонного назначения, о технических средствах и (или) методах защиты ядерных боеприпасов от несанкционированного применения

Минатом России, Минобороны России, Минэкономики России.

Сведения, раскрывающие содержание ранее осуществлявшихся работ в области оружия массового поражения, достигнутые при этом результаты, а также сведения о составе образца и (или) рецептуре, технологии производства или снаряжении изделий

Минатом России, Минздрав России, Минобороны России, Минэкономики России, ФСБ России.

10. Сведения о проектировании, сооружении, эксплуатации или обеспечении безопасности объектов ядерного комплекса

Минатом России, МВД России, Минздрав России, Минобороны России, Минэкономики России.

11. Сведения, раскрывающие достижения атомной науки и техники, имеющие важное оборонное и экономическое значение или определяющие качественно новый уровень возможности создания вооружения и военной техники и (или) принципиально новых изделий и технологий

Минатом России, Минобороны России, Минэкономики России.

12. Сведения, раскрывающие свойства, рецептуру или технологию производства ракетных топлив, а также баллистических порохов, взрывчатых веществ или средств взрывания военного назначения, а также новых сплавов, спецжидкостей, новых топлив для вооружения и военной техники

Минобороны России, Минобразования России, Минэкономики России.

13. Сведения, раскрывающие дислокацию, действительные наименования, организационную структуру, вооружение, численность войск, не подлежащие открытому объявлению в соответствии с международными обязательствами Российской Федерации

Минатом России, МВД России, Минобороны России, МПС России, МЧС России, ФАПСИ, ФПС России.

14. Сведения об использовании инфраструктуры Российской Федерации в интересах обеспечения обороноспособности и безопасности государства

МВД России, Минздрав России, Минобороны России, МПС России, Минсельхозпрод России, Минтопэнерго России, Минтранс России, МЧС России, Минэкономики России, ФСБ России, ФПС России, ГУСП, Администрация Президента Российской Федерации.

15. Сведения о дислокации, назначении, степени готовности или защищенности режимных объектов, не подпадающие под обязательства Российской Федерации по международным договорам, о выборе, отводе земельных участков, недр или акваторий для строительства указанных объектов, а также о планируемых или проводимых изыскательских, проектных и иных работах по созданию этих объектов

Минатом России, МВД России, Минобороны России, МПР России, МЧС России, Минэкономики России, ФСБ России, ФСО России, Госкомзем России, Госкомэкологии России.

Те же сведения применительно к специальным объектам органов государственной власти
ГУСП.

16. Сведения об использовании или перспективах развития взаимоувязанной сети связи Российской Федерации в интересах обеспечения обороноспособности и безопасности государства

МВД России, Минобороны России, Госкомсвязи России, ФСБ России, ФАПСИ, ФСО России.

17. Сведения, раскрывающие распределение или использование полос радиочастот радиоэлектронными средствами военного или специального назначения

МВД России, Минобороны России, Госкомсвязи России, ФСБ России, ФАПСИ, ФСО России.

18. Сведения, раскрывающие организацию или функционирование всех видов связи, радиолокационного, радиотехнического обеспечения войск

МВД России, Минобороны России, ФАПСИ, ФПС России.

19. Сведения, раскрывающие содержание, организацию или результаты основных видов деятельности органов пограничной службы ФПС России, построение охраны государственной границы Российской Федерации, исключительной экономической зоны и континентального шельфа Российской Федерации или государств-участников СНГ

ФПС России.

20. Сведения, раскрывающие направления развития средств, технологий двойного назначения, содержание, результаты выполнения целевых программ, научно-исследовательских и (или) опытно-конструкторских работ по созданию или модернизации этих средств, технологий.

Сведения о применении в военных целях средств, технологий двойного назначения

Минатом России, МВД России, Минобороны России, Минобрнауки России, Минэкономики России, Госкомсвязи России, ФАПСИ, ФСБ России, ФСО России, РКА.

21. Сведения о перспективах развития и (или) об использовании космической инфраструктуры Российской Федерации в интересах обеспечения обороноспособности и безопасности государства

Минобороны России, Минэкономики России, ФСБ России, РКА.

22. Сведения, раскрывающие состояние и (или) направления развития гидронавтики в интересах обороны и безопасности государства

Минобороны России, Минэкономики России.

3. Сведения о внешнеполитической и внешнеэкономической деятельности

23. Сведения по вопросам внешней политики, внешней торговли, научно-технических связей, раскрывающие стратегию и тактику внешней политики Российской Федерации, преждевременное распространение которых может нанести ущерб интересам государства

МВЭС России, Минздрав России, МИД России, Миннауки России, Минобороны России, Администрация Президента Российской Федерации.

24. Сведения по политическим, военным, научно-техническим или экономическим вопросам в отношении одного или ряда иностранных государств, полученные в доверительном порядке, если их разглашение может привести к выявлению источника этих сведений

Минатом России, МВЭС России, МИД России, Миннауки России, Минобороны России, МПС России, Минэкономики России, ФПС России.

25. Сведения о переговорах между представителями Российской Федерации и представителями других государств о выработке единой принципиальной позиции в международных отношениях, если, по мнению участников переговоров, разглашение этих сведений может повлечь для одной из сторон дипломатические осложнения

МВЭС России, МИД России, Минобороны России, СВР России.

26. Сведения о подготовке, заключении, ратификации, подготовке денонсации, содержании или выполнении договоров, конвенций или соглашений с иностранными государствами, преждевременное распространение которых может нанести ущерб обороноспособности, безопасности, политическим или экономическим интересам Российской Федерации

Минатом России, МВЭС России, МИД России, Минобороны России, Минэкономики России, СВР России, ФПС России, ФСО России.

27. Сведения о российском экспорте и импорте вооружения и военной техники, их ремонте и эксплуатации, об оказании технического содействия иностранным государствам в создании вооружения, военной техники, военных объектов и объектов оборонной промышленности, а также сведения об оказании Российской Федерацией военно-технической помощи иностранным государствам, если разглашение этих сведений может повлечь для одной из сторон дипломатические осложнения

МВЭС России, Минобороны России, Минэкономики России, ФАПСИ.

Сведения, раскрывающие планы (задания) государственного оборонного заказа в части экспортно-импортных поставок в области военно-технического сотрудничества Российской Федерации с иностранными государствами

МВЭС России, Минобороны России, Минфин России, Минэкономики России, ФАПСИ.

28. Сведения, раскрывающие существо или объем экономического сотрудничества Российской Федерации с иностранными государствами в особый период, а также взаимодействие военно-мобилизационных органов внешнеэкономических организаций государств-участников СНГ по этим вопросам

МВЭС России, Минобороны России, Минэкономики России, МЧС России.

29. Сведения, раскрывающие содержание мероприятий по обеспечению взаимных поставок сырья, материалов, топлива, оборудования, медикаментов между Российской Федерацией и государствами-участниками СНГ на расчетный год или мероприятий по оказанию последним технического содействия в строительстве предприятий и объектов на расчетный год в целом по Российской Федерации

МВЭС России, Минобороны России, МПС России, МЧС России, Минэкономики России.

30. Сведения, раскрывающие объемы перевозок экспортно-импортных грузов между Российской Федерацией и государствами-участниками СНГ на расчетный год в целом по Российской Федерации

МВЭС России, Минобороны России, МЧС России, Минэкономики России.

4. Сведения в области экономики, науки и техники

31. Сведения о показателях, определяющих подготовку экономики Российской Федерации к устойчивому функционированию в военное время

Минатом России, МВД России, МВЭС России, Минобороны России, Минобрнауки России, МПС России, Минтопэнерго России, Минфин России, МЧС России, Минэкономики России, ФСБ России, Администрация Президента Российской Федерации.

32. Сведения, раскрывающие существо новейших достижений в области науки и техники, которые могут быть использованы в создании принципиально новых изделий, технологических процессов в различных отраслях экономики, а также сведения, определяющие качественно новый уровень возможностей вооружения и военной техники, повышения их боевой эффективности, разглашение которых может нанести ущерб интересам государства

МВЭС России, Минздрав России, Миннауки России, Минобороны России, Минобрнауки России, МПС России, Минтопэнерго России, МЧС России, Минэкономики России, Росгидромет, СВР России, ФАПСИ, ФПС России, ФСО России, РКА.

33. Сведения, раскрывающие содержание и (или) направленность научно-исследовательских, опытно-конструкторских или проектных работ, проводимых в интересах обороны и обеспечения безопасности государства

Минатом России, МВЭС России, Миннауки России, Минобороны России, Минобрнауки России, МПР России, Минтранс России, МЧС России, Минэкономики России, СВР России, ФАПСИ, ФПС России, ФСБ России, ФСО России, ГУСП, РКА.

34. Сведения о подготовке или распределении кадров, раскрывающие мероприятия, проводимые в интересах обеспечения безопасности государства

Минобороны России, Минобрнауки России, Минэкономики России, СВР России, ФПС России, ФСБ России, ФСО России, Администрация Президента Российской Федерации.

35. Сведения, раскрывающие результаты работ в области гидрометеорологии или гелиогеофизики, а также результаты специальных геолого-геофизических исследований, проводимых в интересах обеспечения безопасности государства

Минобороны России, МПР России, Росгидромет.

36. Сведения, раскрывающие планы (задания) государственного оборонного заказа, объемы поставок вооружения и военной техники, производственные мощности по их выпуску. Сведения о кооперационных связях предприятий, о разработчиках или изготовителях вооружения и

военной техники, если эти сведения раскрывают данные о производственных мощностях по их выпуску и (или) основные тактико-технические характеристики вооружения и военной техники Минатом России, МВД России, МВЭС России, Минобороны России, Минтопэнерго России, Минтранс России, МЧС России, Минэкономики России, ФАПСИ, ФСБ России, ФСО России, РКА.

37. Сведения, раскрывающие состояние метрологического обеспечения вооружения и военной техники, технические или метрологические характеристики военных эталонов или средств метрологического обеспечения, определяющие качественно новый уровень вооружения и военной техники.

Сведения, раскрывающие основные направления или программы развития стандартизации, а также содержание стандартов в области вооружения и военной техники

Минобороны России, Минэкономики России, Госстандарт России, ФАПСИ.

38. Сведения, раскрывающие прогнозные оценки научно-технического прогресса в Российской Федерации и его социально-экономические последствия по направлениям, определяющим обороноспособность государства

Минобороны России, Минэкономики России.

39. Сведения о производстве металлургической промышленности цветных, редких металлов или других материалов, имеющих стратегическое значение

Минобороны России, Минэкономики России.

40. Сводные сведения о государственных запасах драгоценных металлов (кроме золота), природных алмазов в натуральном или денежном выражении в целом по Российской Федерации, федеральным органам исполнительной власти

Минфин России, Минэкономики России, Банк России.

41. Сведения, раскрывающие прогнозные данные о производстве золота, добыче природных алмазов, а также отчетные данные о добыче природных алмазов за период от одного года и более в натуральном выражении в целом по Российской Федерации, субъектам Российской Федерации, федеральным органам исполнительной власти

Минфин России, Минэкономики России, Банк России.

42. Сведения, раскрывающие прогнозные или фактические объемы производства платины, металлов платиновой группы (палладия, иридия, родия, рутения, осмия), серебра в натуральном выражении в целом по Российской Федерации, субъектам Российской Федерации, федеральным органам исполнительной власти

Минфин России, Минэкономики России, Банк России.

43. Сводные сведения о поступлениях драгоценных металлов и драгоценных камней в Госфонд России, об отпуске их потребителям Российской Федерации за период от одного года и более в натуральном или денежном выражении в целом по Российской Федерации

Минфин России, Минэкономики России, Банк России.

44. Сводные сведения об объемах потребления или отпуска драгоценных металлов и природных алмазов в сопоставлении с объемами их добычи в натуральном или денежном выражении за период от одного года и более в целом по Российской Федерации, федеральным органам исполнительной власти

Минфин России, Минэкономики России.

45. Сведения об объемах потребления отдельно платины, металлов платиновой группы (палладия, иридия, родия, рутения, осмия), серебра в натуральном выражении в сопоставлении с объемами производства указанных металлов за период от одного года и более в целом по Российской Федерации

Минфин России, Минэкономики России.

46. Сведения о балансовых запасах в недрах страны природных алмазов от 25 млн карат и выше, золота от 100 тонн и выше, платины, металлов платиновой группы (палладия, иридия, родия, рутения, осмия) от 50 тонн и выше, серебра от 10 тыс. тонн и выше, о приросте разведанных запасов этих полезных ископаемых в целом по Российской Федерации, субъектам Рос-

сийской Федерации, отдельным крупным месторождениям, если размеры запасов соответствуют указанным размерам

Минфин России, Минэкономики России, Банк России.

47. Сведения о себестоимости серебра, платины, металлов платиновой группы (палладия, иридия, родия, рутения, осмия), природных алмазов в целом по Российской Федерации, субъектам Российской Федерации, а также сведения, применяемые для расчета кондиций, необходимых при подсчете разведанных запасов золота в его месторождениях или месторождениях комплексных руд в размерах, указанных в позиции 46 настоящего перечня

Минфин России, Минэкономики России, Банк России.

48. Сведения, раскрывающие ресурсный потенциал, балансовые запасы в недрах или данные о добыче стратегических видов полезных ископаемых в целом по Российской Федерации, субъектам Российской Федерации

МПР России, Минэкономики России.

49. Сведения о расходах федерального бюджета, связанных с обеспечением безопасности Российской Федерации (кроме обобщенных показателей)

МВЭС России, Минфин России, Минэкономики России.

50. Сведения, раскрывающие затраты на научно-исследовательские, опытно-конструкторские работы по созданию вооружения, военной техники

Минатом России, МВД России, МВЭС России, Минобороны России, МЧС России, Минэкономики России, ФАПСИ, ФПС России, ФСБ России, ФСО России, РКА.

Те же сведения применительно к работам, проводимым в интересах специальных объектов ГУСП.

51. Сведения, раскрывающие ассигнования или фактические затраты на заказы, разработку, производство или ремонт вооружения и военной техники, режимных объектов

Минатом России, МВЭС России/Минобороны России, МЧС России, Минэкономики России, СВР России, ФАПСИ, ФПС России, ФСБ России, ФСО России, РКА.

Те же сведения применительно к специальным объектам

ГУСП.

52. Сведения по неурегулированным расчетам Российской Федерации с иностранными государствами (кроме обобщенных показателей по внешней задолженности)

МВЭС России, МИД России, Минфин России, Банк России.

53. Сведения о финансовой и (или) денежно-кредитной деятельности, преждевременное распространение которых может нанести ущерб безопасности государства

Минфин России.

54. Сведения, раскрывающие расходы денежных средств на содержание войск по отдельным статьям смет федеральных органов исполнительной власти

МВД России, Минобороны России, МЧС России, Минэкономики России, ФАПСИ, ФПС России.

55. Сведения о денежных банкнотах нового образца или проектах монет (кроме юбилейных и памятных) до официального опубликования

Банк России.

56. Сведения о производстве банкнот Банка России в натуральном или денежном выражении, способах, обеспечивающих защиту этих банкнот и других изделий Гознака от подделок, а также о способах определения их подлинности

МВД России, Минфин России.

57. Сведения, раскрывающие объемы выпуска или поставок стратегических видов сельскохозяйственного сырья

Минобороны России, Минсельхозпрод России, Минэкономики России.

58. Сведения, раскрывающие объемы поставок и запасов стратегических видов топлива

Минобороны России, Минтопэнерго России, Минэкономики России.

59. Сведения о мобилизационных мощностях по изготовлению (ремонту) вооружения, военной техники, о создании и (или) развитии (сохранении) этих мощностей

Федеральные органы исполнительной власти, имеющие мобилизационные задания.

60. Сведения о мобилизационных мощностях по производству продукции общего применения, стратегических видов сырья, материалов, о создании и (или) развитии (сохранении) этих мощностей

Федеральные органы исполнительной власти, имеющие мобилизационные задания.

61. Сведения, раскрывающие работы, проводимые в целях создания средств индикации, дегазации, химической или биологической защиты от оружия массового поражения или новых сорбционных и других материалов для них

Минздрав России, Минобороны России, Минобрнауки России, МЧС России, Минэкономики России.

62. Сведения, раскрывающие результаты топографической, геодезической или картографической деятельности, имеющие важное оборонное или экономическое значение

Минобороны России, Минэкономики России, Роскартография, Госкомзем России.

63. Сводные данные о российском экспорте и импорте немонетарного золота, драгоценных металлов и камней или изделий из них

МВЭС России, Минэкономики России.

64. Сведения, раскрывающие состояние, оборудование, подготовку для военных целей транспортной сети, средств транспорта, объемы воинских перевозок и маршруты транспортировки вооружения и военной техники

МВД России, Минобороны России, Минтранс России, Минэкономики России.

65. Сведения, раскрывающие возможности и (или) мобилизационные резервы железных дорог и МГТС России по обеспечению железнодорожных перевозок грузов, организацию и объемы воинских перевозок, объемы перевозок и маршруты транспортировки стратегических видов энергетического, минерального, сельскохозяйственного сырья, топлива, материалов, отдельных видов вооружения или военной техники, организацию и (или) функционирование системы связи или управления, а также специальные меры по обеспечению безопасности железнодорожного движения или сохранности грузов

МВД России, Минобороны России, МПС России, Минэкономики России.

66. Сведения, раскрывающие дислокацию, специализацию, мощности и (или) пропускную способность пунктов погрузки или выгрузки войск, данные об их продовольственном, медико-санитарном обслуживании

Минобороны России, МПС России.

67. Сведения, раскрывающие мобилизационную потребность в транспортных средствах, в том числе по отдельным видам транспорта, и (или) мобилизационную обеспеченность ими

Минздрав России, Минобороны России, МПС России, Минтранс России, МЧС России, Минэкономики России.

68. Сведения, раскрывающие состояние сил или средств гражданской обороны в целом по Российской Федерации

Федеральные органы исполнительной власти, располагающие силами гражданской обороны.

69. Сведения, раскрывающие структурную организацию или показатели мобилизационного плана экономики Российской Федерации, а также состояние мобилизационной подготовки федеральных органов исполнительной власти или отдельных организаций

Федеральные органы исполнительной власти, имеющие мобилизационные задания.

70. Сведения, раскрывающие дислокацию, фактические запасы государственных и (или) мобилизационных резервов, их использование

МВД России, Минздрав России, Минобороны России, МПС России, Минэкономики России, Госкомрезерв России.

71. Сведения, характеризующие состояние страхового фонда документации на вооружение и военную технику, основные виды гражданской продукции, включаемые в мобилизационные планы, на объекты повышенного риска и (или) системы жизнеобеспечения населения, на объек-

ты, являющиеся национальным достоянием, а также сведения о дислокации объектов (баз) хранения страхового фонда документации в целом по Российской Федерации

Минатом России, Минобороны России, МПС России, МЧС России, Минэкономики России.

72. Сведения, раскрывающие планы, содержание или результаты научно-исследовательских работ в области мобилизационной подготовки промышленности Российской Федерации

Минобороны России, МЧС России, Минэкономики России.

73. Сведения, раскрывающие платежный баланс Российской Федерации с зарубежными странами в целом на военный период

МВЭС России, Минобороны России, Минэкономики России, Банк России.

74. Сведения о горных выработках, естественных полостях, метрополитенах или других сооружениях, которые могут быть использованы в интересах обороны страны, а также сведения, раскрывающие схемы водоснабжения городов с населением более 500 тыс. человек, железнодорожных узлов и (или) расположение головных сооружений водопровода и водовода, их питающих

Минобороны России, МПР России, МЧС России, Госстрой России.

75. Сведения о физико-химических явлениях (полях), сопутствующих созданию, производству и (или) эксплуатации вооружения, военной техники, раскрывающие их охраняемые параметры

Минатом России, МВД России, Минздрав России, Минобороны России, Минобрнауки России, Минтопэнерго России, Минтранс России, МЧС России, Минэкономики России, Росгидромет, ФАПСИ, ФПС России, ФСБ России, РКА, Гостехкомиссия России.

5. Сведения в области разведывательной, контрразведывательной, оперативно-розыскной деятельности и организации защиты государственной тайны

76. Сведения в области разведывательной, контрразведывательной деятельности и защиты информации, раскрывающие организацию или фактическое состояние защиты государственной тайны

Органы государственной власти, организующие обеспечение защиты государственной тайны.

77. Сведения, раскрывающие методы и средства защиты информации, содержащей сведения, составляющие государственную тайну, планируемые и (или) проводимые мероприятия по защите информации от несанкционированного доступа, иностранных технических разведок и утечки по техническим каналам

Минобороны России, ФАПСИ, ФСБ России, ФСО России, Гостехкомиссия России, СВР России.

78. Сведения о системе президентской, правительственной, шифровальной связи, в том числе кодированной и засекреченной, о шифрах, их разработке, изготовлении и обеспечении ими, о методах и средствах анализа шифровальных средств и средств специальной защиты, об информационно-аналитических системах специального назначения

Минобороны России, ФАПСИ, ФСО России, ФСБ России, Администрация Президента Российской Федерации.

79. Сведения, раскрывающие организацию, силы, средства или методы обеспечения безопасности объектов государственной охраны, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения

ФСО России, Администрация Президента Российской Федерации.

80. Сведения, раскрывающие силы, средства, методы, планы, состояние или результаты разведывательной, контрразведывательной или оперативно-розыскной деятельности, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения.

Сведения о лицах, сотрудничающих или сотрудничавших на конфиденциальной основе с органами, осуществляющими контрразведывательную или оперативно-розыскную деятельность, о сотрудниках ФСБ России, выполняющих (выполнявших) специальные задания в специальных службах и организациях иностранных государств, в преступных группах.

Сведения, раскрывающие принадлежность конкретных лиц к кадровому составу органов контрразведки Российской Федерации.

Сведения, раскрывающие состояние, результаты, а также мероприятия оперативно-мобилизационной работы

Минобороны России, ФСБ России, ФСО России, МВД России, ФПС России, ФАПСИ, ФСНП России.

81. Сведения, раскрывающие силы, средства, источники, методы, планы, состояние, организацию, результаты разведывательной или оперативно-розыскной деятельности.

Сведения, раскрывающие принадлежность конкретных лиц к кадровому составу органов внешней разведки Российской Федерации.

Сведения о лицах, оказывающих (оказавших) конфиденциальное содействие органам внешней разведки Российской Федерации.

Сведения, раскрывающие состояние и результаты оперативно-мобилизационной работы, проводимой в области внешней разведки

Минобороны России, СВР России, ФСБ России, МВД России, ФПС России, ФАПСИ, ФСНП России.

81. Сведения, раскрывающие силы, средства, методы, планы и результаты оперативно-розыскной деятельности, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения.

Сведения о лицах, сотрудничающих или сотрудничавших на конфиденциальной основе с органами, осуществляющими оперативно-розыскную деятельность

МВД России, ФСНП России, ГТК России.

82. Сведения, раскрывающие принадлежность конкретных лиц к подразделениям по борьбе с организованной преступностью, а также проводимые ими оперативно-поисковые и оперативно-технические мероприятия

МВД России, ФСБ России.

83. Сведения, раскрывающие принадлежность конкретных лиц к кадровому составу оперативных подразделений таможенных органов

ГТК России.

84. Сведения, раскрывающие силы, средства и методы ведения следствия по уголовным делам о государственных преступлениях

МВД России, ФСБ России.

85. Сведения, раскрывающие силы, средства, методы, планы, состояние и результаты деятельности органов радиоэлектронной разведки средств связи, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения

Минобороны России, ФАПСИ, ФСБ России.

86. Сведения, раскрывающие силы, средства, методы, планы или результаты разведывательной, контрразведывательной, оперативно-розыскной деятельности органов пограничной службы ФПС России, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения.

Сведения о лицах, сотрудничающих или сотрудничавших на конфиденциальной основе с органами пограничной службы ФПС России, осуществляющими разведывательную, контрразведывательную или оперативно-розыскную деятельность

ФПС России.

П-09. Об утверждении перечня сведений конфиденциального характера**УКАЗ ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ****Об утверждении перечня сведений конфиденциального характера**

В целях дальнейшего совершенствования порядка опубликования и вступления в силу актов Президента Российской Федерации, Правительства Российской Федерации и нормативных правовых актов федеральных органов исполнительной власти постановляю:

Утвердить прилагаемый перечень сведений конфиденциального характера.

Президент Российской Федерации

Б. ЕЛЫЦИН

Москва, Кремль

6 марта 1997 г.

№ 188

УТВЕРЖДЕН

Указом Президента

от 6 марта 1997 г. № 188

ПЕРЕЧЕНЬ**сведений конфиденциального характера**

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 др.).
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.

П-10. Положение о лицензировании деятельности по технической ЗИ**ПОЛОЖЕНИЕ О ЛИЦЕНЗИРОВАНИИ
ДЕЯТЕЛЬНОСТИ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ
КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ**

Постановление Правительства Российской Федерации от 30 апреля 2002 г. № 290 г. Москва

О ЛИЦЕНЗИРОВАНИИ ДЕЯТЕЛЬНОСТИ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

В соответствии с Федеральным законом «О лицензировании отдельных видов деятельности» Правительство Российской Федерации постановляет:

Утвердить прилагаемое Положение о лицензировании деятельности по технической защите конфиденциальной информации.

Председатель Правительства
Российской Федерации
М. Касьянов

1. Настоящее Положение определяет порядок лицензирования деятельности юридических лиц и индивидуальных предпринимателей по технической защите конфиденциальной информации.

2. Конфиденциальной является информация, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничен в соответствии с законодательством Российской Федерации. Под технической защитой конфиденциальной информации понимается комплекс мероприятий и (или) услуг по защите ее от несанкционированного доступа, в том числе и по техническим каналам, а также от специальных воздействий на нее в целях уничтожения, искажения или блокирования доступа.

3. Лицензирование деятельности по технической защите конфиденциальной информации осуществляет Государственная техническая комиссия при Президенте Российской Федерации (далее именуется лицензирующий орган).

4. Лицензионными требованиями и условиями при осуществлении деятельности по технической защите конфиденциальной информации являются:

а) осуществление лицензируемой деятельности специалистами, имеющими высшее профессиональное образование по специальности «компьютерная безопасность», «комплексное обеспечение информационной безопасности автоматизированных систем» или «информационная безопасность телекоммуникационных систем», либо специалистами, прошедшими переподготовку по вопросам защиты информации;

б) соответствие производственных помещений, производственного, испытательного и контрольно-измерительного оборудования техническим нормам и требованиям, установленным государственными стандартами Российской Федерации, руководящими и нормативно-методическими документами, утвержденными приказами Государственной технической комиссии при Президенте Российской Федерации, которые зарегистрированы в Министерстве юстиции Российской Федерации;

в) использование сертифицированных (аттестованных по требованиям безопасности информации) автоматизированных систем, обрабатывающих конфиденциальную информацию, а также средств защиты такой информации;

г) использование третьими лицами программ для электронно-вычислительных машин или баз данных на основании договора с их правообладателем.

5. Для получения лицензии соискатель лицензии представляет в лицензирующий орган следующие документы:

а) заявление о выдаче лицензии с указанием:

■ лицензируемой деятельности;

■ наименования, организационно-правовой формы и места нахождения - для юридического лица;

■ фамилии, имени, отчества, места жительства, данных документа, удостоверяющего личность, - для индивидуального предпринимателя;

б) копии учредительных документов и свидетельства о государственной регистрации соискателя лицензии - юридического лица;

в) копия свидетельства о государственной регистрации соискателя лицензии - индивидуального предпринимателя;

г) копия свидетельства о постановке соискателя лицензии на учет в налоговом органе с указанием идентификационного номера налогоплательщика;

д) документ, подтверждающий уплату лицензионного сбора за рассмотрение заявления о выдаче лицензии;

е) сведения о квалификации специалистов по защите информации соискателя лицензии.

Если копии документов не заверены нотариально, вместе с копиями предъявляются оригиналы.

6. При предоставлении лицензии лицензирующий орган имеет право провести проверку соответствия соискателя лицензии указанным в пункте 4 настоящего Положения лицензионным требованиям и условиям, а также запросить у соискателя лицензии сведения, подтверждающие возможность соблюдения таких требований и условий.

7. Лицензирующий орган в срок, не превышающий шестидесяти дней с даты получения документов, предусмотренных пунктом 5 настоящего Положения, принимает решение о выдаче или об отказе в выдаче лицензии и направляет (вручает) соискателю лицензии уведомление о выдаче лицензии либо об отказе в выдаче лицензии с указанием причин отказа.

8. Срок действия лицензии составляет пять лет и может быть продлен по заявлению лицензиата в порядке, предусмотренном для переоформления лицензии.

Переоформление лицензии осуществляется в течение десяти дней со дня получения лицензирующим органом соответствующего заявления.

9. Лицензирующий орган ведет реестр лицензий, в котором указываются:

а) наименование лицензирующего органа;

б) наименование, организационно-правовая форма, место нахождения юридического лица, фамилия, имя, отчество, место жительства индивидуального предпринимателя, а также данные документа, удостоверяющего его личность;

в) идентификационный номер налогоплательщика;

г) код лицензиата по Общероссийскому классификатору предприятий и организаций;

д) лицензируемая деятельность;

е) срок действия лицензии;

ж) дата принятия решения о выдаче лицензии;

з) номер лицензии и дата ее выдачи;

и) сведения о регистрации лицензии в реестре; к) основания и даты приостановления и возобновления действия лицензии;

л) основания и сроки продления лицензии; м) основание и дата аннулирования лицензии.

10. Контроль за выполнением лицензиатом лицензионных требований и условий осуществляется лицензирующим органом.

Плановая проверка выполнения лицензиатом лицензионных требований и условий проводится не чаще одного раза в год.

Деятельность лицензиата, при проведении плановой проверки которой выявлены нарушения лицензионных требований и условий, подлежит внеплановой проверке, предметом которой является контроль исполнения предписаний об устранении выявленных нарушений.

Внеплановая проверка выполнения лицензиатом лицензионных требований и условий проводится лицензирующим органом также в случае:

получения информации от юридических лиц, индивидуальных предпринимателей, органов государственной власти о нарушении лицензиатом лицензионных требований и условий;

обращения граждан, юридических лиц и индивидуальных предпринимателей с жалобами на нарушения их прав и законных интересов в связи с невыполнением лицензиатом лицензионных требований и условий, его бездействием, а также получения иной информации, подтверждаемой, документами и другими доказательствами, свидетельствующими о наличии признаков таких нарушений.

Продолжительность проверки выполнения лицензиатом лицензионных требований и условий не должна превышать одного месяца.

По результатам проверки оформляется соответствующий акт.

В акте указываются конкретные нарушения лицензионных требований и условий и устанавливается срок их устранения.

Лицензиат в обязательном порядке знакомится с актом.

11. Принятие решения о выдаче лицензии, переоформление, приостановление действия и аннулирование лицензии, а также взимание лицензионных сборов осуществляются в порядке, установленном Федеральным законом «О лицензировании отдельных видов деятельности» и настоящим Положением.

П-11. Инструкция по ЗИ при работе с зарубежными партнерами**ИНСТРУКЦИЯ****по защите конфиденциальной информации при работе с зарубежными партнерами****1. Общие положения**

Настоящая Инструкция определяет порядок работы с зарубежными партнерами. Положениями настоящей Инструкции необходимо руководствоваться также и при контактах с представителями совместных предприятий и с представителями конкурирующих фирм и организаций.

При работе с зарубежными партнерами также следует руководствоваться положениями «Инструкции по защите коммерческой тайны».

Инструкция устанавливает режим работы с иностранцами с целью защиты конфиденциальной информации.

Под работой с иностранцами следует понимать совокупность всех видов деятельности при контактах с иностранными компаниями, фирмами (переписка, телефонные разговоры, передача телексных и факсимильных сообщений) либо личных встреч с их представителями по служебным делам.

1.5. Ответственность за организацию работы с зарубежными партнерами и соблюдение требований настоящей Инструкции несут руководство, служба безопасности и руководители соответствующих структурных подразделений фирмы.

1.6. Для работы с зарубежными партнерами ежегодно составляются списки сотрудников, выделенных для этой работы.

2. Основания для работы с зарубежными партнерами

2.1. Основанием для работы с зарубежными партнерами по служебной необходимости являются: планы международных научно-технических связей, заключенные контракты и протоколы, соглашения об установлении прямых производственных, научно-технических связей, решения о совместной деятельности, а также инициатива самих зарубежных представителей и представителей российской стороны.

Решение о приеме иностранцев принимается генеральным директором или его заместителями по представлению руководителей структурных подразделений, согласованных с отделом по международным связям, службой безопасности, техническим отделом и отделом документационного обеспечения.

Основанием для командирования сотрудников за рубеж служит решение генерального директора или его заместителей, выносимое на основании представляемых руководителями соответствующих отделов материалов, оформленных в установленном порядке. Принятое решение излагается письменно непосредственно на докладной записке, представляемой в установленные сроки.

В докладной записке отражаются следующие сведения: цель выезда; страна командирования и принимающая организация (фирма); срок командирования; условия финансирования поездки; фамилия, имя, отчество и занимаемая должность командируемых.

3. Формы работы с зарубежными партнерами**3.1. Прием зарубежных делегаций.**

3.1.1. Прием приглашенных зарубежных делегаций осуществляется на основе утвержденных программ, составляемых по установленной форме, а также сметы расходов по приему.

Программы пребывания приглашенных зарубежных делегаций и сметы расходов составляются соответствующими подразделениями, отвечающими за прием, согласовываются с отделом международных связей, службой безопасности и утверждаются генеральным директором.

Ответственным за выполнение программы пребывания иностранной делегации является руководитель соответствующего отдела.

3.2. Организация деловых встреч (переговоров).

3.2.1. Деловые встречи с зарубежными партнерами организуются на основе заявок, оформленных соответствующими отделами, отвечающими за прием по установленной форме.

3.2.2. Заявки согласовываются с руководителем отдела международных связей, службой безопасности, отделом технического обеспечения и утверждаются генеральным директором или его заместителями.

3.2.3. Переводчиков на деловые встречи приглашает отдел, принимающий зарубежных представителей.

3.2.4. Для участия в деловых встречах с зарубежными партнерами, как правило, привлекаются специалисты из числа сотрудников, выделенных для работы с зарубежными представителями, в количестве не менее двух человек.

3.2.5. Деловые встречи могут проводиться в кабинете генерального директора, кабинете его первого заместителя и специально выделенном для этого помещении.

3.2.6. Встречу, сопровождение и проводы зарубежных партнеров осуществляют сотрудники соответствующих отделов и отдела по международным связям.

3.2.7. Лица, участвующие в переговорах, обязаны:

- хранить конфиденциальную информацию фирмы;
- не входить в обсуждение вопросов, не относящихся к их компетенции.

3.3. Посещение приемов, симпозиумов, семинаров, выставок и других мероприятий, организуемых зарубежными партнерами или с их участием

3.3.1. Сотрудники фирмы посещают приемы, симпозиумы и семинары, организуемые зарубежными партнерами или с участием зарубежных партнеров, по служебным вопросам по согласованию с отделом международных связей, отделом технического обеспечения и с разрешения генерального директора.

3.3.2. При поступлении письменных или устных приглашений на подобные мероприятия непосредственно в адрес сотрудников следует руководствоваться п. 3.3.1. настоящей Инструкции.

3.4. Передача материалов зарубежным представителям

Передача зарубежным партнерам научно-технических и других материалов допускается после их предварительного рассмотрения руководством и службой безопасности с целью определения возможности их передачи.

3.5. Ведение служебной переписки. Прием и передача телексных и факсимильных сообщений, ведение телефонных разговоров с зарубежными партнерами

3.5.1. Общие положения

3.5.1.1. Руководство фирмы, отделы и подразделения фирмы ведут служебную переписку, прием и передачу телексных и факсимильных сообщений через отдел документационного обеспечения.

Вся входящая международная корреспонденция (вне зависимости от ее вида) регистрируется и первично рассматривается в отделе документационного обеспечения. Корреспонденция докладывается генеральному директору или его заместителям или направляется на рассмотрение и исполнение непосредственно в отделы.

После рассмотрения руководством корреспонденция в соответствии с резолюцией направляется исполнителям, и контроль за сроками исполнения поручения осуществляется в соответствии с установленным порядком.

Право подписи корреспонденции в адрес зарубежных представительств имеют генеральный директор, его заместители и начальники отделов.

Любая корреспонденция в адрес зарубежных представительств подлежит визированию у руководства и в службе безопасности фирмы. Один экземпляр документов остается в отделе документационного обеспечения.

3.5.2. Работа с письмами

Служебные письма, адресуемые зарубежным партнерам, пишутся на фирменных бланках с указанием наименования фирмы на английском языке, а также с разрешенными номерами те-

лефонов, факсов и телексов, выделенных для работы с зарубежными представителями. Ставить какие-либо штампы и печати на таких письмах не разрешается.

Проекты писем в адрес зарубежных партнеров готовятся в отделах фирмы при строгом соблюдении конфиденциальности. Наименование отдела, фамилия и номер телефона исполнителя письма на подлиннике не указываются, а приводятся на копиях.

3.5.3. Работа с телексными сообщениями

Телексные сообщения от иностранцев принимаются на специально выделенный аппарат сети Телекс.

Подготовка проектов телексных сообщений осуществляется отделами по установленной форме на иностранном языке.

3.5.3.3. Отправка телексных сообщений зарубежным партнерам осуществляется в порядке, установленном настоящей Инструкцией.

3.5.4. Работа с факсимильными сообщениями

Все факсимильные сообщения от иностранцев подлежат регистрации в отделе документационного обеспечения.

Подготовка проектов факсимильных сообщений осуществляется отделами на бланках, используемых для письменной корреспонденции и со специальным титульным листом. Тексты сообщений могут быть как на русском, так и на иностранных языках. Требования к реквизитам исполнителя аналогичны требованиям п. 3.5.2.2. настоящей Инструкции.

3.5.4.3. Передача факсимильных сообщений иностранцам осуществляется отделами со специально выделенного аппарата факсимильной связи с предварительной регистрацией в отделе документационного обеспечения.

3.5.5. Ведение телефонных разговоров Сотрудники фирмы могут вести телефонные разговоры с зарубежными партнерами с телефонов, выделяемых для этих целей в каждом отделе: список телефонов подлежит согласованию с отделом международных связей и службой безопасности.

3.6. Командирование за рубеж

3.6.1. Состав делегаций, командируемых за рубеж за счет собственных средств, формируется соответствующими отделами и согласовывается с отделом международных связей, службой безопасности и руководством фирмы.

3.6.2. При командировании за рубеж по служебной линии делегациям и отдельным специалистам выдается техническое задание, в котором отражается перечень конкретных вопросов, для решения которых организуется поездка.

Технические задания составляются отделом международных связей и представляются на утверждение руководству не позднее чем за две недели до выезда.

3.6.3. Оформление выездных документов производится в отделе международных связей в установленном порядке.

4. Оформление результатов работы с иностранцами, учет и отчетность

4.1. Соответствующие отделы, принимающие иностранцев, по итогам работы с зарубежными партнерами и командирования за рубеж составляют отчеты произвольной формы. По итогам деловых встреч составляются записи бесед по установленной форме. Записи бесед представляются в отдел по международным связям в двухдневный срок после окончания работы с иностранцами, а отчеты, как правило, - в двухнедельный срок (два печатных экземпляра).

4.2. В записях бесед и отчетах указывается: когда, где, с кем состоялась встреча; ее основание и цель; кем дано разрешение на встречу, какое учреждение, организацию или фирму представляли иностранцы, их фамилии и должностное положение; кто присутствовал со стороны фирмы; содержание беседы (существо вопросов и ответы на них); какая документация и какие образцы изделий и материалов переданы зарубежным представителям или получены от них, обязательства сторон по существу обсуждавшихся вопросов, а также другая заслуживающая внимания информация.

4.3. Отдел международных связей ведет учет принимаемых иностранных делегаций и деловых встреч, а также учет сообщений от фирмы о контактах с иностранцами.

5. Организационные мероприятия по результатам работы с иностранцами

5.1. Отчеты по результатам работы с зарубежными представительствами и записи бесед, содержание обязательства и предложения сторон докладываются соответствующими отделами, организовавшими встречу, руководству фирмы и службе безопасности.

5.2. Координация работ по выполнению поручений руководства по данным документам возлагается на отдел международных связей и службу безопасности.

5.3. Контроль за выполнением положений настоящей Инструкции возлагается на руководство фирмы, отдел международных связей и службу безопасности.

П-12. Обеспечение сохранности коммерческой тайны предприятия**ОБЕСПЕЧЕНИЕ СОХРАНЕНИЯ КОММЕРЧЕСКОЙ ТАЙНЫ ПРЕДПРИЯТИЯ****Введение**

Важными источниками конфиденциальной информации являются люди, документы и публикации. От того, как организована работа с людьми и документами, зависит и безопасность предприятия. Целям предотвращения нанесения экономического, финансового и материального ущерба предприятию (организации), вызванного неправомерными или неосторожными действиями, а также неквалифицированным обращением или разглашением коммерческой тайны, служат настоящие предложения.

Предложения по обеспечению коммерческой тайны носят общий рекомендательный характер, не являются нормативным документом, ориентированы в основном на работу с документами, содержащими сведения коммерческого характера, и предусматривают главным образом организационные меры защиты коммерческих секретов.

При подготовке данного пособия были использованы материалы и опыт государственных и коммерческих структур по защите информации.

1. Общие положения

1.1. Под коммерческой тайной понимаются не являющиеся государственными секретами сведения, связанные с производственно-технической, научно-исследовательской, опытно-конструкторской и другой деятельностью предприятия, а также с их технологической информацией, управлением, финансами, разглашение, утечка или неправомерное овладение которыми может нанести ущерб его интересам.

1.2. К сведениям, составляющим коммерческую тайну, относятся несекретные сведения, предусмотренные «Перечнем конкретных сведений, составляющих коммерческую тайну», утвержденным и введенным в действие приказом директора предприятия.

Коммерческая тайна является собственностью предприятия. Если коммерческая тайна является результатом совместной деятельности с другими предприятиями, основанной на договорных началах, то коммерческая тайна может быть собственностью двух сторон. Это обстоятельство должно найти отражение в договоре.

Примечание. Единой установки на обозначение грифа ограничения доступа к документу, содержащему коммерческую тайну, нет, таким грифом может быть «коммерческая тайна». На других предприятиях могут быть:

- «коммерческая тайна»,
- «секрет предприятия»,
- «тайна предприятия» и др.

Такой ограничительный" гриф не является грифом секретности, а лишь показывает, что право собственности на данную информацию охраняется законодательством.

1.3. Под разглашением коммерческой тайны имеются в виду противоправные, умышленные или неосторожные действия должностных или иных лиц, приведшие к преждевременному, не вызванному служебной необходимостью, оглашению охраняемых сведений, подпадающих под эту категорию, а также передача таких сведений по открытым техническим каналам или обработка их на не категорированных ЭВМ.

1.4. Под открытым опубликованием вышеуказанных сведений имеется в виду публикация материалов в открытой печати, передача по радио и телевидению, оглашение на международных, зарубежных и открытых внутренних съездах, конференциях, совещаниях, симпозиумах, при публичной защите диссертаций и других публичных выступлениях, свободная рассылка, вывоз материалов за границу или передача их в любой форме иностранным фирмам, организациям или отдельным лицам вне сферы прямых служебных обязанностей.

1.5. Необходимость и возможность открытого опубликования этих сведений, а также их объемы, формы и время опубликования определяются директором или его заместителями по направлениям по заключению постоянно действующей экспертной комиссии.

1.6. Меры по ограничению открытых публикаций коммерческой информации не могут быть использованы во вред принципу гласности и для сокрытия от общественности фактов бесхозяйственности, расточительства, недобросовестной конкуренции и других негативных явлений.

Использование для открытого опубликования сведений, полученных на договорной или доверительной основе или являющихся результатом совместной производственной деятельности, допускается лишь с общего согласия партнеров.

1.7. Передача информации сторонним организациям, не связанным прямыми служебными контактами, должна регулироваться, как правило, договорными отношениями, предусматривающими обязательства и ответственность пользователей, включая возмещение материальных затрат на предоставление информации и компенсацию за нарушение договорных обязательств.

1.8. Предоставление коммерческой информации представителям служебных, ревизионных, фискальных и следственных органов, народным депутатам, органам печати, радио регулируется соответствующими положениями.

1.9. Тиражированные документы и издания с грифом «коммерческая тайна» рассматриваются как материалы, содержащие сведения ограниченного распространения.

1.10. Ответственность за обеспечение режима при работе с материалами с грифом «КТ», своевременную разработку и осуществление необходимых мероприятий по сохранению коммерческой тайны возлагается на директора, его заместителей по направлениям и руководителей структурных подразделений. Ответственность за организацию и осуществление работы по защите коммерческой тайны и проведение постоянного контроля за ее соблюдением возлагается на службу безопасности.

Служба безопасности принимает меры по сохранению коммерческой тайны путем максимального ограничения круга лиц, физической сохранности документов, содержащих такие сведения, обработки информации с грифом «КТ» на защищенных ЭВМ, внесения требований по конфиденциальности конкретной информации в договоры с внутренними и внешнеторговыми партнерами и других мер по решению руководства.

1.11. Защита коммерческой тайны предусматривает:

- порядок определения информации, содержащей коммерческую тайну, и сроков ее действия;
- систему допуска сотрудников, командированных и частных лиц к сведениям, составляющим коммерческую тайну;
- порядок работы с документами с грифом «КТ»;
- обеспечение сохранности документов, дел и изданий с грифом «КТ»;
- обязанности лиц, допущенных к сведениям, составляющим коммерческую тайну;
- принципы организации и проведения контроля за обеспечением режима при работе со сведениями, составляющими коммерческую тайну;
- ответственность за разглашение сведений, утрату документов, содержащих коммерческую тайну.

Контроль за осуществлением учета, размножением, хранением и использованием документов, дел и изданий с грифом «КТ» возлагается на уполномоченных службы безопасности.

Контроль за неразглашением сведений, содержащихся в документах, делах и изданиях с грифом «КТ», осуществляется отделами службы безопасности.

2. Порядок определения информации, содержащей коммерческую тайну, и сроков ее действия

2.1. Определение необходимости проставления грифа «коммерческая тайна» производится на основании Перечня, указанного в п. 1.2: на документе - исполнителем и лицом, подписывающим документ, а на издании - автором (составителем) и руководителем, утверждающим издание к печати.

2.2. Срок действия коммерческой тайны, содержащейся в документе, определяется в каждом конкретном случае исполнителем или лицом, подписавшим документ, в виде конкретной даты, или «до заключения контракта», или «бессрочно».

2.3. На документах, делах и изданиях, содержащих сведения, составляющие коммерческую тайну, проставляется гриф «коммерческая тайна», а на документах и изданиях, кроме того, - номера экземпляров.

Гриф «коммерческая тайна» и номер экземпляра проставляются в правом верхнем углу первой страницы документа, на обложке, титульном листе издания и на первой странице сопроводительного письма к этим материалам.

На обратной стороне последнего листа каждого экземпляра документа, содержащего коммерческую тайну, печатается разметка, в которой указывается: количество отпечатанных экземпляров, номер, фамилия исполнителя и его телефон, дата, срок действия коммерческой тайны, содержащейся в документе (конкретная дата, «до заключения контракта» или «бессрочно»), фамилия машинистки.

2.4. Решение вопроса о снятии грифа «коммерческая тайна» возлагается на создаваемую в установленном порядке специальную комиссию, в состав которой включаются представители службы безопасности и соответствующих структурных подразделений.

Решение комиссии оформляется составляемым в произвольной форме актом, который утверждается директором или его заместителем по направлению. В акте перечисляются дела, с которых гриф «КТ» снимается. Один экземпляр акта вместе с делами передается в архив, а на дела постоянного хранения - в государственный архив.

2.5. На обложках дел гриф «КТ» погашается штампом или записью от руки с указанием даты и номера акта, послужившего основанием для его снятия.

Аналогичные отметки вносятся в описи и номенклатуры дела.

3. Система допуска сотрудников, командированных и частных лиц к сведениям, составляющим коммерческую тайну

2.1. Допуск сотрудников к сведениям, составляющим коммерческую тайну, осуществляется директором, его заместителями по направлениям и руководителями структурных подразделений.

Руководители подразделений и службы безопасности ответственны за подбор лиц, допускаемых к сведениям с грифом «КТ», обязаны обеспечить систематический контроль за тем, чтобы к этим сведениям получали доступ только те лица, которым такие сведения необходимы для выполнения своих служебных обязанностей.

2.2. К сведениям, составляющим коммерческую тайну, допускаются лица, обладающие необходимыми высоконравственными и деловыми качествами, способные хранить коммерческую тайну, и только после оформления в службе безопасности индивидуального письменного обязательства по сохранению коммерческой тайны.

2.3. Допуск сотрудников к работе с делами с грифом «КТ», имеющих к ним непосредственное отношение, производится в соответствии с оформленным на внутренней стороне обложки списком за подписью руководителя структурного подразделения, а к документам - согласно указаниям, содержащимся в резолюциях руководителей подразделений.

2.4. Командированные и частные лица допускаются к ознакомлению и работе с документами и изданиями с грифом «КТ» с письменного разрешения руководителей предприятия и подразделений, в ведении которых находятся эти материалы, при наличии письменного запроса тех организаций, в которых они работают, с указанием темы и объема выполняемого задания, а также предписания на выполнение задания.

Выписки из документов и изданий, содержащих сведения с грифом «КТ», производятся в тетрадях, имеющих такой же гриф, и после окончания работы представителя высылаются в адрес организации.

3.5. Дела и издания с грифом «КТ» выдаются исполнителям и принимаются от них под расписку в «Карточке учета выдаваемых дел и изданий» (форма 4).

4. Порядок работы с документами с грифом «КТ»

4.1. Документы, содержащие сведения, составляющие коммерческую тайну, подлежат обязательной регистрации "в канцелярии службы безопасности или в общем делопроизводстве

подразделения уполномоченным службы безопасности. Они должны иметь реквизиты, предусмотренные п. 2.3, и гриф «КТ» (или полностью «коммерческая тайна»). На документах, передаваемых иностранцам, гриф «КТ» не проставляется. Полученные от иностранцев документы маркируются грифом «КТ» графитным карандашом.

В тексте документа и его реквизитах дополнительно могут оговариваться права на информацию, порядок пользования ею, сроки ограничения на публикацию и др.

Отсутствие грифа «КТ» и предупредительных оговорок в тексте и реквизитах означает свободную рассылку и предполагает, что автор информации и должностное лицо, санкционирующее (подписавшее, утверждавшее документ) ее распространение, предусмотрели все возможные последствия от свободной рассылки и несут за это всю полноту ответственности.

4.2. Вся поступающая корреспонденция с грифом «КТ» или другими грифами, указанными в п. 1.2, принимается и вскрывается сотрудниками канцелярии, которым поручена работа с этими материалами. При этом проверяется количество листов и экземпляров документов и изданий, а также наличие указанных в сопроводительном письме приложений.

В случае отсутствия в конвертах (пакетах) документов «КТ» или приложений к ним составляется акт в двух экземплярах, один из которых отправляется адресанту.

4.3. Регистрации подлежат все входящие, исходящие и внутренние документы, а также издания с грифом «КТ». Такие документы учитываются по количеству листов, а издания (книги, журналы, брошюры) по экземплярно.

4.4. Учет документов и изданий с грифом «КТ» ведется в журналах (форма 1) или на карточках (форма 2) отдельно от учета другой несекретной документации. Листы журналов нумеруются, прошиваются и опечатываются. Издания, которые не подшиваются в дела, учитываются в журнале инвентарного учета (форма 5).

Движение документов и изданий с грифом «КТ» должно своевременно, отражаться в журналах или на карточках.

4.5. На каждом зарегистрированном документе, а также на сопроводительном листе к изданиям с грифом «КТ» проставляется штамп, в котором указываются наименование, регистрационный номер документа и дата его поступления.

4.6. Тираж издания с грифом «КТ», полученный для рассылки, регистрируется под одним входящим номером в журнале учета и распределения изданий (форма 3).

Дополнительно размноженные экземпляры документа (издания) учитываются за номером этого документа (издания), о чем делается отметка на размножаемом документе (издании) и в учетных формах. Нумерация дополнительно размноженных экземпляров производится от последнего номера ранее учтенных экземпляров.

4.7. Печатающие материалы с грифом «КТ» производится в бюро оформления технической документации или в структурных подразделениях под ответственность их руководителей.

4.8. Отпечатанные и подписанные документы с грифом «КТ» вместе с их черновиками и вариантами передаются для регистрации сотруднику канцелярии, осуществляющему их учет. Черновики и варианты уничтожаются этим сотрудником с подтверждением факта уничтожения записью на копии исходящего документа: «Черновик (и варианты) уничтожены». Дата. Подпись.

4.9. Размножение документов и изданий с грифом «КТ» в типографиях и на множительных аппаратах производится с разрешения службы безопасности и под контролем канцелярии по заказам, подписанным руководителем подразделения и утвержденным заместителем директора по направлению. Учет размноженных документов и изданий осуществляется по экземплярно в специальном журнале.

4.10. Рассылка документов и изданий с грифом «КТ» осуществляется на основании подписанных руководителем структурного подразделения разнарядок с указанием учетных номеров отправляемых экземпляров.

Документы с грифом «КТ» после исполнения группируются в отдельные дела. Порядок их группировки предусматривается номенклатурами дел несекретного делопроизводства. В но-

менклатуру дел в обязательном порядке включаются все справочные картотеки и журналы и издания с грифом «КТ».

При пользовании открытой радиосвязью запрещается передавать сведения, имеющие гриф «КТ». Такие сведения могут передаваться только по закрытым техническим средствам связи или по открытой телетайпной связи с проставлением на документах и телеграммах соответствующего штампа.

При пользовании проводной связью запрещается указывать должности адресатов отправителей, разрешается указывать только телеграфные адреса и фамилии отправителей и получателей.

4.13. Снятие копий (рукописных, машинописных, микро- и фотокопий, электрографических и др.), а также производство выписок из документов и изданий с грифом «КТ» сотрудниками производится по разрешению руководителей подразделений.

Снятие копий для сторонних организаций с документов и изданий с грифом «КТ» производится на основании письменных запросов по разрешению руководителей подразделений, подготовивших эти документы и издания.

Аналогично отметки вносятся в описи и номенклатуры" дел.

4.14. Порядок работы на ЭВМ при обработке информации с грифом «КТ» осуществляется в соответствии с требованиями «Инструкции о порядке работы на ПЭВМ при обработке несекретной информации».

5. Обеспечение сохранности документов, дел и изданий

5.1. Документы, дела и издания с грифом «КТ» должны храниться в служебных помещениях и библиотеках в надежно запираемых и опечатываемых шкафах (хранилищах). При этом должны быть созданы надлежащие условия, обеспечивающие их физическую сохранность.

5.2. Выданные для работы дела с грифом «КТ» подлежат возврату в канцелярию или уполномоченному службы безопасности в тот же день.

Отдельные дела с грифом «КТ» с разрешения начальника канцелярии или уполномоченного службы безопасности могут находиться у исполнителя в течение срока, необходимого для выполнения задания, при условии полного обеспечения их сохранности и соблюдения правил хранения.

5.3. Передача документов, дел и изданий с грифом «КТ» другим сотрудникам, допущенным к этим документам, производится только через канцелярию или уполномоченного службы безопасности.

5.4. Запрещается изъятие из дел или перемещение документов с грифом «КТ» из одного дела в другое без санкции канцелярии или уполномоченного службы безопасности, осуществляющего их учет. Обо всех проведенных изъятиях или перемещениях делаются отметки в учетных документах, включая внутренние описи.

5.5. Запрещается выносить документы, дела и издания с грифом «КТ» из служебных помещений для работы с ними дома, в гостиницах и т. д.

В необходимых случаях директор, его заместители по направлениям или руководители структурных подразделений могут разрешить исполнителям или сотрудникам канцелярии вынос из здания документов с грифом «КТ» для их согласования, подписи и т. д. в организации, находящиеся в пределах данного города.

5.6. Лицам, командированным в другие города, запрещается иметь при себе в пути следования документы, дела или издания с грифом «КТ». Эти материалы должны быть направлены заранее в адрес организации по месту командировки сотрудника, как правило, заказными или ценными почтовыми отправлениями, а также с курьерами.

5.7. При смене сотрудников, ответственных за учет и хранение документов, дел и изданий с грифом «КТ», составляется по произвольной форме акт приема-передачи этих материалов, утверждаемый заместителями директора по направлениям или руководителями структурных подразделений.

6. Обязанности лиц, допущенных к сведениям, составляющим коммерческую тайну

6.1. Лица, допущенные к работам, документам и сведениям, составляющим коммерческую тайну, несут личную ответственность за соблюдение ими установленного режима. Прежде чем получить доступ к коммерческой информации, они должны изучить требования настоящей инструкции и других нормативных документов по защите коммерческой тайны в части, их касающейся, сдать зачет на знание указанных требований и дать индивидуальное письменное обязательство по сохранению коммерческой тайны.

6.2. Лица, допущенные к работам, документам и сведениям, составляющим коммерческую тайну, обязаны:

а) строго хранить коммерческую тайну, ставшую им известной по службе или работе или иным путем, пресекать действия других лиц, которые могут привести к разглашению коммерческой тайны. О таких фактах, а также о других причинах или условиях возможной утечки коммерческой тайны немедленно информировать непосредственного начальника и службу безопасности;

б) в течение договорного периода не использовать известную коммерческую тайну в своих личных целях, а также без соответствующего разрешения руководства не заниматься любой деятельностью, которая в качестве конкурентного действия может нанести ущерб предприятию, являющемуся владельцем этой коммерческой тайны;

в) выполнять только те работы и знакомиться только с теми документами, к которым получили доступ в силу своих служебных обязанностей; знать степень важности выполняемых работ, правильно определять ограничительный гриф документов, строго соблюдать правила пользования ими, порядок их учета и хранения;

г) при составлении документов со сведениями, составляющими коммерческую тайну, ограничиваться минимальными, действительно необходимыми в документе этими сведениями; определять количество экземпляров документов в строгом соответствии с действительной служебной необходимостью и не допускать рассылки их адресатам, к которым они не имеют отношения;

д) на черновиках документов проставлять соответствующий ограничительный гриф и другие необходимые реквизиты. Передавать их для печатания только с письменного разрешения руководителя подразделения;

е) после получения из машинописного бюро отпечатанных документов проверять их наличие, сличать эти данные с записями в журнале и расписываться (с указанием даты) за получение отпечатанных документов и черновиков, после чего учесть в канцелярии или у уполномоченного службы безопасности;

ж) получать документы с грифом «КТ» лично в канцелярии или у уполномоченного службы безопасности. Своевременно знакомиться с полученными документами и разборчиво расписываться на них с указанием даты ознакомления;

з) поступившие документы с грифом «КТ» своевременно направлять для приобщения к делу с соответствующими отметками об исполнении (номер дела, что сделано по документу, дата, подпись) и с резолюцией начальника подразделения;

и) сдавать в канцелярию или уполномоченному по службе безопасности исполненные входящие документы, а также предназначенные для рассылки, подшивки в дело, уничтожения и взятия на инвентарный учет под расписку в журналах учета;

к) иметь внутреннюю опись документов с грифом «КТ», в которой отводится отдельный раздел, и немедленно вносить с нее все полученные для исполнения документы, хранить их только в рабочей папке, а при выходе в рабочее время из помещения рабочую папку с документами запирать в сейф;

л) по окончании работы с документами с грифом «КТ» своевременно возвращать их в канцелярию или уполномоченному службы безопасности;

м) об утрате или недостатке документов с грифом «КТ», ключей от сейфов, личных печатей немедленно сообщать в службу безопасности;

н) при увольнении, перед уходом в отпуск, отъездом в командировку своевременно сдать или отчитаться перед канцелярией или уполномоченным за все числящиеся за ним документы;

о) ознакомить представителей других учреждений с документами с грифом «КТ» с ведома и с письменного разрешения руководителя подразделения; лично знакомиться с разрешениями указанных руководителей на предписании, в котором должны быть определены вопросы и объем сведений, подлежащих рассмотрению; требовать от командированных лиц расписки на документах, с которыми они ознакомились, или в учетных карточках этих документов;

п) документы с грифом «КТ» во время работы располагать так, чтобы исключить возможность ознакомления с ними других лиц, в том числе допущенных к подобным работам и документам, но не имеющих к ним прямого отношения;

р) по первому требованию канцелярии и отдела службы безопасности предъявлять для проверки все числящиеся и имеющиеся документы с грифом «КТ»; представлять по требованию начальника отдела устные или письменные объяснения о нарушениях установленных правил выполнения работ с грифом «КТ», учета и хранения документов с грифом «КТ», а также о фактах разглашения сведений с грифом «КТ», утраты документов, содержащих такие сведения.

7. Принципы организации и проведения контроля за обеспечением режима при работе со сведениями, содержащими коммерческую тайну

7.1. Контроль за обеспечением режима при работе со сведениями, составляющими коммерческую тайну, осуществляется в целях изучения и оценки фактического состояния сохранности коммерческой тайны, выявления недостатков и нарушений режима при работе с материалами с грифом «КТ», установления причин таких недостатков и нарушений и выработки предложений, направленных на их устранение и предотвращение.

7.2. Контроль за обеспечением режима при работе с материалами с грифом «КТ» осуществляет служба безопасности и руководители структурных подразделений.

7.3. Комиссия для проверки обеспечения режима при работе с материалами с грифом «КТ» комплектуется из опытных и квалифицированных работников в составе не менее 2-х человек, имеющих допуск к этой работе. Участие в проверке не должно приводить к необоснованному увеличению осведомленности проверяющих об этих сведениях.

7.4. Проверки обеспечения режима при работе с материалами с грифом «КТ» проводятся не реже одного раза в год комиссиями на основании предписания, подписанного директором или его заместителем по направлению.

7.5. Проверки проводятся в присутствии руководителя структурного подразделения или его заместителя.

7.6. Проверяющие имеют право знакомиться со всеми документами, журналами (карточками) учета и другими материалами, имеющими отношение к проверяемым вопросам, а также проводить беседы и консультации со специалистами и исполнителями, требовать представления письменных объяснений, справок, отчетов по всем вопросам, входящим в компетенцию комиссии.

7.7. По результатам проверок составляется акт (справка) с отражением в нем состояния режима при работе с материалами с грифом «КТ», выявленных недостатков и нарушений, предложений по их устранению.

С актом после утверждения его директором или заместителем под роспись знакомится руководитель структурного подразделения.

7.8. Об устранении выявленных в результате проверки недостатков и нарушений в режиме при работе с материалами с грифом «КТ» и реализации предложений руководитель подразделения в установленные комиссией сроки сообщает начальнику службы безопасности.

7.9. В случае установления факта утраты документов, дел и изданий с грифом «КТ» либо разглашения содержащихся в них сведений немедленно ставятся в известность директор, его заместители по направлениям и начальник службы безопасности.

Для расследования факта утраты документов, дел и изданий с грифом «КТ» при установлении факта разглашения сведений, содержащихся в этих материалах приказом директора (рас-

поряжением руководителя структурного подразделения) назначается комиссия, заключение которой о результатах расследования утверждается руководителем, создавшим данную комиссию.

На утраченные документы, дела и издания с грифом «КТ» составляется акт. Соответствующие отметки вносятся в учетные документы.

Акты на утраченные дела постоянного хранения после их утверждения директором или его заместителями по направлениям передаются в архив для включения в дело фонда.

8. Ответственность за разглашение, утрату документов, содержащих коммерческую тайну

8.1. Разглашение сведений, составляющих коммерческую тайну, - это предание огласке сведений лицом, которому эти сведения были доверены по службе, работе или стали известны иным путем, в результате чего они стали достоянием посторонних лиц.

8.2. Утрата документов, содержащих сведения коммерческой тайны, - это выход (в том числе и временный) документов из владения ответственного за их сохранность лица, которому они были доверены по службе или работе, являющийся результатом нарушения установленных правил обращения с ними, вследствие чего эти документы стали или могли стать достоянием посторонних лиц.

8.3. Иные нарушения режима при работе с материалами коммерческой тайны - это нарушение требований, могущее привести к разглашению этих сведений, утрате документов, содержащих такие сведения.

8.4. За утрату и незаконное уничтожение документов, дел и изданий с грифом «КТ», за разглашение сведений, содержащихся в этих материалах, а также за нарушение требований виновные лица привлекаются к ответственности в установленном порядке.

Приложения к П-12:

1. Договорное обязательство

Договорное обязательство

Я, _____
(фамилия, имя, отчество)

оформляясь на работу, _____ обязуюсь:
(должность, подразделение)

а) в период работы не разглашать сведения, составляющие коммерческую тайну, которые мне будут доверены или станут известны при исполнении служебных обязанностей;

б) беспрекословно и аккуратно выполнять относящиеся ко мне требования приказов, инструкций и положений по защите коммерческой тайны, с которыми я ознакомлен;

в) не сообщать устно или письменно кому бы то ни было сведения, составляющие коммерческую тайну;

г) в случае увольнения не разглашать и не использовать для себя или других сведения, составляющие коммерческую тайну.

Я предупрежден, что в случае нарушения данного обязательства должен возместить ущерб или буду привлечен к дисциплинарной или уголовной ответственности в соответствии с законодательством.

(подпись)

Проинструктировал
«__» _____ 200__ г.

2. Журнал учета документов и изданий с грифом «Коммерческая тайна» (Форма № 1)

Форма № 1

Журнал учета документов и изданий с грифом «Коммерческая тайна»

Порядковый номер (входящий, исходящий)	Дата поступления и индекс документа	Дата и индекс документа	Откуда поступил или куда направлен	Наименование документа и краткое содержание	Количество		Количество и номера экземпляров
					документа	приложения	
1	2	3	4	5	6	7	8

Резолюция или кому направ- лен на испол- нение	Отметка о взя- тии на кон- троль и срок исполнения	Дата и рас-		Индекс (номер) дела, куда подшит документ	Отметка об уничтожении	Примечание
		в по- луче- нии	о воз- врате			
9	10	11	12	13	14	15

3. Карточка учета входящих (исходящих) документов и изданий с грифом «КТ» (Форма № 2)

Форма № 2

Карточка учета входящих (исходящих) документов и изданий с грифом «КТ»

Вход, (исход.) номер и гриф	Дата регистрации	Исход, номер и дата поступившего документа	Количество листов	
			основного документа	приложения

Наименование отправителя: _____

Краткое содержание: _____

Подшивка			Регистрация приложения		
номер дела	номер листов	подписи о сверке, дата	вид	инв. №о	подписи о сверке, дата

Отметка о сверках наличия

Карточка проверена, все позиции закрыты

(ПОДПИСЬ)

« » 20 Г.

(лицевая сторона)

Движение

Дата	Количество основных приложений	Кому выдан или куда отправлен	Роспись в получении или № реестра	Подписи о сверке, дата	Датавозврата	Роспись в приеме или отм. о возврате
------	--------------------------------	-------------------------------	-----------------------------------	------------------------	--------------	--------------------------------------

Для разных отметок:
(оборотная сторона)

4. Журнал учета и распределения изданий с грифом «КТ» (Форма № 3)

Форма № 3

Журнал учета и распределения изданий с грифом «КТ»

[illegible]

5. Карточка учета выдаваемых дел и изданий с грифом «КТ» (Форма № 4)

Форма № 4

Карточка учета выдаваемых дел и изданий с грифом «КТ»					
Наименование дела или издания					
№ п/п	№ дела, экз. изданий кол-во листов	Подразделение и сотрудника фамилия	Расписка		Примечание
			в получении и дата	о возврате и дата	
1	2	3	4	5	6

6. Журнал учета служебных изданий с грифом «КТ» (Форма № 5)

Форма № 5

Журнал учета служебных изданий с грифом «КТ»								
№ п/п	Дата и № сопроводительного письма (накладной)	Откуда поступило, название и год издания	Количество экз.	№ экз	Кому отправлено, дата и исход. №	Кол-во экз.	№ Экз.	Отметка о перучете или уничтожении
1	2	3	4	5	6	7	8	9

7. Типовой договор на комплексное режимное обслуживание

Коммерческая тайна
Экз. № __

ДОГОВОР**коллективного подряда на комплексное режимное обслуживание предприятия**

Настоящий договор заключен между предприятием _____ в лице директора _____ и коллективом службы безопасности в лице зам. директора - начальника службы безопасности _____ о нижеследующем:

1. Служба безопасности берет на себя выполнение нижеперечисленных работ по обеспечению безопасности и сохранения коммерческой тайны предприятия:

1.1. Круглосуточная охрана предприятия и контроль за соблюдением мер пожарной безопасности.

1.2. Выписка пропусков для сотрудников предприятия.

1.3. Прием командированных, выписка пропусков для них.

1.4. Выписка предписаний для выполнения заданий командируемым сотрудникам и выдача справок о допуске.

1.5. Разработка номенклатуры должностей, подлежащих согласованию с контрольными органами, и оформление пропусков.

1.6. Подготовка по представлению директора перечня сведений, составляющих коммерческую тайну, приказов, инструкций о сохранении коммерческой тайны предприятия.

1.7. Оказание услуг по передаче корреспонденции по телетайпу, телексу, телефаксу и другим системам связи.

1.8. Прием, учет и рассылка открытой корреспонденции.

2. Директор предприятия обязуется:

2.1. За работы, перечисленные в настоящем договоре, производить оплату из своих фондов по ведомости на работников службы безопасности в размере _____ рублей ежемесячно.

2.2. Принимать работы по акту, утвержденному директором _____ и зам. директора - начальником службы безопасности _____.

2.3. Обязать сотрудников предприятия выполнять все режимные требования, предусмотренные инструкцией по обеспечению сохранения коммерческой тайны.

2.4. При определении грифа документов руководствоваться ограничительными перечнями сведений, обязательными для исполнителей.

2.5. Немедленно представлять в службу безопасности сведения о вступлении в связь с иносфирмами.

3. Настоящий договор заключается на календарный год, с 01.01.20__ г. до 31.12.20__ г., готовится в 2-х экземплярах, каждый экземпляр хранится у директора и в службе безопасности.

Директор предприятия

Зам. директора -

« » 20 г.« » 20 г.

8. Типовой акт приемки выполнения договорных обязательств

АКТ
о выполнении работ по Договору №

« » 20 Г.

Комиссия в составе представителя предприятия в лице его директора _____ и представителя коллектива безопасности в лице зам. директора - начальника службы безопасности _____ провели работу по установлению фактического выполнения коллективом службы безопасности договора № ____ коллективного подряда на комплексное режимное обслуживание _____ за 20 ____ г.

В результате проверки комиссия установила, что все работы по договору в _____ 20__ г. выполнены качественно, в полном объеме и в установленные сроки.

К акту прилагается ведомость на выплату.

Директор предприятия

Зам. директора -
начальник службы безопасности

« » 20 Г.

« » 20 Г.

П-13. Каталог обобщенных мероприятий по ЗИ

КАТАЛОГ обобщенных мероприятий по защите конфиденциальной информации

В каталоге рассматриваются обобщенные мероприятия по защите конфиденциальной информации от разглашения, утечки по техническим каналам и от несанкционированного доступа со стороны злоумышленников, конкурентов и иных субъектов противоправных интересов.

Каталог состоит из трех разделов:

1. Мероприятия по предупреждению разглашения конфиденциальной информации.
2. Мероприятия по защите информации от утечки по техническим каналам.
3. Мероприятия по пресечению несанкционированного доступа к конфиденциальной информации.

1. Мероприятия по предупреждению разглашения конфиденциальной информации

РАЗГЛАШЕНИЕ - умышленные или неосторожные действия должностных лиц и граждан, приводящие к оглашению конфиденциальной информации, доверенной им по службе, и ознакомлению с ней лиц, не имеющих на это права.

РАЗГЛАШЕНИЕ выражается в сообщении, передаче, предоставлении, пересылке, опубликовании, утере и других способах и реализуется по каналам распространения и средствам массовой информации.

ПРЕДУПРЕЖДЕНИЕ РАЗГЛАШЕНИЯ – это комплекс мероприятий, исключающих или ослабляющих возможность неконтролируемого оглашения конфиденциальной информации.

Таблица П-13.1.

№№ п/п	Способы разглашения	Особенности	ДЕЙСТВИЯ		
			Организационные	Организационно-технические	Технические
1.	Открытое оставление конфиденциальных документов	1. На рабочем столе 2. На экране ПЭВМ и в средствах коллективного пользования 3. В квартире 4. В автомашине	Общеорганизационные меры: 1. Перечень сведений, составляющих коммерческую тайну 2. Обязательства сотрудников о неразглашении коммерческих секретов 3. Мониторинг за лояльностью сотрудников 4. Меры ответственности за разглашение конфиденциальной информации 5. Охрана зданий, помещений и мест хранения документов 1. Расположение рабочего места, исключающее или ограничивающее возможность наблюдения за документами 1. Запрет на работу с конфиденциальной информацией дома 1. Строгий контроль за перевозкой документов	1. Использование технических средств контроля помещений, хранения документов 1. Использование штор, занавесок, драпировок	1. Автоматизированные системы мониторинга за лояльностью сотрудников 1. Комплексные системы охраны и режима 1. Возможный контроль за служебными помещениями с помощью телевизионных систем 1. Использование программных средств гашения информации по регламенту

№№ п/п	Способы разглашения	Особенности	ДЕЙСТВИЯ		
			Организационные	Организационно- технические	Технические
2	Передачи конфиденци- альной ин- формации	1. По каналам электросвязи 2. При разра- ботке и обра- ботке доку- ментов	1.Использование мер сокрытия содержания пере- даваемых сведений 2. Сокращение времени пе- редачи информации 3. Использование методов скрытного ведения сеансов связи 1. Разработка документов в специальных тетрадах и блокнотах	1. Использование тех- нических средств за- щиты информации 2. Использование мас- кираторов, скрембле- ров, средств шифро- вания и электронной подписи в системах связи и телекоммуни- кации 1. Разработка доку- ментов на ПЭВМ с соблюдением требо- ваний защиты конфи- денциальной инфор- мации	1. Передача сообщений по защищенным системам связи и телекоммуникации
3	Сообщение, оглашение	1. На деловых встречах (пе- реговорах) 2. При дело- вой перепис- ке 3. На семина- рах, симпози- умах, в печат- и и других средствах массовой ин- формации 4. На выстав- ках, реклама	1.Четкая регламентация те- матики переговоров 2. Проведение переговоров в специальных помещениях 3. Ограничение на запись информации участниками переговоров: - спец. блокноты - тетради и др. 1.Контроль содержания пе- реписки 1. Соблюдение требований конфиденциальности 1. Тщательный анализ и от- бор информационных мате- риалов и демонстрационных изделий 2. Строгий инструктаж со- трудников в целях соблюде- ния режима конфиденци- альности	1. Запись (аудио или аудио/видео) перегово- ров с целью после- дующего анализа их конфиденциальности 1. Шифрование текста документов 2. Применение устройств скрытного фиксирования неза- конного доступа к до- кументам	1. Использование замкну- тых систем ведения кон- фиденциальных перегово- ров 1. Использование техниче- ских средств шифрования документов

№№ п/п	Способы разглашения	Особенности	ДЕЙСТВИЯ		
			Организационные	Организационно- технические	Технические
4	Пересылка	1. По каналам почтовой связи	1. Шифрование документов 2. Применение специальных конвертов, исключающих проникновение к документам 3. Опечатывание конвертов и упаковок 4. Пересылка спецсвязью или курьерами 5. Предварительное оповещение адресата о высылке документов 6. Уведомление адресата об ответственности за разглашение конфиденциальных сведений 7. Нарочным (знакомый, попутчик)]. Использование аппаратуры шифрования документов]. Использование технических средств шифрования документов
5	Опубликование	1. В печати, диссертационных исследованиях, на радио, телевидении	1. Предварительный контроль публикуемых материалов 2. Перечень сведений, разрешенных к опубликованию в открытой печати		
6	Личное общение	1. На встречах 2. При телефонных переговорах	1. Соблюдение требований о неразглашении конфиденциальной информации 1. Запрещение ведения частных переговоров по служебным телефонам	1. Запись переговоров по служебным телефонам на магнитофон 2. Использование аппаратуры закрытия телефонных переговоров	1. Мониторинг телефонных переговоров специальными системами контроля
7	Утеря, утрата документов	1. На работе 2. За пределами работы	1. Строгий учет и контроль за разработкой, использованием, хранением документов конфиденциального характера 2. Служебное расследование 1. Запрет на вынос служебных документов за пределы организации без надлежащих мер по защите 2. Служебное расследование		

Продолжение табл. П-13.1

8	Бесконтрольная разработка документов	1. Необоснованное изготовление документов 2. Включение в обычные документы сведений конфиденциального характера	1. Регламентация состава конфиденциальных документов 1. Контроль за содержанием документов 2. Контроль за степенью секретности документов		1. Программный контроль изготовления документов на ПЭВМ 1. Программный контроль за содержанием документов 1. Программный контроль секретности документов
9	Бесконтрольный документооборот	1. Необоснованная рассылка документов 2. Необоснованное ознакомление с конфиденциальными документами сотрудников	1. Контроль размножения и рассылки документов 1. Контроль ознакомления сотрудников с конфиденциальными документами с учетом системы разграничения допуска 2. Контроль передачи документов исполнителям 3. Контроль за порядком работы с конфиденциальными документами		1. Программный контроль изготовления и рассылки документов почтой, средствами телекоммуникации и электронной почты 1. Программный контроль допуска сотрудников к конфиденциальной информации 1. Контроль исполнения документов
10	Бесконтрольное хранение и уничтожение документов		1. Обеспечение сохранности документов 2. Своевременное уничтожение документов	1. Использование технических средств механического уничтожения документов	1. Своевременное программное уничтожение документов на ПЭВМ
11	Бесконтрольный прием поступающей корреспонденции		1. Строгий учет поступающих документов 2. Своевременное доведение поступивших документов до руководства и исполнителей		

2. Мероприятия по защите информации от утечки по техническим каналам

УТЕЧКА - это бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена в установленном порядке.

УТЕЧКА возможна по различным техническим каналам утечки информации, в частности по визуально-оптическим, акустическим, электронным и материально-вещественным.

ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ - это комплекс мероприятий, исключающих образование технических каналов утечки конфиденциальной информации.

Таблица П-13.2.

№ п/п	Способы (каналы)	Особенности	ДЕЙСТВИЯ		
			Организационные	Организационно-технические	Технические
1	Визуально-оптические	1. При обычном освещении и в сложных условиях (сумерки, ночь)	1. Расширение зоны безопасности 2. Контроль возможности установления наблюдения 3. Использование особенностей местности	1. Использование защитных средств (шторы, защитные пленки, специальные стекла) 2. Использование средств маскировки	1. Снижение заметности объектов на фоне местности 2. Активное противодействие наблюдению

№ п/п	Способы (каналы)	Особенности	ДЕЙСТВИЯ		
			Организационные	Организационно-технические	Технические
2	Акустические	<p>1. Прямое распространение звука в закрытых объемах</p> <p>2. Прямое распространение звука на открытом пространстве</p> <p>3. Распространение звука в жестких средах (структурный звук)</p>	<p>1. Ведение конфиденциальных переговоров в специальных защищенных помещениях</p> <p>1. Ограничение ведения конфиденциальных переговоров на открытом пространстве</p> <p>2. Использование местных предметов и условий при ведении конфиденциальных переговоров</p> <p>1. Выявление возможности образования каналов утечки информации в жестких средах (стены, воздуховоды, коммуникации)</p>	<p>1. Оборудование помещений средствами защиты переговоров от утечки информации по акустическим каналам</p> <p>1. Строительно-конструкционные меры, исключающие возможность образования акустических каналов</p>	<p>1. Использование защищенных технических средств для ведения конфиденциальных переговоров</p> <p>1. Использование технических средств подавления акустических каналов</p>
3	Электромагнитные	<p>1. За счет микрофонного эффекта в технических средствах</p> <p>2. За счет магнитной составляющей электромагнитного поля</p> <p>3. За счет паразитной генерации усилителей</p> <p>4. По цепям питания электронных систем</p> <p>5. По цепям заземления</p>	<p>1. Принятие мер, исключающих возможность образования канала утечки информации за счет микрофонного эффекта</p> <p>2. Обеспечение контролируемой зоны безопасности</p> <p>1. Обеспечение контролируемой зоны безопасности</p> <p>1. Контроль наличия паразитной генерации усилителей различного назначения в выделенных помещениях</p> <p>1. Использование сетей питания, не имеющих выхода за пределы контролируемой зоны</p> <p>1. Обязательное использование самостоятельных контуров заземления для выделенных помещений</p>	<p>1. Установка аппаратных средств защиты от утечки информации за счет микрофонного эффекта</p> <p>1. Экранирование аппаратуры и помещений</p> <p>2. Заземление аппаратуры</p> <p>1. Экранирование и заземление технических средств и помещений</p> <p>1. Разборка электрических цепей</p> <p>1. Регулярное измерение сопротивления заземления на соответствие нормативным требованиям</p>	<p>1. Использование технических средств, не имеющих микрофонного эффекта</p> <p>1. Использование защищенных технических средств</p> <p>1. Использование сетевых фильтров</p> <p>1. Использование отдельного контура заземления</p>

№ п/п	Способы (каналы)	Особенности	ДЕЙСТВИЯ		
			Организационные	Организационно-технические	Технические
4	Материально-вещественные	<p>6. За счет взаимного влияния проводов и линий связи</p> <p>7. За счет высокочастотного навязывания</p> <p>8. По волоконно-оптическим каналам связи</p> <p>1. Бесконтрольный выход продуктов отхода производства за пределы территории предприятия</p> <p>2. Бесконтрольный выход отходов информационных технологий за пределы территории предприятия</p>	<p>1. Исключить параллельный пробег телефонных проводов и линий связи, по которым ведется передача конфиденциальной информации</p> <p>1. Исследование возможностей образования каналов утечки информации за счет ВЧ-навязывания</p> <p>1. Контроль возможного образования каналов утечки по волоконно-оптическим каналам</p> <p>1. Строгий контроль и ограничение (исключение) выхода продуктов отхода производства за пределы территории предприятия</p> <p>1. Организация уничтожения информации на технических носителях</p>	<p>1. Использование экранированных кабелей</p> <p>2. Использование различных приемов прокладки проводов, ослабляющих взаимное влияние</p> <p>1. Строгое соблюдение требований по соблюдению мер защиты от утечки информации</p> <p>1. Исключение отходов в качестве вторичного сырья</p> <p>2. Утилизация отходов</p>	<p>1. Системы безотходного производства</p> <p>2. Система очистки жидких и газообразных веществ</p> <p>1. Установки уничтожения информации на неисправных носителях</p>

3. Мероприятия по пресечению НСД к конфиденциальной информации

НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП (НСД) к источникам конфиденциальной информации - это противоправное преднамеренное овладение охраняемыми сведениями лицом, не имеющим права доступа к ним.

НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП (НСД) реализуется различными способами посредством каналов проникновения на объекты криминальных интересов.

ПРЕСЕЧЕНИЕ несанкционированного доступа - это комплекс мероприятий, исключающих или ослабляющих возможность проникновения к коммерческим секретам заходными и беззаходными способами.

Таблица П-13.3.

№ п/п	Способ несанкционированного доступа	Особенности	ПРОТИВОДЕЙСТВИЕ		
			Организационные меры	Организационно-технические меры	Технические меры
1.	Инициативное сотрудничество	1. Условия, провоцирующие инициативное сотрудничество	<p>1. Исключение условий способствующих инициативному сотрудничеству</p> <p>2. Анализ и контроль социальных условий в трудовых коллективах</p> <p>3. Изучение сотрудников, потенциально способных к инициативному сотрудничеству</p>	1. Использование технических средств контроля социально-морального климата	

№ п/п	Способ несанкционированного доступа	Особенности	ПРОТИВОДЕЙСТВИЕ		
			Организационные меры	Организационно-технические меры	Технические меры
2	Склонение к сотрудничеству	1. Шантаж, запугивание, подкуп	1. Изучение сотрудников, представляющих интерес для конкурентов и преступных групп		
3	Выпытывание, выводывание	1. Провоцирование на разговоры сотрудников на служебные темы на работе, в общественных местах, на отдыхе и др. 2. Выведывание при ведении телефонных разговоров	1. Обучение и воспитание кадров в направлении строгого соблюдения требований по защите коммерческих секретов	1. Использование портативных магнитофонов для контроля и последующего анализа на предмет выявления злонамеренных действий	
4	Подслушивание	1. Подслушивание конфиденциальных разговоров руководства и сотрудников в помещениях 2. Подслушивание конфиденциальных переговоров в автотранспорте 3. Подслушивание конфиденциальных разговоров на открытой местности	1. Ведение конфиденциальных разговоров в специальных помещениях 1. Запрет на ведение конфиденциальных переговоров в автотранспорте 1. Информирование сотрудников о возможности использования злоумышленниками направленных микрофонов	1. Использование специальных магнитофонов для записи и анализа злонамеренных действий 1. Оборудование помещений шумопоглощающими средствами 2. Постановка акустических помех 1. Использование средств постановки акустических помех	1. Использование аппаратуры контроля телефонных переговоров 1. Использование специальных систем ведения конфиденциальных бесед (переговоров)
5	Визуальное наблюдение	1. Использование злоумышленником визуальных средств наблюдения за состоянием и деятельностью предприятия (организации) 2. Использование злоумышленником оптических средств наблюдения	2. Ведение переговоров с использованием маскирующих свойств местности 1. Использование штор, занавесей, драпировок	1. Использование специальных стекол	1. Постановка оптических помех
6	Хищение	1. Первичных документов 2. Носителей конфиденциальной информации	1. Строгий учет и контроль разработки движения и уничтожения документов	1. Строгий учет и контроль движения технических носителей информации организационно-техническими мерами	1. Широкое использование программных методов обеспечения защиты информации

№ п/п	Способ несанкционированного доступа	Особенности	ПРОТИВОДЕЙСТВИЕ		
			Организационные меры	Организационно-технические меры	Технические меры
7	Копирование	3. Промежуточных документов 4. Исходящих документов 5. Производственных отходов 1. Копирование документов	1. Строгая регламентация правил сбора и уничтожения отходов 1. Регламентация и учет разработки, размножения и рассылки конфиденциальных документов 2. Копирование данных и программ на ЭВМ	1. Установка специальных ящиков для отходов производства 1. Строгая регламентация технологий обработки информации 2. Учет и регистрация режимов работы и выдачи документов	1. Использование аппаратуры и оборудования для уничтожения отходов производства 1. Использование программкой защиты от несанкционированных действий с конфиденциальной информацией при работе на ПЭВМ
8	Подделка (модификация)	1. Подделка деловых документов 2. Подделка финансовых документов 3. Подделка личных документов	1. Строгий контроль изготовления, учета и рассылки документов I. Использование специальных методов изготовления личных документов	1. Использование специальных средств подтверждения подлинности документов (специальные чернила и краски и др.)	I. Использование специальной аппаратуры обнаружения исправлений и подделки документов
9.	Уничтожение (порча, разрушение)	1. Документов 2. Продукции 3. Программного обеспечения	1. Исключение несанкционированного доступа к конфиденциальным документам 1. Обеспечение мер по охране и защите продукции в местах ее нахождения I. Обеспечение мер по разграничению доступа к программному обеспечению	1. Использование специальных сейфов для хранения конфиденциальных документов 1.Использование программно-аппаратных методов защиты программ и массивов данных от неправомерного воздействия	1.Использование охранно-пожарных систем наблюдения и контроля
10	Незаконное подключение к линиям и системам связи	I. Контактное 2.Бесконтактное	1.Использование скрытых коммуникаций 2.Охрана мест возможного подключения 1. Использование скрытых коммуникаций 2. Охрана мест возможного подключения	1. Контроль линий и систем связи на наличие подключений 2. Использование экранированных кабелей 1. Использование экранированных кабелей	1. Использование средств противодействия незаконному подключению (заземление прожигание) 2. Использование средств маскирования или шифрования передаваемой информации 1. Использование средств маскирования или шифрования передаваемой информации

№ п/п	Способ несанкционированного доступа	Особенности	ПРОТИВОДЕЙСТВИЕ		
			Организационные меры	Организационно-технические меры	Технические меры
11	Перехват	1. Перехват информации, передаваемой по системам радио-связи 2. Перехват информации за счет побочных электромагнитных излучений и наводок	1. Использование методов скрытого ведения связи 2. Запрещение ведения переговоров конфиденциального характера 1. Проведение мероприятий по исключению образования побочных электромагнитных излучений	1. Использование технических средств засекречивания информации 1. Использование способов ослабления ПЭМИН 2. Экранирование помещений	1. Использование защищенных средств связи 2. Использование активных мер подавления ПЭМИН
12	Негласное озвучивание	1.С документами 2.С информацией на экранах ПЭВМ	1. Организация работы с документами, исключаящими ознакомления с их содержанием		
13	Фотографирование	1. Документов 2. Продукции	1. Организация работы с документами, исключаящими ознакомления с их содержанием		
14	Сбор и аналитическая обработка		1. Разработка системы мер по сокрытию конфиденциальной информации 2. Четко организованная работа по дезинформированию злоумышленников		

П-14. Специальные требования Гостехкомиссии по технической ЗИ

ГОСУДАРСТВЕННАЯ ТЕХНИЧЕСКАЯ КОМИССИЯ ПРИ ПРЕЗИДЕНТЕ РФ

СПЕЦИАЛЬНЫЕ ТРЕБОВАНИЯ И РЕКОМЕНДАЦИИ
ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ
КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ
(СТР-К)

Москва, 2001

Содержание

1. Термины, определения и сокращения
2. Общие положения
3. Организация работ по защите информации
4. Требования и рекомендации по защите речевой информации
 - 4.1. Общие положения
 - 4.2. Основные требования и рекомендации по защите информации, циркулирующей в защищаемых помещениях
 - 4.3. Защита информации, циркулирующей в системах звукоусиления и звукового сопровождения кинофильмов
 - 4.4. Защита информации при проведении звукозаписи
 - 4.5. Защита речевой информации при ее передаче по каналам связи
5. Требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники
 - 5.1. Общие требования и рекомендации
 - 5.2. Основные требования и рекомендации по защите служебной тайны и персональных данных
 - 5.3. Основные рекомендации по защите информации, составляющей коммерческую тайну
 - 5.4. Порядок обеспечения защиты конфиденциальной информации при эксплуатации АС
 - 5.5. Защита конфиденциальной информации на автоматизированных рабочих местах на базе автономных ПЭВМ
 - 5.6. Защита информации при использовании съемных накопителей большой емкости для автоматизированных рабочих мест на базе автономных ПЭВМ
 - 5.7. Защита информации в локальных вычислительных сетях
 - 5.8. Защита информации при межсетевом взаимодействии
 - 5.9. Защита информации при работе с системами управления базами данных
6. Рекомендации по обеспечению защиты информации, содержащейся в негосударственных информационных ресурсах, при взаимодействии абонентов с информационными сетями общего пользования
 - 6.1. Общие положения
 - 6.2. Условия подключения абонентов к Сети
 - 6.3. Порядок подключения и взаимодействия абонентских пунктов с Сетью, требования и рекомендации по обеспечению безопасности информации
7. Приложения
 - № 1. Акт классификации АС обработки информации
 - № 2. Аттестат соответствия требованиям по безопасности информации на АС
 - № 3. Аттестат соответствия требованиям по безопасности информации на ЗП
 - № 4. Форма технического паспорта на ЗП
 - № 5. Форма технического паспорта на АС
 - № 6. Пример оформления перечня сведений конфиденциального характера
 - № 7. Основные нормативные правовые акты и методические документы по защите конфиденциальной информации

1. Термины, определения и сокращения

В настоящем документе приняты следующие основные термины, определения и сокращения:

1.1. Абонент Сети - лицо, являющееся сотрудником учреждения (предприятия), имеющее соответствующим образом оформленное разрешение и технические возможности на подключение и взаимодействие с Сетями.

1.2. Абонентский пункт (АП) - средства вычислительной техники учреждения (предприятия), подключаемые к Сетям с помощью коммуникационного оборудования.

АП могут быть в виде автономных персональных электронно-вычислительных машин (ПЭВМ) с модемом и не иметь физических каналов связи с другими средствами вычислительной техники (СВТ) предприятия, а также в виде одной или нескольких объединенных локальных вычислительных сетей (ЛВС) с рабочими станциями и серверами, соединенных с Сетями через коммуникационное оборудование (модемы, мосты, шлюзы, маршрутизаторы-роутеры, мультиплексоры, коммуникационные серверы и т.п.).

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

1.4. Администратор АС - лицо, ответственное за функционирование автоматизированной системы в установленном штатном режиме работы.

1.5. Администратор защиты (безопасности) информации - лицо, ответственное за защиту автоматизированной системы от несанкционированного доступа к информации.

1.6. Безопасность информации - состояние защищенности информации, характеризующееся способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность (т.е. сохранение в тайне от субъектов, не имеющих полномочий на ознакомление с ней), целостность и доступность информации при ее обработке техническими средствами.

1.7. Вспомогательные технические средства и системы (ВТСС) - технические средства и системы, не предназначенные для передачи, обработки и хранения конфиденциальной информации, устанавливаемые совместно с основными техническими средствами и системами или в защищаемых помещениях.

К ним относятся:

- различного рода телефонные средства и системы;
- средства и системы передачи данных в системе радиосвязи;
- средства и системы охранной и пожарной сигнализации;
- средства и системы оповещения и сигнализации;
- контрольно-измерительная аппаратура;
- средства и системы кондиционирования;
- средства и системы проводной радиотрансляционной сети и приема программ радиовещания и телевидения (абонентские громкоговорители, системы радиовещания, телевизоры и радиоприемники и т.д.);
- средства электронной оргтехники;
- средства и системы электрочасофикации;
- иные технические средства и системы.

1.8. Доступ к информации (доступ) - ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации.

1.9. Доступность (санкционированная доступность) информации - состояние информации, характеризующееся способностью технических средств и информационных технологий обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия.

1.10. Закладочное устройство - элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограж-

дение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

1.11. Защита информации от несанкционированного доступа (защита от НСД) или воздействия - деятельность, направленная на предотвращение или существенное затруднение несанкционированного доступа к информации (или воздействия на информацию) с нарушением установленных прав или правил.

1.12. Специальный защитный знак (СЗЗ) - сертифицированное и зарегистрированное в установленном порядке изделие, предназначенное для контроля несанкционированного доступа к объектам защиты путем определения подлинности и целостности СЗЗ, путем сравнения самого знака или композиции «СЗЗ - подложка» по критериям соответствия характерным признакам визуальными, инструментальными и другими методами.

1.13. Защищаемые помещения (ЗП) – помещения (служебные кабинеты, актовые, конференц-залы и т.д.), специально предназначенные для проведения конфиденциальных мероприятий (совещаний, обсуждений, конференций, переговоров и т.п.).

1.14. Информативный сигнал – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация, передаваемая, хранящаяся или обрабатываемая в основных технических средствах и системах и обсуждаемая в ЗП.

1.15. Информационные сети общего пользования (далее Сети) — вычислительные (информационно-телекоммуникационные) сети, открытые для пользования всем физическим и юридическим лицам, в услугах которых этим лицам не может быть отказано.

1.16. Контролируемая зона (КЗ) - это пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового пропуска, и посторонних транспортных средств.

Границей КЗ могут являться:

- периметр охраняемой территории учреждения (предприятия) ;
- ограждающие конструкции охраняемого здания или охраняемой части здания, если оно размещено на неохраняемой территории.

В отдельных случаях, на период обработки техническими средствами конфиденциальной информации, КЗ временно может устанавливаться большей, чем охраняемая территория предприятия. При этом должны приниматься организационно-режимные и технические меры, исключающие или существенно затрудняющие возможность ведения перехвата информации в этой зоне.

1.17. Конфиденциальная информация - информация содержащая сведения, не составляющие государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

1.18. Локальная вычислительная сеть (ЛВС) - совокупность ЭВМ, сетевого оборудования и структурированной кабельной системы, осуществляющая обмен информации с другими информационными системами, в том числе с ЛВС, через определенные точки входа/ выхода информации, которые являются границей ЛВС.

1.19. 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.

1.20. Несанкционированный доступ (несанкционированные действия) (НСД) - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

1.21. Основные технические средства и системы (ОТСС) - технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденци-

альной информации. В контексте настоящего документа к ним относятся технические средства и системы автоматизированных систем различного уровня и назначения на базе средств вычислительной техники, средства и системы связи и передачи данных, используемые для обработки конфиденциальной информации.

1.22. Провайдер Сети - уполномоченная организация, выполняющая функции поставщика услуг Сети для абонентского пункта и непосредственно для абонентов Сети.

1.23. Система защиты информации от НСД (СЗИ НСД), - комплекс организационных мер и программно-технических (в том числе криптографических) средств защиты от несанкционированного доступа к информации (несанкционированных действий с ней) в автоматизированных системах.

1.24. Служебная информация СЗИ НСД - информационная база АС, необходимая для функционирования СЗИ НСД (уровень полномочий эксплуатационного персонала АС, матрица доступа, ключи, пароли и т.д.).

1.25. Технический канал утечки информации совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

1.26. Техническая защита конфиденциальной информации (ТЗИ) - защита информации не криптографическими методами, направленными на предотвращение утечки защищаемой информации по техническим каналам, от несанкционированного доступа к ней и от специальных воздействий на информацию в целях ее уничтожения, искажения и блокирования.

1.27. Услуги Сети - комплекс функциональных возможностей, предоставляемых абонентам сети с помощью прикладных протоколов {протоколы электронной почты, FTP - File Transfer Protocol - прием/передача файлов, HTTP - Hiper Text Transfer Protocol - доступ к Web-серверам, IRC - Internet Relay Chat - диалог в реальном времени, Telnet - терминальный доступ в сети, WAIS - Wide Area Information Servers - система хранения и поиска документов в сети и т.д.).

1.28. Целостность информации - устойчивость информации к несанкционированному или случайному воздействию на нее в процессе обработки техническими средствами, результатом которого может быть уничтожение и искажение информации.

1.29. Web-сервер - общедоступный в Сети информационный сервер, использующий гипертекстовую технологию.

2. Общие положения

2.1. Настоящий документ устанавливает порядок организации работ, требования и рекомендации по обеспечению технической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну (далее конфиденциальная информация) на территории Российской Федерации.

2.2. Документ разработан на основании федеральных законов «Об информации, информатизации и защите информации», «Об участии в международном информационном обмене», Указа Президента Российской Федерации от 06.03.97 г. № 188 «Перечень сведений конфиденциального характера», «Доктрины информационной безопасности Российской Федерации», утвержденной Президентом Российской Федерации 09.09.2000 г. № 1895, «Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти», утвержденного постановлением Правительства Российской Федерации от 03.11.94 г. № 1233, других нормативных правовых актов по защите информации (Приложение № 7), а также опыта реализации мер защиты информации в министерствах и ведомствах, в учреждениях и на предприятиях.

2.3. Требования и рекомендации настоящего документа распространяются на защиту государственных информационных ресурсов не криптографическими методами, направленными на предотвращение утечки защищаемой информации по техническим каналам, от несанкционированного доступа к ней и от специальных воздействий на информацию в целях ее уничтожения, искажения и блокирования.

Защита государственных информационных ресурсов криптографическими методами в настоящем документе не рассматривается.

Для негосударственных информационных ресурсов (составляющих коммерческую, банковскую тайну и т.д.) данный документ носит рекомендательный характер.

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

Режим защиты конфиденциальной информации устанавливается собственником информационных ресурсов или уполномоченным лицом в соответствии с законодательством Российской Федерации.

Уровень технической защиты конфиденциальной информации, а также перечень необходимых мер защиты определяется дифференцированно по результатам обследования объекта информатизации, с учетом соотношения затрат на организацию технической защиты информации и величины ущерба, который может быть нанесен собственнику конфиденциальной информации (информационных ресурсов) при (ее) их разглашении, утрате, уничтожении, искажении, блокировании.

Для персональных данных и сведений, составляющих служебную тайну, уровень технической защиты информации должен быть не ниже требований, установленных данным документом и государственными стандартами Российской Федерации.

2.5. Документ определяет следующие основные вопросы защиты информации:

- организацию работ по защите информации, в том числе при разработке и модернизации объектов информатизации и их систем защиты информации;
- состав и основное содержание организационно-распорядительной, проектной, эксплуатационной и иной документации по защите информации;
- требования и рекомендации по защите речевой информации при осуществлении переговоров, в том числе с использованием технических средств?
- требования и рекомендации по защите информации при ее автоматизированной обработке и передаче с использованием технических средств;
- порядок обеспечения защиты информации при эксплуатации объектов информатизации;
- особенности защиты информации при разработке и эксплуатации автоматизированных систем, использующих различные типы средств вычислительной техники и информационные технологии;
- порядок обеспечения защиты информации при взаимодействии абонентов с информационными сетями общего пользования.

Порядок разработки, производства, реализации и использования средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, определяется Положением ПКЗ-99, утвержденным приказом ФАПСИ от 23.09.99 г. № 158 и зарегистрированным Министерством юстиции Российской Федерации за № 2029 от 28.12.99 г., а также Инструкцией об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной приказом ФАПСИ от 13.06.2001 г. № 152, зарегистрированным Министерством юстиции Российской Федерации за № 2848 от 06.08.2001 г.

2.6. Защита информации, обрабатываемой с использованием технических средств, является составной частью работ по созданию и эксплуатации объектов информатизации различного назначения и должна осуществляться в установленном настоящим документом порядке в виде системы (подсистемы) защиты информации во взаимосвязи с другими мерами по защите информации.

2.7. Защите подлежит информация, как речевая, так и обрабатываемая техническими средствами, а также представленная в виде информативных электрических сигналов, физических

полей, носителей на бумажной, магнитной, оптической и иной основе, в виде информационных массивов и баз данных в АС.

Объектами защиты при этом являются:

- средства и системы информатизации (средства вычислительной техники, автоматизированные системы различного уровня и назначения на базе средств вычислительной техники, в том числе информационно-вычислительные комплексы, сети и системы, средства и системы связи и передачи данных, технические средства приема, передачи и обработки информации (телефонии, звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), средства защиты информации, используемые для обработки конфиденциальной информации;
- технические средства и системы, не обрабатывающие непосредственно конфиденциальную информацию, но размещенные в помещениях, где она обрабатывается (циркулирует);
- защищаемые помещения.

2.8. Защита информации должна осуществляться посредством выполнения комплекса мероприятий и применения (при необходимости) средств ЗИ по предотвращению утечки информации или воздействия на нее по техническим каналам, за счет несанкционированного доступа к ней, по предупреждению преднамеренных программно-технических воздействий с целью нарушения целостности (уничтожения, искажения) информации в процессе ее обработки, передачи и хранения, нарушения ее доступности и работоспособности технических средств.

2.9. При ведении переговоров и использовании технических средств для обработки и передачи информации возможны следующие каналы утечки и источники угроз безопасности информации:

- акустическое излучение информативного речевого сигнала;
- электрические сигналы, возникающие посредством преобразования информативного сигнала из акустического в электрический за счет микрофонного эффекта и распространяющиеся по проводам и линиям, выходящим за пределы КЗ;
- виброакустические сигналы, возникающие посредством преобразования информативного акустического сигнала при воздействии его на строительные конструкции и инженерно-технические коммуникации защищаемых помещений;
- несанкционированный доступ и несанкционированные действия по отношению к информации в автоматизированных системах, в том числе с использованием информационных сетей общего пользования;
- воздействие на технические или программные средства информационных систем в целях нарушения конфиденциальности, целостности и доступности информации, работоспособности технических средств, средств защиты информации посредством специально внедренных программных средств;
- побочные электромагнитные излучения информативных сигналов от технических средств и линий передачи информации;
- наводки информативного сигнала, обрабатываемого техническими средствами, на цепи электропитания и линии связи, выходящие за пределы КЗ;
- радиоизлучения, модулированные информативным сигналом, возникающие при работе различных генераторов, входящих в состав технических средств, или при наличии паразитной генерации в узлах (элементах) технических средств;
- радиоизлучения или электрические сигналы от внедренных в технические средства и защищаемые помещения специальных электронных устройств съема речевой информации («закладочные устройства»), модулированные информативным сигналом;
- радиоизлучения или электрические сигналы от электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки информации;

- прослушивание ведущихся телефонных и радиопереговоров;
- просмотр информации с экранов дисплеев и других средств ее отображения, бумажных и иных носителей информации, в том числе с помощью оптических средств;
- хищение технических средств с хранящейся в них информацией или отдельных носителей информации.

2.10. Перехват информации или воздействие на нее с использованием технических средств могут вестись:

- из-за границы КЗ из близлежащих строений и транспортных средств;
- из смежных помещений, принадлежащих другим учреждениям (предприятиям) и расположенным в том же здании, что и объект защиты;
- при посещении учреждения (предприятия) посторонними лицами;
- за счет несанкционированного доступа (несанкционированных действий) к информации, циркулирующей в АС, как с помощью технических средств АС, так и через информационные сети общего пользования.

2.11. В качестве аппаратуры перехвата или воздействия на информацию и технические средства могут использоваться портативные возимые и носимые устройства, размещаемые вблизи объекта защиты либо подключаемые к каналам связи или техническим средствам обработки информации, а также электронные устройства съема информации «закладочное устройство», размещаемые внутри или вне защищаемых помещений.

2.12. Кроме перехвата информации техническими средствами возможно непреднамеренное попадание защищаемой информации к лицам, не допущенным к ней, но находящимся в пределах КЗ. Это возможно, например, вследствие:

- непреднамеренного прослушивания без использования технических средств конфиденциальных разговоров из-за недостаточной звукоизоляции ограждающих конструкций защищаемых помещений и их инженерно-технических систем;
- случайного прослушивания телефонных разговоров при проведении профилактических работ в сетях телефонной связи;
- некомпетентных или ошибочных действий пользователей и администраторов АС при работе вычислительных сетей;
- просмотра информации с экранов дисплеев и других средств ее отображения.

2.13. Выявление и учет факторов, воздействующих или могущих воздействовать на защищаемую информацию (угроз безопасности информации) в конкретных условиях, в соответствии с ГОСТ Р 51275-99, составляют основу для планирования и осуществления мероприятий, направленных на защиту информации на объекте информатизации.

2.14. Основное внимание должно быть уделено защите информации, в отношении которой угрозы безопасности информации реализуются без применения сложных технических средств перехвата информации:

- речевой информации, циркулирующей в защищаемых помещениях;
- информации, обрабатываемой средствами вычислительной техники, от несанкционированного доступа и несанкционированных действий;
- информации, выводимой на экраны видеомониторов;
- информации, передаваемой по каналам связи, выходящим за пределы КЗ.

2.15. Разработка мер и обеспечение защиты информации осуществляются подразделениями по защите информации (службами безопасности) или отдельными специалистами, назначаемыми руководством предприятия (учреждения) для проведения таких работ.

Разработка мер защиты информации может осуществляться также сторонними предприятиями, имеющими соответствующие лицензии Гостехкомиссии России либо ФСБ России и ФАПСИ России на право осуществления соответствующих работ.

2.16. Для защиты конфиденциальной информации рекомендуется использовать сертифицированные по требованиям безопасности информации технические средства обработки и передачи информации, технические и программные средства защиты информации.

Для защиты информации, составляющей служебную тайну, и персональных данных средства защиты информации должны быть сертифицированы в обязательном порядке.

2.17. Объекты информатизации должны быть аттестованы на соответствие требованиям по защите информации* /Здесь и далее под аттестацией понимается комиссия приемка объекта информатизации силами предприятия с обязательным участием специалиста по защите информации/.

2.18. Ответственность за обеспечение требований по технической защите конфиденциальной информации возлагается на руководителей учреждений и предприятий, эксплуатирующих объекты информатизации.

3. Организация работ по защите информации

3.1. Организация и проведение работ по технической защите информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, при ее обработке техническими средствами определяются настоящим документом, действующими государственными стандартами и другими нормативными и методическими документами Гостехкомиссии России.

3.2. Организация работ по защите информации возлагается на руководителей учреждений и предприятий, руководителей подразделений, осуществляющих разработку проектов объектов информатизации и их эксплуатацию, а методическое руководство и контроль за эффективностью предусмотренных мер защиты информации, на руководителей подразделений по защите информации (служб безопасности) учреждения (предприятия).

3.3. Научно-техническое руководство и непосредственную организацию работ по созданию (модернизации) системы защиты информации (СЗИ) объекта информатизации осуществляет его главный конструктор или другое должностное лицо, обеспечивающее научно-техническое руководство созданием объекта информатизации.

3.4. Разработка СЗИ может осуществляться как подразделением учреждения (предприятия), так и специализированными предприятиями, имеющими лицензии Гостехкомиссии России и/или ФАПСИ на соответствующий вид деятельности.

В случае разработки СЗИ или ее отдельных компонентов специализированным предприятием, в учреждении (на предприятии), для которого осуществляется разработка (предприятие-заказчик), определяются подразделения (или отдельные специалисты), ответственные за организацию и проведение (внедрение и эксплуатацию) мероприятий по защите конфиденциальной информации.

Разработка и внедрение СЗИ осуществляется во взаимодействии разработчика со службой безопасности предприятия-заказчика, которая осуществляет методическое руководство и участвует в разработке конкретных требований по защите информации, аналитическом обосновании необходимости создания СЗИ, согласовании выбора средств вычислительной техники и связи, технических и программных средств защиты, организации работ по выявлению возможностей и предупреждению утечки и нарушения целостности защищаемой информации, в аттестации объектов информатизации.

3.5. Организация работ по созданию и эксплуатации объектов информатизации и их СЗИ определяется в разрабатываемом на предприятии «Руководстве по защите информации» или в специальном «Положении о порядке организации и проведения работ по защите информации» и должна предусматривать:

- порядок определения защищаемой информации;
- порядок привлечения подразделений предприятия, специализированных сторонних организаций к
- разработке и эксплуатации объектов информатизации и СЗИ, их задачи и функции на различных стадиях создания и эксплуатации объекта информатизации;
- порядок взаимодействия всех занятых в этой работе организаций, подразделений и специалистов;
- порядок разработки, ввода в действие и эксплуатацию объектов информатизации;

- ответственность должностных лиц за своевременность и качество формирования требований по технической защите информации, за качество и научно-технический уровень разработки СЗИ.

3.6. В учреждении (на предприятии) должен быть документально оформлен перечень сведений конфиденциального характера (приложение № 6), подлежащих защите в соответствии с нормативными правовыми актами, а также разработана соответствующая разрешительная система доступа персонала к такого рода сведениям.

Рекомендуются следующие стадии создания системы защиты информации:

- предпроектная стадия, включающая предпроектное обследование объекта информатизации, разработку аналитического обоснования необходимости создания СЗИ и технического (частного технического) задания на ее создание;
- стадия проектирования (разработки проектов) и реализации объекта информатизации, включающая разработку СЗИ в составе объекта информатизации;
- стадия ввода в действие СЗИ, включающая опытную эксплуатацию и приемосдаточные испытания средств защиты информации, а также аттестацию объекта информатизации на соответствие требованиям безопасности информации.

3.8. На предпроектной стадии по обследованию объекта информатизации:

- устанавливается необходимость обработки (обсуждения) конфиденциальной информации на данном объекте информатизации;
- определяется перечень сведений конфиденциального характера, подлежащих защите от утечки по техническим каналам; определяются (уточняются) угрозы безопасности информации и модель вероятного нарушителя применительно к конкретным условиям функционирования;
- определяются условия расположения объектов информатизации относительно границ КЗ;
- определяются конфигурация и топология автоматизированных систем и систем связи в целом и их отдельных компонентов, физические, функциональные и технологические связи как внутри этих систем, так и с другими системами различного уровня и назначения;
- определяются технические средства и системы, предполагаемые к использованию в разрабатываемой АС и системах связи, условия их расположения, общесистемные и прикладные программные средства, имеющиеся на рынке и предлагаемые к разработке;
- определяются режимы обработки информации в АС в целом и в отдельных компонентах;
- определяется класс защищенности АС;
- определяется степень участия персонала в обработке (обсуждении, передаче, хранении) информации, характер их взаимодействия между собой и со службой безопасности;
- определяются мероприятия по обеспечению конфиденциальности информации в процессе проектирования объекта информатизации.

3.9. По результатам предпроектного обследования разрабатывается аналитическое обоснование необходимости создания СЗИ.

На основе действующих нормативных правовых актов и методических документов по защите конфиденциальной информации, в том числе настоящего документа, с учетом установленного класса защищенности АС задаются конкретные требования по защите информации, включаемые в техническое (частное техническое) задание на разработку СЗИ.

3.10. Предпроектное обследование в части определения защищаемой информации должно базироваться на документально оформленных перечнях сведений конфиденциального характера.

Перечень сведений конфиденциального характера составляется заказчиком объекта информатизации и оформляется за подписью соответствующего руководителя.

3.11. Предпроектное обследование может быть поручено специализированному предприятию, имеющему соответствующую лицензию, но и в этом случае анализ информационного

обеспечения в части защищаемой информации целесообразно выполнять представителям предприятия-заказчика при методической помощи специализированного предприятия.

Ознакомление специалистов этого предприятия с защищаемыми сведениями осуществляется в установленном на предприятии-заказчике порядке.

3.12. Аналитическое обоснование необходимости создания СЗИ должно содержать:

- информационную характеристику и организационную структуру объекта информатизации;
 - характеристику комплекса основных и вспомогательных технических средств, программного обеспечения, режимов работы, технологического процесса обработки информации;
 - возможные каналы утечки информации и перечень мероприятий по их устранению и ограничению;
- перечень предлагаемых к использованию сертифицированных средств защиты информации;
- обоснование необходимости привлечения специализированных организаций, имеющих необходимые лицензии на право проведения работ по защите информации;
 - оценку материальных, трудовых и финансовых затрат на разработку и внедрение СЗИ;
 - ориентировочные сроки разработки и внедрения СЗИ;
 - перечень мероприятий по обеспечению конфиденциальности информации на стадии проектирования объекта информатизации.

Аналитическое обоснование подписывается руководителем предпроектного обследования, согласовывается с главным конструктором (должностным лицом, обеспечивающим научно-техническое руководство созданием объекта информатизации), руководителем службы безопасности и утверждается руководителем предприятия-заказчика.

3.13. Техническое (частное техническое) задание на разработку СЗИ должно содержать:

- обоснование разработки;
- исходные данные создаваемого (модернизируемого) объекта информатизации в техническом, программном, информационном и организационном аспектах;
- класс защищенности АС;
- ссылку на нормативные документы, с учетом которых будет разрабатываться СЗИ и приниматься в эксплуатацию объект информатизации;
- конкретизацию требований к СЗИ на основе действующих нормативно-методических документов и установленного класса защищенности АС;
- перечень предполагаемых к использованию сертифицированных средств защиты информации;
- обоснование проведения разработок собственных средств защиты информации, невозможности или нецелесообразности использования имеющихся на рынке сертифицированных средств защиты информации;
- состав, содержание и сроки проведения работ по этапам разработки и внедрения;
- перечень видов работ подрядных организаций-исполнителей;
- перечень предъявляемой заказчику научно-технической продукции и документации.

3.14. Техническое (частное техническое) задание на разработку СЗИ подписывается разработчиком, согласовывается со службой безопасности предприятия-заказчика, подрядными организациями и утверждается заказчиком.

3.15. В целях дифференцированного подхода к защите информации производится классификация АС по требованиям защищенности от НСД к информации.

Класс защищенности АС от НСД к информации устанавливается совместно заказчиком и разработчиком АС с привлечением специалистов по защите информации в соответствии с требованиями руководящего документа (РД) Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» и раздела 5 настоящего документа и оформляется актом.

Пересмотр класса защищенности АС производится в обязательном порядке, если произошло изменение хотя бы одного из критериев, на основании которых он был установлен.

3.16. На стадии проектирования и создания объекта информатизации и СЗИ в его составе на основе предъявляемых требований и заданных заказчиком ограничений на финансовые, материальные, трудовые и временные ресурсы осуществляются:

- разработка задания и проекта на строительные, строительно-монтажные работы (или реконструкцию) объекта информатизации в соответствии с требованиями технического (частного технического) задания на разработку СЗИ;
- разработка раздела технического проекта на объект информатизации в части защиты информации;
- строительно-монтажные работы в соответствии с проектной документацией, утвержденной заказчиком, размещением и монтажом технических средств и систем;
- разработка организационно-технических мероприятий по защите информации в соответствии с предъявляемыми требованиями;
- закупка сертифицированных образцов и серийно выпускаемых в защищенном исполнении технических средств обработки, передачи и хранения информации либо их сертификация;
- закупка сертифицированных технических, программных и программно-технических средств защиты информации и их установка;
- разработка (доработка) или закупка и последующая сертификация по требованиям безопасности информации программных средств защиты информации в случае, когда на рынке отсутствуют требуемые сертифицированные программные средства;
- организация охраны и физической защиты помещений объекта информатизации, исключающих несанкционированный доступ к техническим средствам обработки, хранения и передачи информации, их хищение и нарушение работоспособности, хищение носителей информации;
- разработка и реализация разрешительной системы доступа пользователей и эксплуатационного персонала к обрабатываемой (обсуждаемой) на объекте информатизации информации;
- определение заказчиком подразделений и лиц, ответственных за эксплуатацию средств защиты информации, обучение назначенных лиц специфике работ по защите информации на стадии эксплуатации объекта информатизации;
- выполнение генерации пакета прикладных программ в комплексе с программными средствами защиты информации;
- разработка эксплуатационной документации на объект информатизации и средства защиты информации, а также организационно-распорядительной документации по защите информации {приказов, инструкций и других документов);
- выполнение других мероприятий, специфичных для конкретных объектов информатизации и направлений защиты информации.

3.17. Задание на проектирование оформляется отдельным документом, согласовывается с проектной организацией, службой (специалистом) безопасности предприятия-заказчика в части достаточности мер по технической защите информации и утверждается заказчиком.

Мероприятия по защите информации от утечки по техническим каналам являются основным элементом проектных решений, закладываемых в соответствующие разделы проекта, и разрабатываются одновременно с ними.

3.18. На: стадии проектирования и создания объекта информатизации оформляются также технический (технорабочий) проект и эксплуатационная документация СЗИ, состоящие из:

- пояснительной записки с изложением решений по комплексу организационных мер и программно-техническим средствам обеспечения безопасности информации, составу средств защиты информации с указанием их соответствия требованиям ТЗ;

- описания технического, программного, информационного обеспечения и технологии обработки (передачи) информации;
- плана организационно-технических мероприятий по подготовке объекта информатизации к внедрению средств и мер защиты информации;
- технического паспорта объекта информатизации (форма технического паспорта на АС приведена в приложении № 5);
- инструкций и руководств по эксплуатации технических и программных средств защиты для пользователей, администраторов системы, а также для работников службы защиты информации.

3.19. На стадии ввода в действие объекта информатизации и СЗИ осуществляются:

- опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе объекта информатизации и отработки технологического процесса обработки (передачи) информации;
- приемо-сдаточные испытания средств защиты информации по результатам опытной эксплуатации с оформлением приемо-сдаточного акта, подписываемого разработчиком (поставщиком) и заказчиком;
- аттестация объекта информатизации по требованиям безопасности информации.

3.20. На этой стадии оформляются:

- акты внедрения средств защиты информации по результатам их приемо-сдаточных испытаний;
- предъявительский акт к проведению аттестационных испытаний;
- заключение по результатам аттестационных испытаний.

При положительных результатах аттестации на объект информатизации оформляется «Аттестат соответствия требованиям по безопасности информации» (форма «Аттестата соответствия» для АС приведена в приложении № 2, для ЗП - в приложении № 3).

3.21. Кроме вышеуказанной документации в учреждении (на предприятии) оформляются приказы, указания и решения:

- о проектировании объекта информатизации и назначении ответственных исполнителей;
- о формировании группы обследования и назначении ее руководителя;
- о заключении соответствующих договоров на проведение работ;
- о назначении лиц, ответственных за эксплуатацию объекта информатизации;
- о разрешении обработки в АС (обсуждения в ЗП) конфиденциальной информации.

3.22. Для объектов информатизации, находящихся в эксплуатации до введения в действие настоящего документа, может быть предусмотрен, по решению их заказчика (владельца), упрощенный вариант их доработки (модернизации), переоформления организационно-распорядительной, технологической и эксплуатационной документации.

Программа аттестационных испытаний такого рода объектов информатизации определяется аттестационной комиссией.

Необходимым условием является их соответствие действующим требованиям по защите информации.

3.23. Эксплуатация объекта информатизации осуществляется в полном соответствии с утвержденной организационно-распорядительной и эксплуатационной документацией, с учетом требований и положений, изложенных в разделах 4-6 настоящего документа.

3.24. С целью своевременного выявления и предотвращения утечки информации по техническим каналам, исключения или существенного затруднения несанкционированного доступа и предотвращения специальных программно-технических воздействий, вызывающих нарушение целостности информации или работоспособности технических средств, в учреждении (на предприятии) проводится периодический (не реже одного раза в год) контроль состояния защиты информации.

Контроль осуществляется службой безопасности учреждения (предприятия), а также отраслевыми и федеральными органами контроля (для информации, режим защиты которой определяет государство) и заключается в оценке:

- соблюдения нормативных и методических документов Гостехкомиссии России;
- работоспособности применяемых средств защиты информации в соответствии с их эксплуатационной документацией;
- знаний и выполнения персоналом своих функциональных обязанностей в части защиты информации.

3.25. Собственник или владелец конфиденциальной информации имеет право обратиться в органы государственной власти для оценки правильности выполнения норм и требований по защите его информации в информационных системах.

3.26. При необходимости по решению руководителя предприятия могут быть организованы работы по поиску электронных устройств съема информации («закладочных устройств»), возможно внедренных в ЗП или технические средства, осуществляемые организациями, имеющими соответствующие лицензии ФАПСИ или ФСБ России на конкретный вид деятельности по поиску «таких устройств». В организациях Минобороны России работы по поиску электронных устройств съема информации («закладочных устройств»), возможно внедренных в ЗП или технические средства, могут проводиться организациями, допущенными к проведению этих работ в установленном порядке.

4. Требования и рекомендации по защите речевой информации

4.1. Общие положения

4.1.1. Требования и рекомендации настоящего раздела направлены на исключение (существенное затруднение) возможности перехвата конфиденциальной речевой информации, циркулирующей в ЗП, в системах звукоусиления (СЗУ) и звукового сопровождения кинофильмов (СЗСК), при осуществлении её магнитной звукозаписи и передачи по каналам связи.

4.1.2. Требования настоящего раздела, если не оговорено специально, являются обязательными на всех стадиях проектирования, строительства, оснащения, эксплуатации ЗП и размещенных в них ОТСС и ВТСС, для систем СЗУ и СЗСК.

4.1.3. При проведении мероприятий с использованием конфиденциальной речевой информации и технических средств ее обработки возможна утечка информации за счет:

- акустического излучения информативного речевого сигнала;
- виброакустических сигналов, возникающих посредством преобразования информативного акустического сигнала при воздействии его на строительные конструкции и инженерно-технические системы ЗП;
- прослушивания разговоров, ведущихся в ЗП, по информационным каналам общего пользования (городская телефонная сеть, сотовая, транкинговая и пейджинговая связь, радиотелефоны) за счет скрытного подключения оконечных устройств этих видов связи;
- электрических сигналов, возникающих в результате преобразования информативного сигнала из акустического в электрический за счет микрофонного эффекта и распространяющихся по проводам и линиям передачи информации, выходящие за пределы КЗ;
- побочных электромагнитных излучений информативного сигнала от обрабатывающих конфиденциальную информацию технических средств, в том числе возникающих за счет паразитной генерации, и линий передачи информации;
- электрических сигналов, наводимых от обрабатывающих конфиденциальную информацию технических средств и линий ее передачи, на провода и линии, выходящих за пределы КЗ;
- радиоизлучений, модулированных информативным сигналом, возникающих при работе различных генераторов, входящих в состав технических средств, установленных в ЗП, или при наличии паразитной генерации в их узлах (элементах);
- радиоизлучений, электрических или инфракрасных сигналов, модулированных информативным сигналом от специальных электронных устройств съема речевой информации («за-

кладочных устройств»), закладываемых в ЗП, в технические средства и системы обработки информации.

Также следует учитывать возможность хищения технических средств с хранящейся в них информацией или отдельных носителей информации.

4.2. Основные требования и рекомендации по защите информации, циркулирующей в защищаемых помещениях

4.2.1. В учреждении (предприятии) должен быть документально определен перечень ЗП и лиц, ответственных за их эксплуатацию в соответствии с установленными требованиями по защите информации, а также составлен технический паспорт на ЗП (форма технического паспорта приведена в приложении № 4).

4.2.2. Защищаемые помещения должны размещаться в пределах контролируемой территории учреждения (предприятия). При этом рекомендуется размещать их на максимальном удалении от границ контролируемой зоны, ограждающие конструкции (стены, полы, потолки) не должны являться смежными с помещениями других учреждений (предприятий). Не рекомендуется располагать ЗП на первых этажах зданий.

Для исключения просмотра текстовой и графической конфиденциальной информации через окна помещения рекомендуется оборудовать их шторами (жалюзи).

4.2.3. Защищаемые помещения рекомендуется оснащать сертифицированными по требованиям безопасности информации ОТСС и ВТСС, либо средствами, прошедшими специальные исследования и имеющими предписание на эксплуатацию.

Эксплуатация ОТСС, ВТСС должна осуществляться в соответствии с предписаниями и эксплуатационной документацией на них.

4.2.4. Специальная проверка ЗП и установленного в нем оборудования с целью выявления возможно внедренных в них электронных устройств съема информации («закладочных устройств») проводится при необходимости по решению руководителя предприятия.

4.2.5. Во время проведения конфиденциальных мероприятий запрещается использование в ЗП радиотелефонов, оконечных устройств сотовой, пейджинговой и транкинговой связи, переносных магнитофонов и других средств аудио- и видеозаписи. При установке в ЗП телефонных и факсимильных аппаратов с автоответчиком или спикерфоном, а также аппаратов с автоматическим определителем номера, следует отключать их из сети на время проведения этих мероприятий.

4.2.6. Для исключения возможности утечки информации за счет электроакустического преобразования рекомендуется использовать в ЗП в качестве оконечных устройств телефонной связи, имеющих прямой выход в городскую АТС, телефонные аппараты (ТА), прошедшие специальные исследования, либо оборудовать их сертифицированными средствами защиты информации от утечки за счет электроакустического преобразования.

4.2.7. Для исключения возможности скрытного подключения ТА и прослушивания ведущихся в ЗП разговоров не рекомендуется устанавливать в них цифровые ТА цифровых АТС, имеющих выход в городскую АТС или к которой подключены абоненты, не являющиеся сотрудниками учреждения (предприятия).

В случае необходимости рекомендуется использовать сертифицированные по требованиям безопасности информации цифровые АТС либо устанавливать в эти ЗП аналоговые аппараты или цифровые ТА с вмонтированными в них сертифицированными средствами защиты.

4.2.8. Ввод системы городского радиотрансляционного вещания на территорию учреждения (предприятия) рекомендуется осуществлять через радиотрансляционный узел (буферный усилитель), размещаемый в пределах контролируемой зоны.

При вводе системы городского радиовещания без буферного усилителя, в ЗП следует использовать абонентские громкоговорители в защищенном от утечки информации исполнении, а также трех программные абонентские громкоговорители в режиме приема 2-й и 3-й программы (с усилителем).

В случае использования однопрограммного или трех программно абонентского громкоговорителя в режиме приема первой программы (без усиления) необходимо их отключать на период проведения конфиденциальных мероприятий.

4.2.9. В случае размещения электрочасовой станции внутри КЗ использование в ЗП электро вторичных часов (ЭВЧ) возможно без средств защиты информации.

При установке электрочасовой станции вне КЗ в линии ЭВЧ, имеющие выход за пределы КЗ, рекомендуется устанавливать сертифицированные средства защиты информации.

4.2.10. Системы пожарной и охранной сигнализации ЗП должны строиться только по проводной схеме сбора информации (связи с пультом) и, как правило, размещаться в пределах одной с ЗП контролируемой зоне.

В качестве оконечных устройств пожарной и охранной сигнализации в ЗП рекомендуется использовать изделия, сертифицированные по требованиям безопасности информации, или образцы средств, прошедшие специальные исследования и имеющие предписание на эксплуатацию.

4.2.11. Звукоизоляция ограждающих конструкций ЗП, их систем вентиляции и кондиционирования должна обеспечивать отсутствие возможности прослушивания ведущихся в нем разговоров из-за пределов ЗП.

Проверка достаточности звукоизоляции осуществляется аттестационной комиссией путем подтверждения отсутствия возможности разборчивого прослушивания вне ЗП разговоров, ведущихся в нем.

При этом уровень тестового речевого сигнала должен быть не ниже используемого во время штатного режима эксплуатации помещения.

Для обеспечения необходимого уровня звукоизоляции помещений рекомендуется оборудование дверных проемов тамбурами с двойными дверями, установка дополнительных рам в оконных проемах, уплотнительных прокладок в дверных и оконных притворах и применение шумопоглотителей на выходах вентиляционных каналов.

Если предложенными выше методами не удастся обеспечить необходимую акустическую защиту, следует применять организационно-режимные меры, ограничивая на период проведения конфиденциальных мероприятий доступ посторонних лиц в места возможного прослушивания разговоров, ведущихся в ЗП.

4.2.12. Для снижения вероятности перехвата информации по виброакустическому каналу следует организационно-режимными мерами исключить возможность установки посторонних (внештатных) предметов на внешней стороне ограждающих конструкций ЗП и выходящих из них инженерных коммуникаций (систем отопления, вентиляции, кондиционирования).

Для снижения уровня виброакустического сигнала рекомендуется расположенные в ЗП элементы инженерно-технических систем отопления, вентиляции оборудовать звукоизолирующими экранами.

4.2.13. В случае, если указанные выше меры защиты информации от утечки по акустическому и виброакустическому каналам недостаточны или нецелесообразны, рекомендуется применять метод активного акустического или виброакустического маскирующего зашумления.

Для этой цели должны применяться сертифицированные средства активной защиты.

4.2.14. При эксплуатации ЗП необходимо предусматривать организационно-режимные меры, направленные на исключение несанкционированного доступа в помещение:

- двери ЗП в период между мероприятиями, а также в нерабочее время необходимо запираться на ключ;
- выдача ключей от ЗП должна производиться лицам, работающим в нем или ответственным за это помещение;
- установка и замена оборудования, мебели, ремонт ЗП должны производиться только по согласованию и под контролем подразделения (специалиста) по защите информации учреждения (предприятия).

4.3. Защита информации, циркулирующей в системах звукоусиления и звукового сопровождения кинофильмов

4.3.1. В качестве оборудования систем звукоусиления, предназначенных для обслуживания проводимых в ЗП закрытых мероприятий, и систем звукового сопровождения кинофильмов, содержащих конфиденциальные сведения, необходимо использовать оборудование, удовлетворяющее требованиям стандартов по электромагнитной совместимости России, Европейских стран, США (например, ГОСТ 22505-97). В случае необходимости для повышения уровня защищенности рекомендуется применять оборудование, сертифицированное по требованиям безопасности информации или прошедшее специальные исследования и имеющее предписание на эксплуатацию.

4.3.2. Системы звукоусиления Должны выполняться по проводной схеме передачи информации экранированными проводами и располагаться в пределах КЗ.

С целью уменьшения побочных электромагнитных излучений целесообразно использовать систему звукоусиления с рассредоточенной системой звукоизлучателей, т.е. следует отдавать предпочтение системам с большим количеством оконечных устройств малой мощности перед системами с малым количеством оконечных устройств большой мощности.

В качестве оконечных устройств рекомендуется использовать звуковые колонки, выпускаемые в защищенном исполнении.

Можно использовать выпускаемые в обычном исполнении громкоговорители с экранированными магнитными цепями (например: 0.5ГДШ-5, 0.5ГД-54, 1ГДШ-2, 1ГДШ-6, 1ГДШ-28, 2ГДШ-3, 2ГДШ-4, 3ГДШ-1) или укомплектованные ими звуковые колонки (например: 2КЗ-7, 6КЗ-8, 12КЗ-18).

В этом случае звуковые колонки (громкоговорители) следует заэкранировать по электрическому полю с помощью металлической сетки с ячейкой не более 1 мм^2 , заземляемой через экранирующую оплетку подводящего кабеля.

4.3.3. В системах звукоусиления рекомендуется применять аппаратуру с симметричными входными и выходными цепями. В случае использования аппаратуры с несимметричным выходом линии оконечных устройств следует подключать к оконечным усилителям через симметрирующие трансформаторы, устанавливаемые в непосредственной близости от оконечных усилителей.

4.3.4. В качестве усилительного оборудования рекомендуется использовать усилители в металлических экранах с возможностью их заземления.

4.3.5. Коммутационное и распределительное оборудование (распределительные, входные и выходные щитки подключения) следует размещать в металлических шкафах (коробках). На корпусах шкафов (коробок) необходимо предусмотреть клеммы (винты) для их заземления и приспособления для опечатывания.

4.3.6. Усилительное и оконечное оборудование СЗУ, СЗСК следует размещать на возможно большем расстоянии относительно границы контролируемой зоны.

4.3.7. Система электропитания и заземления должна соответствовать требованиям «Правил устройства электроустановок (ПУЭ)».

Рекомендуется электропитание и заземление аппаратуры СЗУ и СЗСК осуществлять от подстанции и на заземлитель, расположенные в пределах КЗ.

4.4. Защита информации при проведении звукозаписи

4.4.1. Запись и воспроизведение конфиденциальной речевой информации аппаратурой звукозаписи разрешается производить только в ЗП.

4.4.2. Для записи (воспроизведения) конфиденциальной информации должны применяться магнитофоны (диктофоны), удовлетворяющие требованиям стандартов по электромагнитной совместимости России, Европейских стран, США (например, ГОСТ 22505-97). Для повышения уровня защищенности информации рекомендуется использовать магнитофоны (диктофоны), сертифицированные по требованиям безопасности информации или прошедшие специальные исследования и имеющие предписание на эксплуатацию.

4.4.3. Носители информации (магнитные ленты, кассеты) должны учитываться и храниться в подразделениях учреждения (предприятия) в порядке, установленном для конфиденциальной информации.

В учреждении (предприятии) должно быть назначено должностное лицо, ответственное за хранение и использование аппаратуры звукозаписи конфиденциальной информации, и обеспечено хранение и использование этой аппаратуры, исключающее несанкционированный доступ к ней.

4.5. Защита речевой информации при её передаче по каналам связи.

Передача конфиденциальной речевой информации по открытым проводным каналам связи, выходящим за пределы КЗ, и радиоканалам должна быть исключена.

При необходимости передачи конфиденциальной информации следует использовать защищенные линии связи (например, защищенные волоконно-оптические), устройства скремблирования или криптографической защиты.

Используемые средства защиты информации должны быть сертифицированы по требованиям безопасности информации.

5. Требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники

5.1. Общие требования и рекомендации

5.1.1. Система (подсистема) защиты информации, обрабатываемой в автоматизированных системах различного уровня и назначения, должна предусматривать комплекс организационных, программных, технических и, при необходимости, криптографических средств и мер по защите информации при ее автоматизированной обработке и хранении, при ее передаче по каналам связи.

Основными направлениями защиты информации являются:

обеспечение защиты информации от хищения, утраты, утечки, уничтожения, искажения и подделки за счет НСД и специальных воздействий;

обеспечение защиты информации от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи.

5.1.3. В качестве основных мер защиты информации рекомендуется:

- документальное оформление перечня сведений конфиденциального характера с учетом ведомственной и отраслевой специфики этих сведений;
- реализация разрешительной системы допуска исполнителей (пользователей, обслуживающего персонала) к информации и связанным с ее использованием работам, документам;
- ограничение доступа персонала и посторонних лиц в защищаемые помещения и помещения, где размещены средства информатизации и коммуникации, а также хранятся носители информации; разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;
- регистрация действий пользователей АС и обслуживающего персонала, контроль за несанкционированным доступом и действиями пользователей, обслуживающего персонала и посторонних лиц; учет и надежное хранение бумажных и машинных носителей информации, ключей (ключевой документации) и их обращение, исключающее их хищение, подмену и уничтожение; использование СЗЗ, создаваемых на основе физико-химических технологий для контроля доступа к объектам защиты и для защиты документов от подделки;
- необходимое резервирование технических средств и дублирование массивов и носителей информации; использование сертифицированных серийно выпускаемых в защищенном исполнении технических средств обработки, передачи и хранения информации;
- использование технических средств, удовлетворяющих требованиям стандартов по электромагнитной совместимости;
- использование сертифицированных средств защиты информации;
- размещение объектов защиты на максимально возможном расстоянии относительно границы КЗ; размещение понижающих трансформаторных подстанций электропитания и контуров заземления объектов защиты в пределах КЗ; развязка цепей электропитания объектов защиты с помощью защитных фильтров, блокирующих (подавляющих) информативный сигнал;

электромагнитная развязка между линиями связи и другими цепями ВТСС, выходящими за пределы КЗ, и информационными цепями, по которым циркулирует защищаемая информация;

- использование защищенных каналов связи;
- размещение дисплеев и других средств отображения информации, исключающее несанкционированный просмотр информации;
- организация физической защиты помещений и собственно технических средств с помощью сил охраны и технических средств, предотвращающих или существенно затрудняющих проникновение в здания, помещения посторонних лиц, хищение документов и информационных носителей, самих средств информатизации, исключающих нахождение внутри контролируемой зоны технических средств разведки или промышленного шпионажа;
- предотвращение внедрения в автоматизированные системы программ-вирусов, программных закладок.

Обязательность тех или иных мер для защиты различных видов конфиденциальной информации конкретизирована в последующих подразделах документа.

5.1.4. В целях дифференцированного подхода к защите информации, обрабатываемой в АС различного уровня и назначения, осуществляемого в целях разработки и применения необходимых и достаточных мер и средств защиты информации, проводится классификация автоматизированных систем (форма акта классификации АС приведена в приложении № 1).

5.1.5. Классифицируются АС любого уровня и назначения. Классификация АС осуществляется на основании требований РД Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» и настоящего раздела документа.

5.1.6. Классификации подлежат действующие, но ранее не классифицированные, а также разрабатываемые АС, предназначенные для обработки конфиденциальной информации.

5.1.7. Если АС, классифицированная ранее, включается в состав вычислительной сети или системы и соединяется с другими техническими средствами линиями связи различной физической природы, образуемая при этом АС более высокого уровня классифицируется в целом, а в отношении АС нижнего уровня классификация не производится.

Если объединяются АС различных классов защищенности, то интегрированная АС должна классифицироваться по высшему классу защищенности входящих в нее АС, за исключением случаев их объединения посредством межсетевого экрана, когда каждая из объединяющихся АС может сохранять свой класс защищенности. Требования к используемым при этом межсетевым экранам изложены в подразделе 5.9.

5.1.8. При рассмотрении и определении режима обработки данных в АС учитывается, что индивидуальным (монопольным) режимом обработки считается режим, при котором ко всей обрабатываемой информации, к программным средствам и носителям информации этой системы допущен только один пользователь.

Режим, при котором различные пользователи, в том числе обслуживающий персонал и программисты, работают в одной АС, рассматривается как коллективный. Коллективным режимом работы считается также и последовательный во времени режим работы различных пользователей и обслуживающего персонала.

5.1.9. В случае, когда признаки классифицируемой АС (п. 1.7. РД Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации») не совпадают с предложенными в РД (п.1.9.) группами по особенностям обработки информации в АС, то при классификации выбирается наиболее близкая группа защищенности с предъявлением к АС соответствующих дополнительных требований по защите информации. (Например, однопользовательская АС с информацией различного уровня конфиденциальности по формальным признакам не может быть отнесена к 3 группе защищенности. Однако, если дополнительно реализовать в такой системе управление потоками информации, то необходимый уровень защиты будет обеспечен).

5.1.10. Конкретные требования по защите информации и мероприятия по их выполнению определяются в зависимости от установленного для АС класса защищенности. Требования к классам защищенности определены в сборнике руководящих документов Гостехкомиссии России по защите информации от несанкционированного доступа:

1. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.

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

3. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации.

4. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации.

5. Защита информации. Специальные защитные знаки. Классификация и общие требования.

6. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники.

5.1.11. Лица, допущенные к автоматизированной обработке конфиденциальной информации, несут ответственность за соблюдение ими установленного в учреждении (на предприятии) порядка обеспечения защиты этой информации.

Для получения доступа к конфиденциальной информации они должны изучить требования настоящего документа, других нормативных документов по защите информации, действующих в учреждении (на предприятии) в части их касающейся.

5.2. Основные требования и рекомендации по защите служебной тайны и персональных данных.

При разработке и эксплуатации АС, предполагающих использование информации, составляющей служебную тайну, а также персональных данных должны выполняться следующие основные требования:

5.2.1. Организация, состав и содержание проводимых работ по защите информации, организационно-распорядительной, проектной и эксплуатационной документации должны отвечать требованиям раздела 3.

5.2.2. В учреждении (на предприятии) должны быть документально оформлены перечни сведений, составляющих служебную тайну, и персональных данных, подлежащих защите. Эти перечни могут носить как обобщающий характер в области деятельности учреждения (предприятия), так и иметь отношение к какому-либо отдельному направлению работ. Все исполнители должны быть ознакомлены с этими перечнями в части их касающейся.

5.2.3. В соответствии с РД Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» устанавливается следующий порядок классификации АС в зависимости от вида сведений конфиденциального характера:

- АС, обрабатывающие информацию, составляющую служебную тайну, должны быть отнесены по уровню защищенности к классам ЗБ, 2Б и не ниже 1Г;

- АС, обрабатывающие персональные данные, должны быть отнесены по уровню защищенности к классам ЗБ, 2Б и не ниже 1Д.

5.2.4. Для обработки информации, составляющей служебную тайну, а также для обработки персональных данных следует использовать СВТ, удовлетворяющие требованиям стандартов Российской Федерации по электромагнитной совместимости, по безопасности и эргономическим требованиям к средствам отображения информации, по санитарным нормам, предъявляемым к видеодисплейным терминалам ПЭВМ (например, ГОСТ 29216-91, ГОСТ Р 50948-96, ГОСТ Р 50949-96, ГОСТ Р 50923-96, СанПиН 2.2.2.542-96).

Для повышения уровня защищенности информации рекомендуется использовать сертифицированные по требованиям безопасности информации СВТ.

5.2.5. Для передачи информации по каналам связи, выходящим за пределы КЗ, необходимо использовать защищенные каналы связи, в том числе защищенные волоконно-оптические линии связи или предназначенные для этого криптографические средства защиты информации. Применяемые средства защиты информации должны быть сертифицированы.

Носители информации на магнитной (магнитооптической) и бумажной основе должны учитываться, храниться и уничтожаться в подразделениях учреждений (предприятий) в порядке, установленном для служебной информации ограниченного распространения, с пометкой «Для служебного пользования».

Доступ к информации исполнителей (пользователей, обслуживающего персонала) осуществляется в соответствии с разрешительной системой допуска исполнителей к документам и сведениям конфиденциального характера, действующей в учреждении (на предприятии).

При необходимости указанный минимальный набор рекомендуемых организационно-технических мер защиты информации по решению руководителя предприятия может быть расширен.

5.3. Основные рекомендации по защите информации, составляющей коммерческую тайну.

При разработке и эксплуатации АС, предполагающих использование сведений, составляющих коммерческую тайну, рекомендуется выполнение следующих основных организационно-технических мероприятий:

5.3.1. На предприятии следует документально оформить «Перечень сведений, составляющих коммерческую тайну». Все исполнители должны быть ознакомлены с этим «Перечнем».

5.3.2. При организации разработки и эксплуатации АС с использованием таких сведений следует ориентироваться на порядок, приведенный в разделе 3. Оформить порядок разработки и эксплуатации таких АС документально.

5.3.3. Рекомендуется относить АС, обрабатывающие информацию, составляющую коммерческую тайну, режим защиты которой определяет ее собственник, по уровню защищенности к классам ЗБ, 2Б и не ниже 1Д (если по решению руководителя предприятия не предъявляются более высокие требования).

5.3.4. Рекомендуется для обработки информации, составляющей коммерческую тайну, использовать средства вычислительной техники, удовлетворяющие требованиям стандартов Российской Федерации по электромагнитной совместимости, по безопасности и эргономическим требованиям к средствам отображения информации, по санитарным нормам, предъявляемым к видеодисплейным терминалам ПЭВМ (например, ГОСТ 29216-91, ГОСТ Р 50948-96, ГОСТ Р 50949-96, ГОСТ Р 50923-96, СанПиН 2.2.2.542-96). Для повышения уровня защищенности информации рекомендуется использовать сертифицированные по требованиям безопасности информации СВТ.

5.3.5. Для передачи информации по каналам связи, выходящим за пределы контролируемой зоны, необходимо использовать защищенные каналы связи, в том числе защищенные волоконно-оптические линии связи или предназначенные для этого криптографические средства защиты информации.

Следует установить на предприятии порядок учета, хранения и уничтожения носителей информации на магнитной (магнитооптической) и бумажной основе в научных, производственных и функциональных подразделениях, а также разработать и ввести в действие разрешительную систему допуска исполнителей к документам и сведениям, составляющим коммерческую тайну.

Указанный минимальный набор рекомендуемых организационно-технических мероприятий по решению руководителя предприятия может быть расширен.

Решение о составе и содержании мероприятий, а также используемых средств защиты информации принимается руководителем предприятия по результатам обследования создаваемой (модернизируемой) АС с учетом важности (ценности) защищаемой информации.

5.4. Порядок обеспечения защиты конфиденциальной информации при эксплуатации АС

5.4.1. Организация эксплуатации АС и СЗИ в ее составе осуществляется в соответствии с установленным в учреждении (на предприятии) порядком, в том числе технологическими инструкциями по эксплуатации СЗИ НСД для пользователей, администраторов АС и работников службы безопасности.

5.4.2. Для обеспечения защиты информации в процессе эксплуатации АС рекомендуется предусматривать соблюдение следующих основных положений и требований:

- допуск к защищаемой информации лиц, работающих в АС (пользователей, обслуживающего персонала), должен производиться в соответствии с установленным разрешительной системой допуска порядком;
- на период обработки защищаемой информации в помещениях, где размещаются ОТСС, могут находиться только лица, допущенные в установленном порядке к обрабатываемой информации, допуск других лиц для проведения необходимых профилактических или ремонтных работ может осуществляться в эти помещения только с разрешения руководителя учреждения (предприятия) или руководителя службы безопасности;
- в случае размещения в одном помещении нескольких технических средств отображения информации должен быть исключен несанкционированный просмотр выводимой на них информации;
- по окончании обработки защищаемой информации или при передаче управления другому лицу, пользователь обязан произвести стирание временных файлов на несъёмных носителях информации и информации в оперативной памяти. Одним из способов стирания информации в оперативной памяти является перезагрузка ПЭВМ;
- изменение или ввод новых программ обработки защищаемой информации в АС должен осуществляться совместно разработчиком АС и администратором АС;
- при увольнении или перемещении администраторов АС руководителем учреждения (предприятия) по согласованию со службой безопасности должны быть приняты меры по оперативному изменению паролей и идентификаторов.

5.4.3. Все носители информации на бумажной, магнитной, оптической (магнитооптической) основе, используемые в технологическом процессе обработки информации в АС, подлежат учету в том производственном, научном или функциональном подразделении, которое является владельцем АС, обрабатывающей эту информацию.

5.4.5. Учет съёмных носителей информации на магнитной или оптической основе (гибкие магнитные диски, съёмные накопители информации большой емкости или картриджи, съёмные пакеты дисков, иные магнитные, оптические или магнитооптические диски, магнитные ленты и т.п.), а также распечаток текстовой, графической и иной информации на бумажной или пластиковой (прозрачной) основе осуществляется по карточкам или журналам установленной формы, в том числе автоматизировано с использованием средств вычислительной техники. Журнальная форма учета может использоваться в АС с небольшим объемом документооборота

5.4.5. Съёмные носители информации на магнитной или оптической основе, в зависимости от характера или длительности использования, допускается учитывать совместно с другими документами по установленным для этого учетным формам.

При этом перед выполнением работ сотрудником, ответственным за их учет, на этих носителях информации предварительно проставляются любым доступным способом следующие учетные реквизиты: учетный номер и дата, пометка «Для служебного пользования», номер экземпляра, подпись этого сотрудника, а также другие возможные реквизиты, идентифицирующие этот носитель.

5.4.6. Распечатки допускается учитывать совместно с другими традиционными печатными документами по установленным для этого учетным формам.

Временно не используемые носители информации должны храниться пользователем в местах, недоступных для посторонних лиц.

5.5. Защита конфиденциальной информации на автоматизированных рабочих местах на базе автономных ПЭВМ

5.5.1. Автоматизированные рабочие места на базе автономных ПЭВМ являются автоматизированными системами, обладающими всеми основными признаками АС. Информационным каналом обмена между такими АС являются носители информации на магнитной (магнитооптической) и бумажной основе.

В связи с этим порядок разработки и эксплуатации АРМ на базе автономных ПЭВМ по составу и содержанию проводимых работ по защите информации, организационно-распорядительной, проектной и эксплуатационной документации должны полностью отвечать требованиям настоящего документа.

5.5.2. АС на базе автономных ПЭВМ в соответствии с требованиями РД Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» должны быть классифицированы и отнесены:

- к 3 группе АС, если в ней работает только один пользователь, допущенный ко всей информации АС;
- ко 2 и 1 группе АС, если в ней последовательно работают несколько пользователей с равными или разными правами доступа (полномочиями), соответственно.

Примечание: При использовании на автономной ПЭВМ технологии обработки информации на съемных накопителях большой емкости классификация АС производится на основании анализа режима доступа пользователей АС к информации на используемом съемном носителе (либо одновременно используемом их комплексе).

5.6. Защита информации при использовании съемных накопителей информации большой емкости для автоматизированных рабочих мест на базе автономных ПЭВМ

5.6.1. Данная информационная технология предусматривает запись на загружаемый съемный накопитель информации большой емкости одновременно общесистемного (ОС, СУБД) и прикладного программного обеспечения, а также обрабатываемой информации одного или группы пользователей.

В качестве устройств для работы по этой технологии могут быть использованы накопители на магнитном, магнитооптическом или лазерном дисках различной конструкции, как встроенные (съемные), так и выносные. Одновременно может быть установлено несколько съемных накопителей информации большой емкости.

Несъемные накопители должны быть исключены из конфигурации ПЭВМ.

Основной особенностью применения данной информационной технологии для АРМ на базе автономных ПЭВМ, с точки зрения защиты информации, является исключение этапа хранения на ПЭВМ в нерабочее время информации, подлежащей защите.

Эта особенность может быть использована для обработки защищаемой информации без применения сертифицированных средств защиты информации от НСД и использования средств физической защиты помещений этих АРМ.

5.6.2. На этапе предпроектного обследования необходимо провести детальный анализ технологического процесса обработки информации, обращая внимание прежде всего на технологию обмена информацией (при использовании съемных накопителей информации большой емкости или гибких магнитных дисков (ГМД или дискет) с другими АРМ, как использующими, так и не использующими эту информационную технологию, на создание условий, исключающих попадание конфиденциальной информации на неучтенные носители информации, несанкционированное ознакомление с этой информацией, на организацию выдачи информации на печать.

5.6.3. Обмен конфиденциальной информацией между АРМ должен осуществляться только на учтенных носителях информации с учетом допуска исполнителей, работающих на АРМ, к переносимой информации.

5.6.4. На рабочих местах исполнителей, работающих по этой технологии, во время работы, как правило, не должно быть неучтенных накопителей информации.

В случае формирования конфиденциальных документов с использованием, как текстовой, так и графической информации, представленной на не конфиденциальных накопителях информации, не конфиденциальные накопители информации должны быть «закрыты на запись».

Условия и порядок применения таких процедур должны быть отражены в технологии обработки информации, использующей съемные накопители информации большой емкости.

5.6.5. При использовании в этой технологии современных средств вычислительной техники, оснащенных энергонезависимой, управляемой извне перезаписываемой памятью, так называемых Flash-Bios (FB), необходимо обеспечить целостность записанной в FB информации. Для обеспечения целостности как перед началом работ с конфиденциальной информацией при загрузке ПЭВМ, так и по их окончании, необходимо выполнить процедуру проверки целостности FB. При несовпадении, необходимо восстановить (записать первоначальную версию) FB, поставить об этом в известность руководителя подразделения и службу безопасности, а также выяснить причины изменения FB.

5.6.6. Должна быть разработана и, по согласованию со службой безопасности, утверждена руководителем учреждения (предприятия) технология обработки конфиденциальной информации, использующая съемные накопители информации большой емкости и предусматривающая вышеуказанные, а также другие вопросы защиты информации, имеющие отношение к условиям размещения, эксплуатации АРМ, учету носителей информации, а также другие требования, вытекающие из особенностей функционирования АРМ.

5.7. Защита информации в локальных вычислительных сетях

5.7.1. Характерными особенностями ЛВС являются: распределенное хранение файлов, удаленная обработка данных (вычисления) и передача сообщений (электронная почта), а также сложность проведения контроля за работой пользователей и состоянием общей безопасности ЛВС.

5.7.2. Средства защиты информации от НСД должны использоваться во всех узлах ЛВС, независимо от наличия (отсутствия) конфиденциальной информации в данном узле ЛВС, и требуют постоянного квалифицированного контроля со стороны администратора безопасности информации.

5.7.3. Информация, составляющая служебную тайну, и персональные данные могут обрабатываться только в изолированных ЛВС, расположенных в пределах контролируемой зоны, или в условиях, изложенных в пунктах 5.8.4. и 5.8.5. следующего подраздела.

5.7.4. Класс защищенности ЛВС определяется в соответствии с требованиями РД Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».

Для управления ЛВС и распределения системных ресурсов в ЛВС, включая управление средствами защиты информации, обрабатываемой (хранимой, передаваемой) в ЛВС, в дополнение к системным администраторам (администраторам ЛВС) могут быть назначены администраторы по безопасности информации, имеющие необходимые привилегии доступа к защищаемой информации ЛВС.

Состав пользователей ЛВС должен устанавливаться по письменному разрешению руководства предприятия (структурного подразделения) и строго контролироваться. Все изменения состава пользователей, их прав и привилегий должны регистрироваться.

Каждый администратор и пользователь должен иметь уникальные идентификаторы и пароли.

5.8. Защита информации при межсетевом взаимодействии

5.8.1. Положения данного подраздела относятся к взаимодействию локальных сетей, ни одна из которых не имеет выхода в сети общего пользования типа Internet.

5.8.2. Взаимодействие ЛВС с другими вычислительными сетями должно контролироваться с точки зрения защиты информации. Коммуникационное оборудование и все соединения с локальными периферийными устройствами ЛВС должны располагаться в пределах КЗ.

При конфигурировании коммуникационного оборудования (маршрутизаторов, концентраторов, мостов и мультиплексоров) и прокладке кабельной системы ЛВС, рекомендуется учитывать разделение трафика по отдельным сетевым фрагментам на производственной основе и видам деятельности предприятия.

Подключение ЛВС к другой автоматизированной системе (локальной или неоднородной вычислительной сети) должно осуществляться с использованием МЭ, требования к которому определяются РД Гостехкомиссии России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации».

5.8.5. Для защиты АС при ее взаимодействии с другой АС по каналам связи необходимо использовать:

- в АС класса 1Г - МЭ не ниже класса 4;
- в АС класса 1Д и 2Б, 3Б - МЭ класса 5 или выше.

Для защиты конфиденциальной информации, передаваемой по каналам связи между АС, если каналы связи выходят за пределы КЗ, необходимо использовать защищенные каналы связи, включая защищенные волоконно-оптические линии связи или сертифицированные ФАПСи криптографические средства защиты.

5.9. Защита информации при работе с системами управления базами данных

5.9.1. При работе с системами управления базами данных (СУБД) и базами данных (БД) необходимо учитывать следующие особенности защиты информации от НСД:

- в БД может накапливаться большой объем интегрированной информации по различным тематическим направлениям, предназначенной для различных пользователей;
 - БД могут быть физически распределены по различным устройствам и узлам сети;
 - БД могут включать информацию различного уровня конфиденциальности;
- разграничение доступа пользователей к БД средствами операционной системы и/или СЗИ НСД может осуществляться только на уровне файлов БД;
- разграничение доступа пользователей к объектам БД. таблицам, схемам, процедурам, записям, полям записей в базах данных и т.п., может осуществляться только средствами СУБД, если таковые имеются;
 - регистрация действий пользователей при работе с объектами БД может осуществляться также только средствами СУБД, если таковые имеются;
 - СУБД могут обеспечивать одновременный доступ многих пользователей (клиентов) к БД с помощью сетевых протоколов, при этом запросы пользователя к БД обрабатываются на сервере и результаты обработки направляются пользователям (клиентам).

5.9.2. С учетом указанных особенностей при создании БД рекомендуется:

- при выборе СУБД ориентироваться на операционные системы и СУБД, включающие либо штатные сертифицированные средства защиты информации от НСД, либо имеющие соответствующие сертифицированные дополнения в виде СЗИ НСД;
- при использовании СУБД, не имеющих средств разграничения доступа, производить разбиение БД на отдельные файлы, разграничение доступа к которым можно проводить средствами ОС и/или СЗИ НСД;
- при использовании современных СУБД, основанных на модели клиент-сервер, использовать их штатные средства защиты информации от НСД, применять средства регистрации (аудита) и разграничение доступа к объектам БД на основе прав, привилегий, ролей, представлений (VIEW), процедур и т.п.

6. Рекомендации по обеспечению защиты информации, содержащейся в негосударственных информационных ресурсах, при взаимодействии абонентов с информационными сетями общего пользования

6.1. Общие положения

6.1.1. В настоящем разделе приведены рекомендации, определяющие условия и порядок подключения абонентов к информационным сетям общего пользования (Сетям), а также реко-

мендации по обеспечению безопасности конфиденциальной информации, содержащейся в негосударственных информационных ресурсах, режим защиты которой определяет собственник этих ресурсов (коммерческая тайна - в соответствии с п.2.3. СТР-К), при подключении и взаимодействии абонентов с этими сетями.

6.1.2. Данные рекомендации определены, исходя из требований РД «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», настоящего документа, а также следующих основных угроз безопасности информации, возникающих при взаимодействии с информационными сетями общего пользования:

- несанкционированного доступа к информации, хранящейся и обрабатываемой во внутренних ЛВС (серверах, рабочих станциях) или на автономных ПЭВМ, как из Сетей, так и из внутренних ЛВС;
- несанкционированного доступа к коммуникационному оборудованию (маршрутизатору, концентратору, мосту, мультиплексору, серверу, Web/Проху серверу), соединяющему внутренние ЛВС учреждения (предприятия) с Сетями;
- несанкционированного доступа к данным (сообщениям), передаваемым между внутренними ЛВС и Сетями, включая их модификацию, имитацию и уничтожение;
- заражения программного обеспечения компьютерными «вирусами» из Сети как посредством приема «зараженных» файлов, так и посредством E-mail, апплетов языка JAVA и объектов ActiveX Control;
- внедрения программных закладок с целью получения НСД к информации, а также дезорганизации работы внутренней ЛВС и ее взаимодействия с Сетями;
- несанкционированной передачи защищаемой конфиденциальной информации ЛВС в Сеть;
- возможности перехвата информации внутренней ЛВС за счет побочных электромагнитных излучений и наводок от основных технических средств, обрабатывающих такую информацию.

6.2. Условия подключения абонентов к Сети

6.2.1. Подключение к Сети абонентского пункта (АП) осуществляется по решению руководителя учреждения (предприятия) на основании соответствующего обоснования.

6.2.2. Обоснование необходимости подключения АП к Сети должно содержать:

- наименование Сети, к которой осуществляется подключение, и реквизиты организации-владельца Сети и провайдера Сети;
- состав технических средств для оборудования АП;
- предполагаемые виды работ и используемые прикладные сервисы Сети (E-Mail, FTP, Telnet, http и т.п.) для АП в целом и для каждого абонента в частности;
- режим подключения АП и абонентов к Сети (постоянный, в т.ч. круглосуточный, временный);
- состав общего и телекоммуникационного программного обеспечения АП и абонентов (ОС, клиентские прикладные программы для сети - Browsers и т.п.);
- число и перечень предполагаемых абонентов (диапазон используемых IP-адресов);
- меры и средства защиты информации от НСД, которые будут применяться на АП, организация-изготовитель, сведения о сертификации, установщик, конфигурация, правила работы с ними;
- перечень сведений конфиденциального характера, обрабатываемых (хранимых) на АП, подлежащих передаче и получаемых из Сети.

6.2.3. Право подключения к Сети АП, не оборудованного средствами защиты информации от НСД, может быть предоставлено только в случае обработки на АП информации с открытым доступом, оформленной в установленном порядке как разрешенной к открытому опубликованию. В этом случае к АП, представляющим собой автономную ПЭВМ с модемом, специальные требования по защите информации от НСД не предъявляются.

6.2.4. Подключение к Сети АП, представляющих собой внутренние (локальные) вычислительные сети, на которых обрабатывается информация, не разрешенная к открытому опубликованию, разрешается только после установки на АП средств защиты информации от НСД, отвечающих требованиям и рекомендациям, изложенным в подразделе 6.3.

6.3. Порядок подключения и взаимодействия абонентских пунктов с Сетью, требования и рекомендации по обеспечению безопасности информации

6.3.1. Подключение АП к Сети должно осуществляться в установленном порядке через провайдера Сети.

6.3.2. Подключение ЛВС предприятия (учреждения) к Сети должно осуществляться через средства разграничения доступа в виде МЭ (Firewall, Брандмауэр). Не допускается подключение ЛВС к Сети в обход МЭ. МЭ должны быть сертифицированы по требованиям безопасности информации.

6.3.3. Доступ к МЭ, к средствам его конфигурирования должен осуществляться только выделенным администратором с консоли. Средства удаленного управления МЭ должны быть исключены из конфигурации.

6.3.4. АП с помощью МЭ должен обеспечивать создание сеансов связи абонентов с внешними серверами Сети и получать с этих серверов только ответы на запросы абонентов. Настройка МЭ должна обеспечивать отказ в обслуживании любых внешних запросов, которые могут направляться на АП.

6.3.5. При использовании почтового сервера и Web-сервера предприятия последние не должны входить в состав ЛВС АП и должны подключаться к Сети по отдельному сетевому фрагменту (через маршрутизатор).

6.3.6. На технических средствах АП должно находиться программное обеспечение только в той конфигурации, которая необходима для выполнения работ, заявленных в обосновании необходимости подключения АП к Сети (обоснование может корректироваться в установленном на предприятии порядке).

Не допускается активизация не включенных в обоснование прикладных серверов (протоколов) и не требующих привязок протоколов к портам.

6.3.7. Установку программного обеспечения, обеспечивающего функционирование АП, должны выполнять уполномоченные специалисты под контролем администратора. Абоненты АП не имеют права производить самостоятельную установку и модификацию указанного программного обеспечения, однако, могут обращаться к администратору для проведения его экспертизы на предмет улучшения характеристик, наличия «вирусов», замаскированных возможностей выполнения непредусмотренных действий. Вся ответственность за использование не прошедшего экспертизу и не рекомендованного к использованию программного обеспечения целиком ложится на абонента АП. При обнаружении фактов такого рода администратор обязан логически (а при необходимости - физически вместе с включающей подсетью) отключить рабочее место абонента от Сети и ЛВС и поставить об этом в известность руководство.

6.3.8. Устанавливаемые межсетевые экраны должны соответствовать классу защищаемого АП (АС) и отвечать требованиям РД Гостехкомиссии России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации».

6.3.9. СЗИ НСД, устанавливаемая на автономную ПЭВМ, рабочие станции и серверы внутренней ЛВС предприятия при обработке на них конфиденциальной информации, должна осуществлять:

- идентификацию и аутентификацию пользователей при доступе к автономной ПЭВМ, рабочим станциям и серверам внутренней ЛВС по идентификатору и паролю;
- контроль доступа к ресурсам автономной ПЭВМ, рабочих станций и серверов внутренней ЛВС на основе дискреционного принципа;
- регистрацию доступа к ресурсам автономной ПЭВМ, рабочих станций и серверов внутренней ЛВС, включая попытки НСД;

- регистрацию фактов отправки и получения абонентом сообщений (файлов, писем, документов).

При этом СЗИ НСД должна запрещать запуск абонентом произвольных программ, не включенных в состав программного обеспечения АП.

Модификация конфигурации программного обеспечения АП должна быть доступна только со стороны администратора, ответственного за эксплуатацию АП.

Средства регистрации и регистрируемые данные должны быть недоступны для абонента. СЗИ НСД должна быть целостной, т.е. защищенной от несанкционированной модификации и не содержащей путей обхода механизмов контроля.

Тестирование всех функций СЗИ НСД с помощью специальных программных средств должно проводиться не реже одного раза в год.

6.3.10. Технические средства АП должны быть размещены либо в отдельном помещении (при автономной ПЭВМ, подключенной к Сети), либо в рабочих помещениях абонентов с принятием организационных и технических мер, исключающих несанкционированную работу в Сети. В этих помещениях должно быть исключено ведение конфиденциальных переговоров, либо технические средства должны быть защищены с точки зрения электроакустики. В нерабочее время помещение автономной ПЭВМ либо соответствующего сервера сдается под охрану в установленном порядке.

6.3.11. При создании АП рекомендуется:

6.3.11.1. По возможности размещать МЭ для связи с внешними Сетями, Web-серверы, почтовые серверы в отдельном ЗП, доступ в которое имел бы ограниченный круг лиц (ответственные специалисты, администраторы). Периодически проверять работоспособность МЭ с помощью сканеров, имитирующих внешние атаки на внутреннюю ЛВС. Не следует устанавливать на МЭ какие-либо другие прикладные сервисы (СУБД, E-mail, прикладные серверы и т.п.).

6.3.11.2. При предоставлении абонентам прикладных сервисов исходить из принципа минимальной достаточности. Тем пользователям АП, которым не требуются услуги Сети, не предоставлять их. Пользователям, которым необходима только электронная почта (E-mail), предоставлять только доступ к ней. Максимальный перечень предоставляемых прикладных сервисов ограничивать следующими: E-mail, FTP, HTTP, Telnet.

6.3.11.3. При создании АП следует использовать операционные системы со встроенными функциями защиты информации от НСД, перечисленными в п.6.3.9, или использовать сертифицированные СЗИ НСД.

6.3.11.4. Эффективно использовать имеющиеся в - маршрутизаторах средства разграничения доступа (фильтрацию), включающие контроль по списку доступа, аутентификацию пользователей, взаимную аутентификацию маршрутизаторов.

6.3.11.5. В целях контроля за правомерностью использования АП и выявления нарушений требований по защите информации осуществлять анализ принимаемой из Сети и передаваемой в Сеть информации, в том числе на наличие «вирусов». Копии исходящей электронной почты и отсылаемых в Сеть файлов следует направлять в адрес защищенного архива АП для последующего анализа со стороны администратора (службы безопасности).

6.3.11.6. Проводить постоянный контроль информации, помещаемой на Web-серверы предприятия. Для этого следует назначить ответственного (ответственных) за ведение информации на Web-сервере. Предусмотреть порядок размещения на Web-сервере информации, разрешенной к открытому опубликованию.

6.3.12. Приказом по учреждению (предприятию) назначаются лица (абоненты), допущенные к работам в Сети с соответствующими полномочиями, лица, ответственные за эксплуатацию указанного АП и контроль за выполнением мероприятий по обеспечению безопасности информации при работе абонентов в Сети (руководители подразделений и администраторы).

6.3.13. Вопросы обеспечения безопасности информации на АП должны быть отражены в инструкции, определяющей:

порядок подключения и регистрации абонентов в Сети;

- порядок установки и конфигурирования на АП общесистемного, прикладного коммуникационного программного обеспечения (серверов, маршрутизаторов, шлюзов, мостов, межсетевых экранов, Browsers), их новых версий;
- порядок применения средств защиты информации от НСД на АП при взаимодействии абонентов с Сетью;
- порядок работы абонентов в Сети, в том числе с электронной почтой (E-mail), порядок выбора и доступа к внутренним и внешним серверам Сети (Web-серверам);
- порядок оформления разрешений на отправку данных в Сеть (при необходимости);
- Обязанности и ответственность абонентов и администратора внутренней ЛВС по обеспечению безопасности информации при взаимодействии с Сетью;
- порядок контроля за выполнением мероприятий по обеспечению безопасности информации и работой абонентов Сети.

6.3.14. К работе в качестве абонентов Сети допускается круг пользователей, ознакомленных с требованиями по взаимодействию с другими абонентами Сети и обеспечению при этом безопасности информации и допускаемых к самостоятельной работе в Сети после сдачи соответствующего зачета.

6.3.15. Абоненты Сети обязаны:

- знать порядок регистрации и взаимодействия в Сети;
- знать инструкцию по обеспечению безопасности информации на АП;
- знать правила работы со средствами защиты информации от НСД, установленными на АП (серверах, рабочих станциях АП);
- уметь пользоваться средствами антивирусной защиты;
- после окончания работы в Сети проверить свое рабочее место на наличие «вирусов».

6.3.16. Входящие и исходящие сообщения (файлы, документы), а также используемые при работе в Сети носители информации, учитываются в журналах несекретного делопроизводства. При этом на корпус (конверт) носителя информации наносится предупреждающая маркировка: «Допускается использование только в Сети».

6.3.17. Для приемки в эксплуатацию АП, подключаемого к Сети, приказом по учреждению (предприятию) назначается аттестационная комиссия, проверяющая выполнение установленных требований и рекомендаций. Аттестационная комиссия в своей работе руководствуется требованиями и рекомендациями настоящего документа.

6.3.18. По результатам работы комиссии оформляется заключение, в котором отражаются следующие сведения:

- типы и номера выделенных технических средств АП, в том числе каждого абонента, их состав и конфигурация;
- состав общего и сервисного прикладного коммуникационного программного обеспечения (ОС, маршрутизаторов, серверов, межсетевых экранов, Browsers и т.п.) на АП в целом и на каждой рабочей станции абонента в частности: логические адреса (IP-адреса), используемые для доступа в Сети;
- мероприятия по обеспечению безопасности информации, проведенные при установке технических средств и программного обеспечения, в том числе ■ средств защиты информации от НСД, антивирусных средств, по защите информации от утечки по каналам ПЭМИН, наличие инструкции по обеспечению безопасности информации на АП.

6.3.19. При работе в Сети категорически запрещается:

- подключать технические средства (серверы, рабочие станции), имеющие выход в Сеть, к другим техническим средствам (сетям), не определенным в обосновании подключения к Сети;
- изменять состав и конфигурацию программных и технических средств АП без санкции администратора и аттестационной комиссии;
- производить отправку данных без соответствующего разрешения;

• использовать носители информации с маркировкой: «Допускается использование только в Сети» на рабочих местах других систем (в том числе и автономных ПЭВМ) без соответствующей санкции.

6.3.20. Ведение учета абонентов, подключенных к Сети, организуется в устанавливаемом в учреждении (на предприятии) порядке.

6.3.21. Контроль за выполнением мероприятий по обеспечению безопасности информации на АП возлагается на администраторов АП, руководителей соответствующих подразделений, определенных приказом по учреждению (предприятию), а также руководителя службы безопасности.

Приложение к П-14

1. Акт классификации автоматизированной системы обработки информации

Для служебного пользования

Экз. № ____

УТВЕРЖДАЮ

Руководитель предприятия

«__» _____ 20__ г.

АКТ классификации автоматизированной системы обработки информации

(наименование автоматизированной системы)

Комиссия в составе:

председатель: _____

члены комиссии: _____

рассмотрев исходные данные на автоматизированную систему обработки информации (АС)

(наименование автоматизированной системы)

условия ее эксплуатации (многопользовательский, однопользовательский; с равными или разными правами доступа к информации), с учетом характера обрабатываемой информации (служебная тайна, коммерческая тайна, персональные данные и т.д.) и в соответствии с руководящими документами Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» и «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)»,

РЕШИЛА: Установить АС _____

(наименование автоматизированной системы)

класс защищенности

Председатель _____

Члены комиссии _____

2. Аттестат соответствия на АС

АТТЕСТАТ СООТВЕТСТВИЯ

№ ____

(указывается полное наименование автоматизированной системы)

требованиям по безопасности информации

Выдан «__» _____ 20__ г.

1. Настоящим аттестатом удостоверяется, что: _____

(приводится полное наименование автоматизированной системы)

класса защищенности соответствует требованиям нормативной документации по безопасности информации.

Состав комплекса технических средств автоматизированной системы (АС) с указанием заводских номеров, модели, изготовителя, номеров сертификатов соответствия, схемы размещения в помещениях и относительно границ контролируемой зоны, перечня используемых программных средств, а также средств защиты (с указанием изготовителя и номеров сертификатов соответствия) указаны в техническом паспорте на АС.

2. Организационная структура, уровень подготовки специалистов, нормативно-методическое обеспечение обеспечивают поддержание уровня защищенности АС в процессе эксплуатации в соответствии с установленными требованиями.

3. Аттестация АС выполнена в соответствии с программой и методиками аттестационных испытаний, утвержденными руководителем предприятия (указываются номера документов).

4. С учетом результатов аттестационных испытаний в АС разрешается обработка конфиденциальной информации.

5. При эксплуатации АС запрещается:

- вносить изменения в комплектность АС, которые могут снизить уровень защищенности информации;
- проводить обработку защищаемой информации без выполнения всех мероприятий по защите информации;
- подключать к основным техническим средствам нештатные блоки и устройства;
- вносить изменения в состав, конструкцию, конфигурацию, размещение средств вычислительной техники;

при обработке на ПЭВМ защищаемой информации подключать измерительную аппаратуру;

- допускать к обработке защищаемой информации лица, не оформленные в установленном порядке;
- производить копирование защищаемой информации на неучтенные магнитные носители информации, в том числе для временного хранения информации;
- работать при отключенном заземлении;
- обрабатывать на ПЭВМ защищаемую информацию при обнаружении каких-либо неисправностей.

6. Контроль за эффективностью реализованных мер и средств защиты возлагается

(наименование подразделения, должность лица осуществляющего контроль)

7. Подробные результаты аттестационных испытаний приведены в заключении аттестационной комиссии (№ __ от ____) и протоколах испытаний.

8. «Аттестат соответствия» выдан на ____ года (лет), в течение которых должна быть обеспечена неизменность условий функционирования АС и технологии обработки защищаемой информации, могущих повлиять на характеристики защищенности АС.

Руководитель аттестационной комиссии _____
(должность с указанием наименования предприятия) Ф.И.О.

«__» _____ 200__ г.

Отметки органа надзора:

3. Аттестат соответствия на защищаемое помещение

АТТЕСТАТ СООТВЕТСТВИЯ № __

(указывается наименование защищаемого помещения)

требованиям по безопасности информации

Выдан «__» _____ 20__ г.

1. Настоящим АТТЕСТАТОМ удостоверяется, что

(полное наименование защищаемого помещения)

и установленное в нем оборудование соответствуют требованиям нормативных документов по безопасности информации (Заключение по результатам аттестации № __ от ____) и в нем разрешается проведение конфиденциальных мероприятий.

Схема размещения помещения относительно границ контролируемой зоны, перечень установленного в нем оборудования, используемых средств защиты информации указаны в техническом паспорте на защищаемое помещение (ЗП).

2. Установленный порядок использования ЗП позволяет осуществлять его эксплуатацию, расположенного в нем оборудования и средств защиты в соответствии с требованиями по защите конфиденциальной информации.

3. Повседневный контроль за выполнением установленных правил эксплуатации ЗП осуществляется

(наименование подразделения, должностного лица, осуществляющего контроль)

4. В ЗП запрещается проводить ремонтно-строительные работы, замену (установку новых) элементов интерьера, вносить изменения в состав оборудования и средства защиты информации без согласования с

(наименование подразделения, должностного лица, осуществляющего контроль)

5. Лицо, ответственное за эксплуатацию защищаемого помещения, обязано незамедлительно извещать

(наименование подразделения, должностного лица, осуществляющего контроль)

- о предполагаемых ремонтно-строительных работах и изменениях в размещении и монтаже установленного оборудования, технических средств и систем, средств защиты информации, в интерьере помещения;
- о нарушениях в работе средств защиты информации;
- о фактах несанкционированного доступа в помещение.

Руководитель аттестационной комиссии _____
(должность с указанием наименования предприятия) Ф.И.О.

«__» _____ 200__ г.

Отметки органа надзора:

4. Технический паспорт на защищаемое помещение

Форма технического паспорта на защищаемое помещение

ТЕХНИЧЕСКИЙ ПАСПОРТ на защищаемое помещение № __

Составил _____
(Подпись специалиста подразделения по защите информации)

Ознакомлен _____
(Подпись лица, ответственного за помещение)

(год)

ПАМЯТКА

по обеспечению режима безопасности и эксплуатации оборудования, установленного
в защищаемом помещении № __

(Примерный текст)

1. Ответственность за режим безопасности в защищаемом помещении (ЗП) и правильность использования установленных в нем технических средств несет лицо, которое постоянно в нем работает, или лицо, специально на то уполномоченное.

2. Установка нового оборудования, мебели и т.п. или замена их, а также ремонт помещения должны проводиться только по согласованию с подразделением (специалистом) по защите информации предприятия.

3. В нерабочее время помещение должно закрываться на ключ.

4. В рабочее время, в случае ухода руководителя, помещение должно закрываться на ключ или оставаться под ответственность лиц, назначенных руководителем подразделения.

5. При проведении конфиденциальных мероприятий бытовая радиоаппаратура, установленная в помещении (телевизоры, радиоприемники и т.п.), должна отключаться от сети электропитания.

6. Должны выполняться предписания на эксплуатацию средств связи, вычислительной техники, оргтехники, бытовых приборов и другого оборудования, установленного в помещении.

7. Запрещается использование в ЗП радиотелефонов, оконечных устройств сотовой, пейджинговой и транкинговой связи. При установке в ЗП телефонных и факсимильных аппаратов с автоответчиком, спикерфоном и имеющих выход в городскую АТС, следует отключать эти аппараты на время проведения конфиденциальных мероприятий.

8. Повседневный контроль за выполнением требований по защите помещения осуществляют лица, ответственные за помещение, и служба безопасности предприятия.

9. Периодический контроль эффективности мер защиты помещения осуществляется специалистами по защите информации. Примечание: В памятку целесообразно включать и другие сведения, учитывающие особенности установленного в ЗП оборудования; действия персонала в случае срабатывания установленной в помещении сигнализации, порядок включения средств защиты, организационные меры защиты и т.п.

Перечень оборудования, установленного в помещении

Вид оборудования	Тип	Учетный (зав.) номер	Дата установки	Класс ТС(ОТСС или ВТСС)	Сведения по сертификации, спец-исследованиям и спецпроверкам

Меры защиты информации

(пример)

1. Телефонный аппарат коммутатора директора (инв. № 5). Выполнены требования предписания на эксплуатацию: (Перечень предусмотренных мер защиты согласно предписанию).

2. Телефонный аппарат № 7-15.

На линию установлено защитное устройство «Сигнал-5», зав. № 01512.

3. Пульт коммутатора.

Выполнены требования предписания на эксплуатацию: (Перечень предусмотренных мер защиты согласно предписанию).

4. Часы электронные.

Выполнены требования предписания на эксплуатацию: (Перечень предусмотренных мер защиты согласно предписанию).

5. Вход в помещение оборудован тамбуром, двери двойные, обшиты слоем ваты и дерматина. Дверные при-
творы имеют резиновые уплотнения.

6. Доступ посторонних лиц к вентиляционным каналам, выходящим на чердак здания, исключен (приводят-
ся предусмотренные для этого меры).

Отметка о проверке средств защиты

Вид оборудо- вания	Учетный номер	Дата проверки	Результаты проверки и № отчетного документа

Результаты аттестационного и периодического контроля помещения

Дата проведения	Результаты аттестации или периодического контроля, № отчетного документа	Подпись проверяющего

5. Технический паспорт на АС

Форма технического паспорта на автоматизированную систему

УТВЕРЖДАЮ

Руководитель предприятия

«__» _____ 20__ г.

ТЕХНИЧЕСКИЙ ПАСПОРТ

(указывается полное наименование автоматизированной системы)

СОГЛАСОВАНО

РАЗРАБОТАЛ

(Представитель подразделения по защите информации)

«__» _____ 200__ г.

1. Общие сведения об АС

1.1. Наименование АС: _____
(полное наименование АС)

1.2. Расположение АС: _____
(адрес, здание, строение, этаж, комнаты)

1.3. Класс АС: _____
(номер и дата акта классификации АС, класс АС)

2. Состав оборудования АС

2.1. Состав ОТСС:

Таблица 5.1

ПЕРЕЧЕНЬ

основных технических средств и систем, входящих в состав АС _____

№п/п	Тип ОТСС	Заводской номер	Сведения по сертификации, специсследованиям и спецпроверкам

2.2. Состав ВТСС объекта:

Таблица 5.2

ПЕРЕЧЕНЬ

вспомогательных технических средств, входящих в состав АС _____

(средств вычислительной техники, не участвующих в обработке конфиденциальной информации)

№ п/п	Тип ВТСС	Заводской номер	Примечание

2.3. Структура, топология и размещение ОТСС относительно границ контролируемой зоны объекта: струк-
турная (топологическая) схема с указанием информационных связей между устройствами; схема размещения и
расположения ОТСС на объекте с привязкой к границам контролируемой зоны; схема прокладки линий передачи
конфиденциальной информации с привязкой к границам контролируемой зоны объекта.

2.4. Системы электропитания и заземления: схемы электропитания и заземления ОТСС объекта; схемы прокладки кабелей и шины заземления. Схемы расположения трансформаторной подстанции и заземляющих устройств с привязкой к границам контролируемой зоны объекта; схемы электропитания розеточной и осветительной сети объекта; сведения о величине сопротивления заземляющего устройства.

2.5. Состав средств защиты информации:

Таблица 5.3

ПЕРЕЧЕНЬ
средств защиты информации, установленных на АС

№ п/п	Наименование и тип технического средства	Заводской номер	Сведения о сертификате	Место и дата установки

3. Сведения об аттестации объекта информатизации на соответствие требованиям по безопасности информации: инвентарные номера аттестата соответствия, заключения по результатам аттестационных испытаний, протоколов испытаний и даты их регистрации.

4. Результаты периодического контроля.

Таблица 5.4

Дата проведения	Наименование организации, проводившей проверку	Результаты проверки, № отчетного документа

Лист регистрации изменений

6. Документальное оформление перечня сведений конфиденциального характера

Пример документального оформления перечня сведений конфиденциального характера

УТВЕРЖДАЮ
Руководитель предприятия

«__» _____ 200__ г.

ПЕРЕЧЕНЬ
сведений конфиденциального характера

№	Наименование сведений	Примечание
1.	Сведения, раскрывающие систему, средства защиты информации ЛВС предприятия от НСД, а также значения действующих кодов и паролей.	
2.	Сводный перечень работ предприятия на перспективу, на год (квартал).	
3.	Сведения, содержащиеся в лицевых счетах пайщиков страховых взносов.	
4.	Сведения, содержащиеся в индивидуальном лицевом счете застрахованного лица.	
5.	Основные показатели задания на проектирование комплекса (установки). НОУ-ХАУ технологии - различные технические, коммерческие и другие сведения, оформленные в виде технической документации.	
6.	Методические материалы, типовые технологические и конструктивные решения, разработанные на предприятии и используемые при проектировании.	А.
7.	Требования по обеспечению сохранения служебной тайны при выполнении работ на предприятии.	
8.	Порядок передачи служебной информации ограниченного распространения другим организациям.	

7. Основные нормативные правовые акты и методические документы по ЗИ

Основные нормативные правовые акты и методические документы по защите конфиденциальной информации

1. Федеральный закон от 20.02.95 г. № 24-ФЗ «Об информации, информатизации и защите информации».

2. Федеральный закон от 04.07.96 г. № 85-ФЗ «Об участии в международном информационном обмене».

3. Федеральный закон от 16.02.95 г. № 15-ФЗ «О связи».

4. Федеральный закон от 08.08.2001 г. № 128-ФЗ «О лицензировании отдельных видов деятельности».
5. Указ Президента Российской Федерации от 19.02.99 г. № 212 «Вопросы Государственной технической комиссии при Президенте Российской Федерации».
6. «Доктрина информационной безопасности Российской Федерации», утверждена Президентом Российской Федерации 09.09.2000 г. Пр. № 1895.
7. Указ Президента Российской Федерации от 17.12.97 г. № 1300 «Концепция национальной безопасности Российской Федерации» в редакции указа Президента Российской Федерации от 10.01.2000 г. № 24.
8. Указ Президента Российской Федерации от 06.03.97 г. № 188 «Перечень сведений конфиденциального характера».
9. Постановление Правительства Российской Федерации от 03.11.94 г. № 1233 «Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».
10. Решение Гостехкомиссии России и ФАПСИ от 27.04.94 г. № 10 «Положение о государственном лицензировании деятельности в области защиты информации» (с дополнением).
11. Постановление Правительства Российской Федерации от 11.04.2000 г. № 326 «О лицензировании отдельных видов деятельности».
12. «Сборник руководящих документов по защите информации от несанкционированного доступа» Гостехкомиссия России, Москва, 1998 г.
13. ГОСТ Р 51275-99 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения».
14. ГОСТ Р 50922-96 «Защита информации. Основные термины и определения».
15. ГОСТ Р 51583-2000 «Порядок создания автоматизированных систем в защищенном исполнении».
16. ГОСТ Р 51241-98 «Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний».
17. ГОСТ 12.1.050-86 «Методы измерения шума на рабочих местах».
18. ГОСТ Р ИСО 7498-1-99 «Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации».
19. ГОСТ 2.114-95 «Единая система конструкторской документации. Технические условия».
20. ГОСТ 2.601-95 «Единая система конструкторской документации. Эксплуатационные документы».
21. ГОСТ 34.201-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем».
22. ГОСТ 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированных систем».
23. ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения».
24. РД Госстандарта СССР 50-682-89 «Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Общие положения».
25. РД Госстандарта СССР 50-34.698-90 «Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов».
26. РД Госстандарта СССР 50-680-89 «Методические указания. Автоматизированные системы. Основные положения».
27. ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадия создания».

28. ГОСТ 6.38-90 «Система организационно-распорядительной документации. Требования к оформлению».
29. ГОСТ 6.10-84 «Унифицированные системы документации. Придание юридической силы документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники, ЕСКД, ЕСПД и ЕСТД».
31. ГОСТ Р-92 «Система сертификации ГОСТ. Основные положения».
32. ГОСТ 28195-89 «Оценка качества программных средств. Общие положения».
33. ГОСТ 28806-90 «Качество программных средств. Термины и определения».
34. ГОСТ Р ИСОЧМЭК 9126-90 «Информационная технология. Оценка программной продукции. Характеристика качества и руководства по их применению».
35. ГОСТ 2.111-68 «Нормоконтроль».
36. ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации».
37. РД Гостехкомиссии России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля не декларированных возможностей», Москва, 1999 г.
38. РД Гостехкомиссии России «Средства защиты информации. Специальные общие технические требования, предъявляемые к сетевым помехоподавляющим фильтрам». – М.: 2000.
39. ГОСТ 13661-92 «Совместимость технических средств электромагнитная. Пассивные помехоподавляющие фильтры и элементы. Методы измерения вносимого затухания».
40. Временная методика оценки защищенности основных технических средств и систем, предназначенных для обработки, хранения и (или) передачи по линиям связи конфиденциальной информации.
41. Временная методика оценки защищенности конфиденциальной информации, обрабатываемой основными техническими средствами и системами, от утечки за счет наводок на вспомогательные технические средства и системы и их коммуникации.
42. Временная методика оценки защищенности речевой конфиденциальной информации от утечки по акустическому и виброакустическому каналам.
43. Временная методика оценки защищенности речевой конфиденциальной информации от утечки за счет электроакустических преобразований во вспомогательных технических средствах и системах.
44. ГОСТ 29216-91 «Совместимость технических средств электромагнитная. Радиопомехи промышленные от оборудования информационной техники. Нормы и методы испытаний».
45. ГОСТ 22505-83 «Радиопомехи промышленные от приемников телевизионных и приемников радиовещательных частотно-модулированных сигналов в диапазоне УКВ. Нормы и методы измерений».
46. ГОСТ Р 50628-93 «Совместимость электромагнитная машин электронных вычислительных персональных. Устойчивость к электромагнитным помехам. Технические требования и методы испытаний».
47. ПУЭ-76 «Правила устройства электроустановок».
48. Решение Гостехкомиссии России от 14.03.95 г. № 32 «Типовое положение о Совете (Технической комиссии) министерства, ведомства, органа государственной власти субъекта Российской Федерации по защите информации от иностранных технических разведок и от ее утечки по техническим каналам».
49. Решение Гостехкомиссии России от 14.03.95 г. № 32 «Типовое положение о подразделении по защите информации от иностранных технических разведок и от ее утечки по техническим каналам в министерствах и ведомствах, в органах государственной власти субъектов Российской Федерации».
50. Решение Гостехкомиссии России от 14.03.95 г. № 32 «Типовое положение о подразделении по защите информации от иностранных технических разведок и от ее утечки по техническим каналам на предприятии (в учреждении, организации)».

51. СанПиН 2.2.2.542-96 «Гигиенические требования к видеодисплейным терминалам, персональным электронно-вычислительным машинам и организация работы».
52. ГОСТ Р 50948-96. «Средства отображения информации индивидуального пользования. Общие эргономические требования и требования безопасности».
53. ГОСТ Р 50949-96 «Средства отображения информации индивидуального пользования. Методы измерений и оценки эргономических параметров и параметров безопасности».
54. ГОСТ Р 50923-96 «Рабочее место оператора. Общие эргономические требования и требования к производственной среде. Методы измерения».
55. Решение Гостехкомиссии России от 03.10.95 г. № 42 «Типовые требования к содержанию и порядку разработки Руководства по защите информации от технических разведок и ее утечки по техническим каналам на объекте».

Лаптев Владимир Николаевич
Лаптев Сергей Владимирович

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Справочник для бакалавров специальности
080500.62 – Бизнес информатика

Лицензия ИД № 02334 от 14.07.2000

Подписано в печать
Бумага офсетная
Печ.л. 4,0
Тираж экз.

Формат 60х84
Офсетная печать
Заказ №

Отпечатано в типографии КубГАУ, 350044, г. Краснодар, ул. Калинина, 13