Книги — это корабли мысли,
странствующие по волнам времени
и бережно несущие свой драгоценный груз
от поколения к поколению.

Ф. Бэкон

Н.Н. Куняев
А.С. Дёмушкин
А.Г. Фабричнов

Конфиденциальное делопроизводство и защищенный электронный документооборот

Под общей редакцией Н.Н. Куняева

Рекомендовано в качестве учебника для студентов высших учебных заведений, обучающихся по направлениям подготовки 032000 «Документоведение и архивоведение», 080500 «Менеджмент», 090100 «Информационная безопасность», 032001 «Документоведение и документационное обеспечение управления», 080507 «Менеджмент организации», 090103 «Организация и технология защиты информации»

Москва
ЛОГОС
2011

УДК 005.92
ББК 65.050.2
К91

Серия основана в 2003 году

Официальный рецензент
системы рецензирования Министерства образования и науки
Российской Федерации – Государственный университет управления.
Регистрационный номер рецензии 977 от 10.08.2010 МГУП

Рецензенты

А.П. Баранов, доктор физико-математических наук

А.А. Брагин, заместитель директора Федеральной службы
технико-экономического контроля России

А.Г. Забелин, доктор экономических наук, профессор,
ректор Московской финансово-юридической академии

Куняев Н.Н.

К91 Конфиденциальное делопроизводство и защищенный электронный документооборот: учебник / Н.Н. Куняев, А.С. Дёмушкин, А.Г. Фабричнов; под общ. ред. Н.Н. Куняева. – М.: Логос, 2011. – 452 с. (Новая университетская библиотека).

ISBN 978-5-98704-541-1

Раскрыты сущность и особенности конфиденциального делопроизводства. Освещены вопросы документирования конфиденциальной информации, оформления конфиденциальных документов, их учета, организации конфиденциального документооборота, классификации и систематизации конфиденциальных документов, обеспечения разрешительной системы доступа и режима конфиденциальной информации, подготовки конфиденциальных документов для передачи в архив и уничтожения. Дан анализ современных нормативных правовых актов в сфере информации ограниченного доступа и конфиденциальной документированной информации: персональных данных; служебной, профессиональной, коммерческой тайн; секретов производства и др.

Для студентов высших учебных заведений, обучающихся по направлениям подготовки 032000 «Документоведение и архивоведение», 080500 «Менеджмент», 090100 «Информационная безопасность», а также специальностям 032001 «Документоведение и документационное обеспечение управления», 080507 «Менеджмент организации», 090103 «Организация и технология защиты информации».

УДК 005.92
ББК 65.050.2

ISBN 978-5-98704-541-1

ОГЛАВЛЕНИЕ

СПИСОК СОКРАЩЕНИЙ

АИС – автоматизированная информационная система
АРМ – автоматизированное рабочее место
БД – база данных
ВЭД – внутренний электронный документооборот
ИКС – информационно-коммуникационная система
КДИ – конфиденциальная документированная информация
ЛВС – локальная вычислительная сеть
МЭД – межведомственный (межсетевой) электронный документооборот
НИОКР – научно-исследовательские и опытно-конструкторские работы
НСД – несанкционированный доступ
НСВ – несанкционированное воздействие
ПД – персональные данные
ПЭМИ – побочное электромагнитное излучение
ПЭМИН – побочное электромагнитное излучение и наводки
СВТ – средства вычислительной техники
СЗИ – средства защиты информации
СКФД – совершенно конфиденциально
СУБД – система управления базами данных
СЭС – система электронных сообщениий
ТЗ – техническое задание
УЦ – удостоверяющий центр
ЭВМ – электронная вычислительная машина
ЭВТ – электронно-вычислительная техника
ЭК – экспертная комиссия
ЭПК – экспертная проверочная комиссия
ЭЦП – электронная цифровая подпись

ВВЕДЕНИЕ

Доктриной информационной безопасности России определено, что одной из составляющих национальных интересов Российской Федерации в информационной сфере является защита 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 также систем и средств информатизации вооружения и военной техники, систем управления войсками и оружием, экологически опасными и экономически важными производствами [71].

Организация системы защиты информации включает защиту единой информационной сферы (среды) организации. *Информационной средой* является совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникших при этом общественных отношений.

Одним из основных разделов Концепции формирования в Российской Федерации электронного правительства до 2010 года [116] является «Развитие защищенной межведомственной системы электронного документооборота», в котором сказано: «В целях повышения эффективности государственного управления требуется завершить работы по созданию и внедрению защищенной технологической системы межведомственного электронного документооборота, которая должна обеспечить оперативный информационный и документационный обмен... Система межведомственного электронного документооборота создается для осуществления защищенного обмена электронными сообщениями. При этом в переходный период электронные документы предполагается дублировать документами, подготовленными на бумажных носителях».

В Федеральном законе «Об информации, информационных технологиях и о защите информации» определено, что документированная информация – это зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию, или в установленных законодательством Российской Федерации случаях ее материальный носитель [23, ст. 2]. В федеральных органах исполнительной власти документирование информации осуществляется в порядке, устанавливаемом Правительством Российской Федерации. Правила делопроизводства и документооборота, установленные иными государственными органами, органами местного самоуправления в пределах их компетенции, должны соответствовать требованиям, установленным Правительством Российской Федерации в части делопроизводства и документооборота для федеральных органов исполнительной власти [23, ст. 11].

Документированная информация представляет собой различные виды документов. Существует множество определений понятия «документ». Мы берем за основу определение, данные в Правилах делопроизводства в федеральных органах исполнительной власти [76], поскольку их возможно применять в любых государственных и негосударственных структурах:

«Документ – официальный документ, созданный государственным органом, органом местного самоуправления, юридическим или физическим лицом, оформленный в установленном порядке и включенный в документооборот федеральных органов исполнительной власти».

Под *делопроизводством*, или документационным обеспечением управления, понимается отрасль деятельности, обеспечивающая документирование и организацию работы с документами, а под *документооборотом* – движение документов в организации с момента их создания или получения до завершения исполнения или отправки [163].

Федеральным законом «Об информации, информационных технологиях и о защите информации» определено, что «обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами, устанавливающими условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение. *Конфиденциальность информации* – обязательное для выполнения лицом, получив-

шим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя» [23, ст. 2].

Соответственно, документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации, является конфиденциальной документированной информацией, или конфиденциальным документом, за исключением информации, которая составляет государственную тайну, имеющую свой правовой режим. Защита информации, составляющей государственную тайну, осуществляется в соответствии с законодательством Российской Федерации о государственной тайне.

Конфиденциальной информацией (Sensitive information) является информация, требующая защиты. Технологии конфиденциального (защищенного) электронного документооборота являются информационными. *Информационные технологии* – это процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов. Технологии обработки, хранения, передачи и защиты информации входят в Перечень технологий, имеющих большое социально-экономическое значение или важное значение для обороны страны и безопасности государства (критические технологии) [113].

Проблемы защиты информации стали более сложными и значимыми в связи с переходом жизненного цикла документированной информации на безбумажную, электронную основу с одновременным применением как «бумажных» технологий делопроизводства и документооборота, так и электронных с использованием автоматизированных информационных систем (АИС).

В Федеральном законе «Об информации, информационных технологиях и о защите информации» *информационная система* определена как совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств [23, ст. 2]. В приведенном определении не присутствует основной субъект отношений в области защиты информации – персонал информационной системы. Поэтому вместо термина «информационная система», как правило, используется термин «автоматизированная система», определяемый ГОСТом 34.003–90 [181] как система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Совмещая термины «информационная система» и «автоматизированная система», используют интегрированный термин «автоматизированная информационная система».

Конфиденциальная документированная информация (КДИ) составляет одну из основных частей информационных ресурсов организации. Конфиденциальное делопроизводство и документооборот, включая электронный, следует определять как жизненный цикл конфиденциальной документированной информации или сумму технологий, обеспечивающих организацию работы с КДИ и ее защиту. При этом под *технологиями конфиденциального делопроизводства* понимается процесс подготовки и создания документов, а *под технологиями конфиденциального документооборота*, включая электронный, – учет, прохождение, исполнение, отправление, классификация, систематизация, разрешительный доступ к информации, хранение, уничтожение, режим хранения и обращения, режим конфиденциальности информации.

Конфиденциальное делопроизводство на бумажных носителях в целом базируется на тех же принципах, что и открытое делопроизводство, но в то же время имеет отличия, обусловленные конфиденциальностью информации. Об этом более подробно будет рассмотрено в гл. 1.

Оформление конфиденциальной информации на бумажном носителе должно соответствовать, как и для открытой информации, требованиям основного стандарта по оформлению документов [151]. Однако отличительной особенностью создания и оформления конфиденциальных документов является определение степени их конфиденциальности и проставление грифа ограничения доступа (отметки конфиденциальности) на документе. В связи с этим в гл. 2 не рассматривается оформление реквизитов открытых документов (по данному вопросу существует достаточное количество научной литературы) [285; 313; 317]. В этой главе акцентируется внимание на особенностях технологий определения степеней конфиденциальности документов и разработке Перечня конфиденциальной документированной информации, который является основой «бумажного» конфиденциального делопроизводства и предпосылкой для создания классификатора автоматизированной информационной системы, или иначе системы электронного документооборота.

Целью технологий открытого и конфиденциального документооборота является обеспечение исполнения и использования документов. Организация исполнения конфиденциальных документов включает в себя оперативное доведение их до исполнителей и обеспечение своевременного и качественного решения содержащихся в них вопросов. В процессе движения документов необходимо создавать условия для их сохранности. В противном случае исключается возможность исполнения и использования этих документов. Вместе

с тем особенность конфиденциального документооборота состоит в том, что требуется защита их от несанкционированного к ним доступа с целью предотвращения утечки содержащейся в них информации на всех этапах прохождения документов.

Защитные мероприятия охватывают не только саму документированную информацию, но и другие объекты, так или иначе связанные с защищаемой информацией (помещения, технические средства обработки и передачи информации и др.).

Технологии конфиденциального делопроизводства и документооборота во многом совпадают с технологиями организации работы с документированной информацией ограниченного доступа, составляющей государственную тайну, которые определены постановлениями Правительства Российской Федерации, например Постановлением Правительства Российской Федерации от 06.02.2010 № 63 «Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне». Самое главное – это то, что по своей сути они не являются секретными и регулируются общедоступными нормативными правовыми актами о государственной тайне, поэтому данные об этих технологиях приведены в главах с соответствующими ссылками.

Обеспечение сохранности и конфиденциальности документированной информации требует создания и поддержания специальных условий хранения, обработки и обращения документов, гарантирующих надежную защиту как самих документов, так и содержащейся в них информации. Достигается это путем организации специального режима хранения конфиденциальной информации и обращения с ней, установления разрешительной системы доступа, разработки регламентированной технологии ее создания и обработки. При этом под *доступом к конфиденциальной информации* понимается санкционированное полномочным должностным лицом ознакомление конкретного лица с данной информацией [50, ст. 2]. Права доступа к документам разграничиваются на основе предоставления различных полномочий должностным лицам организации на различных участках технологий делопроизводства и документооборота, в том числе электронного, по приему и отправке, ознакомлению, регистрации, учету, контролю исполнения, качества исполнения, ведению баз данных, редактированию, снятию с контроля, списанию в дело, хранению, использованию и уничтожению. В гл. 4 рассмотрены основные требования к разрешительной системе доступа и особенности допуска и доступа к различным видам конфиденциальной информации.

Требования к конфиденциальному делопроизводству и документообороту, в том числе электронному, обусловливаются организационными и технологическими особенностями, основными из которых являются следующие:

• регламентирование состава создаваемых документов и процессов документирования, в том числе на стадии подготовки черновиков и проектов документов;

• обязательный поэкземплярный и полистный учет всех, без исключения, документов, проектов и черновиков;

• необходимая полнота учетных и регистрационных данных о каждом документе, включая электронные документы (электронные сообщения), циркулирующие в автоматизированной информационной системе;

• фиксация прохождения и местонахождения каждого документа, включая электронные документы (электронные сообщения), циркулирующие в автоматизированной информационной системе;

• регламентация обшей технологии документирования, организации работы с документами и их защиты;

• проведение систематических проверок наличия документов;

• система доступа к документам и делам, включая электронные документы (электронные сообщения), циркулирующие в автоматизированных информационных системах, обеспечивающая правомерное и санкционированное ознакомление с ними;

• основательные требования к условиям хранения документов и обращения с ними, которые должны обеспечивать сохранность и конфиденциальность документированной информации;

• персональная и обязательная ответственность за учет, сохранность конфиденциальных документов и порядок обращения с ними.

Руководство организации в пределах своей компетенции определяет:

• категории должностных лиц, уполномоченных относить информацию (документы) к конфиденциальной;

• круг должностных лиц, имеющих доступ к документам и информации различной степени конфиденциальности;

• порядок снятия отметки конфиденциальности с документов, включая электронные, циркулирующие в АИС, иными словами, системах электронного документооборота;

• организацию защиты информации на бумажном носителе;

• организацию защиты информации, циркулирующей в системах электронного документооборота, а также защиту самих автоматизированных информационных систем.

Правительство Российской Федерации утвердило Положение о системе межведомственного электронного документооборота (МЭД), определяющее взаимодействие федеральных информационных систем электронного документооборота [74]. Под *взаимодействием информационных систем электронного документооборота* в Положении понимается обмен электронными сообщениями (ведение служебной переписки в электронной форме) между участниками межведомственного электронного документооборота. Система МЭД – федеральная информационная система, обеспечивающая в автоматизированном режиме защищенный обмен электронными сообщениями, в том числе сообщениями, содержащими информацию, отнесенную к сведениям, составляющим служебную тайну, о чем более подробно рассмотрено в гл. 8.

Должностные лица организации, принявшие решение об отнесении документов к информации ограниченного доступа, несут персональную ответственность за обоснованность такого решения и за соблюдения ограничений. Одним из основных принципов правового регулированияявляется открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации. В отдельных нормативных правовых актах в области защиты информации существуют перечни сведений, которые запрещено относить к какой-либо тайне (см. приложение 1).

За нарушение режима конфиденциальности информации, основных положений работы с конфиденциальными документами, утрату и незаконное их уничтожение, за разглашение конфиденциальных сведений виновные лица, сотрудники и работники организации должны привлекаться к предусмотренной законодательством ответственности. По этому поводу существуют определенные статьи Уголовного кодекса Российской Федерации и Кодекса об административных правонарушениях Российской Федерации, выписки из которых приведены в приложении 6.

Контроль за выполнением требований при работе с конфиденциальными документами возлагается на Службу открытого делопроизводства или Службу конфиденциального делопроизводства (если такая предусмотрена в организации), на сотрудников структурных подразделений организации, отвечающих за ведение открытого и конфиденциального делопроизводства, а также на Службу безопасности (если такая служба или ответственное лицо за безопасность также предусмотрены в организации) (далее по тексту Служба делопроизводства).

Контроль за выполнением требований по работе с кадровой документацией – персональными данными работников и сотрудников, также являющимися конфиденциальной информацией, возлагается на Службы кадров и безопасности организации.

Типовой порядок использования электронных документов с электронной цифровой подписью (подписанных ЭЦП), приведен в приложении 7. Общее описание организации взаимодействия системы межведомственного (межсетевого) электронного документооборота с системой внутреннего электронного документооборота дано в приложении 8.

Содержание книги отражает последовательность работы с конфиденциальной документированной информацией и базируется на действующих в настоящее время нормативных правовых актах и нормативно-методических документах, стандартах, руководящих документах, а также научных разработках.

В заключение следует отметить, что проводимые, в целях укрепления Российской государственности административные реформы, одной из главных задач нашего государства ставят обеспечение информационной безопасности. Информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации. Законом определено, что передача, предоставление и распространение информации ограниченного доступа и ее защита напрямую зависят от соблюдения конфиденциальности информации и мер по обеспечению этого режима, т.е. соответствующей организации конфиденциального делопроизводства и защищенного электронного документооборота.

Непрерывное развитие информационно-коммуникационных технологий влечет за собой развитие соответствующей нормативной правовой базы. В этих условиях авторы стремятся к объективному освещению всех поставленных вопросов и надеются в соответствии с Вашими рекомендациями выпустить исправленное и дополненное издание.

Коллектив авторов выражает огромную благодарность руководителю Федеральной налоговой службы Михаилу Владимировичу Мишустину и директору Всероссийского научно-исследовательского института документоведения и архивного дела Михаилу Васильевичу Ларину, а также всем тем, кто своим участием способствовал созданию данного учебника.

ГЛАВА 1

ПОНЯТИЕ И ОСОБЕННОСТИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ. ОБЩАЯ ХАРАКТЕРИСТИКА НОРМАТИВНОЙ ПРАВОВОЙ БАЗЫ

1.1. Общие положения

Характеристика понятий «ограничение доступа к информации» и «ограничение распространения информации» состоит в раскрытии системы признаков, использование которых необходимо для решения задач защиты информации, а также определения понятий «тайна» и «конфиденциальная информация», которые используются повсеместно при работе с конфиденциальными документами.

В Федеральном законе «Об информации, информационных технологиях и защите информации» в качестве основных принципов правового регулирования в информационной сфере названы [23, ст. 3]:

- свобода поиска, получения, передачи, производства и распространения информации любым законным способом;
- установление ограничений доступа к информации только федеральными законами;
- открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;
- обеспечение безопасности Российской Федерации при создании и эксплуатации информационных систем и защите содержащейся в них информации;
- достоверность информации и своевременность ее предоставления;
- неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;

• недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

В соответствии с Федеральным законом ограничение доступа к информации устанавливается в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства [23].

Обязательными являются соблюдение конфиденциальности информации ограниченного доступа, или «конфиденциальной информации», за исключением информации, составляющей государственную тайну [23, ст. 9].

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя. *Обладатель информации* – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам [23, ст. 2]. Обладателями информации могут быть гражданин (физическое лицо), юридическое лицо, государственные органы и органы местного самоуправления (далее – государственные и негосударственные структуры) в пределах их полномочий. Обладатель информации вправе:

• разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;

• использовать информацию, в том числе распространять ее по своему усмотрению;

• передавать информацию другим лицам по договору или на ином установленном законом основании.

Более подробно организация разрешительного доступа к конфиденциальной информации рассмотрена в гл. 4.

При осуществлении своих прав обладатель информации обязан:

• принимать меры по защите информации;

• ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

Информация ограниченного доступа, относящаяся к конфиденциальной и составляющая какую-либо тайну, за исключением государственной, не существует сама по себе. Она отображается на

различных носителях, которые могут ее сохранять, накапливать, передавать. Использование такой информации осуществляется с помощью носителей. *Документированная информация* – это зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию, или в установленных законодательством Российской Федерации случаях ее материальный носитель [23, ст. 2]. В ГОСТ 50922–96 содержится определение носителя информации как физического лица или материального объекта, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов [172]. Данное определение аналогично определению носителя государственной тайны в соответствии с Законом «О государственной тайне» [50, ст. 2].

Из сказанного следует, что:

• материальные объекты – это не только то, что можно увидеть, но и физические поля;

• информация на носителях отображается не только символами, т.е. буквами, цифрами, знаками, но и образами в виде рисунков, чертежей, схем, других знаковых моделей, сигналами в физических полях, техническими решениями в изделиях, техническими процессами в технологии изготовления продукции.

Типы материальных объектов как носителей информации различны. Ими могут быть бумажные носители, магнитные ленты, магнитные и лазерные диски, фото-, кино-, видео- и аудиопленки, различные виды промышленной продукции, технологические процессы, автоматизированные информационные системы и др.

Таким образом, понятие «конфиденциальная документированная информация», составляющая какую-либо тайну, за исключением государственной, является своего рода собирательным понятием, включающим различные носители с соответствующей информацией ограниченного доступа.

Государственная тайна – самостоятельная правовая категория, и ее правовой режим является предметом регулирования отдельной отрасли законодательства. Если рассмотреть более подробно общедоступную нормативную правовую базу о государственной тайне, то можно отметить следующее:

• сведения, составляющие государственную тайну или отнесенные к государственной тайне, – это информация ограниченного доступа, особенности которой необходимо знать при изучении особенностей конфиденциальной информации, также относящейся к категории ограниченного доступа;

• технологии конфиденциального делопроизводства и документооборота во многом совпадают с технологиями организации работы с документированной информацией, составляющей государственную тайну, и самое главное – по своей сути они не являются секретными и определены в общедоступной нормативной правовой базе о государственной тайне.

Перечень сведений конфиденциального характера утвержден Указом Президента Российской Федерации в марте 1997 г. [68]. К ним относятся:

1. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях [22] (см. разд. 1.2).

2. Сведения, составляющие тайну следствия и судопроизводства, а также сведения о защищаемых лицах и мерах государственной защиты, осуществляемой в соответствии с Федеральным законом от 20.08.2004 № 119-ФЗ "О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства" [28] и другими нормативными правовыми актами Российской Федерации (см. разд. 1.3).

3. Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации [11, ст. 1465, 1470] и федеральными законами (служебная тайна) (см. разд. 1.4).

4. Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная [19, ст. 61], нотариальная [20, ст. 5, 16], адвокатская тайна [36, ст. 8], тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений [32; 42, ст. 14] и т.д.) (см. разд. 1.5).

5. Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна) [29] (см. разд. 1.6).

6. Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них [5, ст. 1465, 1470] (см. разд. 1.7).

Законодательством Российской Федерации могут быть установлены виды информации ограниченного доступа, или конфиденциальной информации, в зависимости от ее содержания или решения обладателя информации.

Федеральный закон «Об информации...» подразделил информацию в зависимости от категории доступа к ней на общедоступную и информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа) [23, ст. 5, п. 2], а также в зависимости от порядка ее предоставления или распространения на следующие виды:

- свободно распространяемую;
- предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;
- предоставляемую или распространяемую в соответствии с федеральными законами;
- распространение которой в Российской Федерации ограничивается или запрещается [23, ст. 5, п. 3].

Постановлением Правительства Российской Федерации утверждено Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти [110] (более подробно см. разд. 1.4).

Законодательством введены два ограничения на отнесение информации к конфиденциальной: к ней не может быть отнесена информация, во-первых, составляющая государственную тайну, и, во-вторых, информация, которая должна быть общедоступной в целях предупреждения сокрытия правонарушений и предотвращения нанесения ущерба законным интересам государства, физических и юридических лиц. Перечни такой информации содержатся в Законе Российской Федерации «О государственной тайне», федеральных законах «Об информации, информационных технологиях и защите информации», «О коммерческой тайне», «О персональных данных», в Положении о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти и др. Более подробно Перечень информации, которую нельзя относить к информации ограниченного доступа, приведен в приложении 1.

Перечни информации, содержащиеся в нормативных актах, в значительной мере дублируют друг друга, имеют различную правовую основу и используются для создания перечней КДИ организаций – государственных и негосударственных структур (см. разд. 2.3). Перечни конфиденциальной документированной информации составляют основу конфиденциального делопроизводства и служат предпосылкой для создания классификаторов АИС, или систем защищенного электронного документооборота (см. гл. 8).

Должно быть и третье ограничение, которое не предусмотрено законодательством и нормативно-правовыми актами. Оно состоит в том, что при переводе информации в разряд конфиденциальной

(ограниченного доступа) необходимо учитывать сопутствующие этому финансовые затраты на ее защиту. То есть должен быть соблюден баланс безопасности организации и положительных экономических показателей от защиты информации и придания ей конфиденциальности. Если эти затраты превышают достигаемые в результате защиты экономические, финансовые и другие количественные и качественные показатели, то придание информации статуса конфиденциальной теряет смысл.

Информация может свободно использоваться любым лицом и передаваться одним лицом другому лицу, если законодательно не установлены ограничения доступа к информации либо иные требования к порядку ее предоставления или распространения.

Предоставление информации – действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц [23, ст. 2]. *Распространение информации* – действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц [Там же]. Следовательно, ограничение распространения информации – действия, направленные на получение информации определенным кругом лиц или передачу ее определенному кругу лиц.

Для понимания определения «информация ограниченного доступа и распространения» необходимо обратиться к рассмотрению категорий, так или иначе связанных с понятиями «тайна», «информация (сведения), составляющая тайну» и «конфиденциальная информация». В мировой практике законодательного регулирования конфиденциальной информации употреблялись различные термины, обозначавшие суть данного понятия и использовавшие ключевое слово «тайна».

Институт тайны имеет в российском законодательстве гораздо более глубокие корни. Правовые нормы, предусматривавшие ответственность за разглашение ценной конфиденциальной информации, содержались еще в Уложении о наказаниях 1845 г. [297]. Так, разд. VIII Уложения, который именовался «О преступлениях и проступках против общественного устройства и благочиния», включал в себя три статьи, посвященные ответственности за разглашение секретной информации.

Придавая той или иной информации конфиденциальность на законном основании, гражданин, организация, государство преследуют конкретные цели, предпринимают меры к сохранению этой информации в тайне. Незаконное получение такой информации, ее использование в ущерб обладателю, а также распространение лица-

ми, которым она была известна по роду их деятельности, наносят материальный или моральный вред обладателю этой информации. Государство принимает на себя обязанность по обеспечению безопасности и защите прав гражданина, организаций, государства на информацию, составляющую тайну, или иную информацию ограниченного доступа – конфиденциальную. Защита указанных прав осуществляется путем принятия соответствующих законов, иных нормативных правовых актов, предусматривающих ответственность третьих лиц за незаконное получение, использование такого рода информации, ее разглашение.

В 1993 г. в Законе Российской Федерации «О государственной тайне» впервые было официально определено понятие «государственной тайны»: «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» [50].

В действующем законодательстве нет определения понятия служебной тайны, но есть отдельные упоминания, как, например, в Федеральном законе «Об информации...». Вместе с тем на основе анализа нормативных правовых актов можно выделить содержание и основные признаки отнесения информации к служебной тайне, что более подробно рассмотрено в разд. 1.4 [217; 219; 222].

В Четвертой части Гражданского кодекса Российской Федерации введены определения новых понятий: «секрет производства (ноу-хау)» и «служебный секрет производства» [5, ст. 1465, 1470] (более подробно см. в разд. 1.7). В Федеральном законе «Об информации...» определено понятие «профессиональная тайна» [3, ст. 9, п. 5] (более подробно оно рассмотрено в разд. 1.5). Принятый в 2004 г. Федеральный закон «О коммерческой тайне» [29] определил понятие «коммерческая тайна» (более подробно об этом см. в разд. 1.6). Новая редакция закона 2007 г. вводит взаимосвязь коммерческой тайны и секрета производства.

В философском смысле тайна определяет два вида глобальной информации:

1) скрытую от нашего понимания или восприятия, в настоящее время не осознанную человеческим интеллектом, – объективные тайны (Вселенной, земли, океана, природы, человека, его рождения, смерти и т.д.), исследованием (или, применяя терминологию в области защиты информации, открытием доступа к информации) которых занимаются ученые и исследовательские центры;

2) известную, но с определенной целью скрытую от других людей, – субъективные тайны (личности, государства, общества, конкретной организации), т.е. защищаемую и охраняемую информацию, несанкционированный доступ к которой, а также санкционированный доступ, влекущий за собой несанкционированное разглашение или распространение информации, может нанести различного рода ущерб субъекту – обладателю информации, влекущий за собой экономические, финансовые, политические, моральные и другие потери.

Как мы предполагаем, понятие «тайна» имеет два смысловых значения: нечто абсолютно неизвестное всем и нечто относительно неизвестное для каких-либо лиц. Иными словами, информация должна быть известна или доверена узкому кругу лиц. При этом основанием известности информации тому или иному лицу могут быть профессиональная или служебная деятельность, семейно-брачные отношения и др. [228].

Термин «конфиденциальный» (от лат. *confidentia* – доверие) означает: доверительный, не подлежащий огласке. Общим для всех видов информации ограниченного доступа является тот факт, что свободный доступ к ней ограничен в силу предписаний федерального законодательства [228].

В настоящее время в российском законодательстве, а также в научных дисциплинах «Информационное право», «Документоведение» отсутствует общее понятие «тайна». В отечественной правовой литературе при определении отдельных видов тайн имеются различные спорные, порой противоречивые точки зрения. В ряде определений отсутствуют четкие признаки тайны, что, безусловно, затрудняет правильную оценку ее классификации в случае посягательства на защищаемые и охраняемые законом тайны.

В русском языке слово «тайна» определяется как «все скрытое, неизвестное, неведомое, или нечто скрываемое, секретное, не оглашаемое (не подлежащее распространению)» [329]. В Словаре русского языка С.И. Ожегова под тайной понимается «нечто скрываемое от других, известное не всем, секретное». В данных определениях тайны отражается весьма общий, скорее всего, бытовой характер взаимоотношений между людьми, так как содержание тайны – «нечто» – совершенно не конкретизировано, не определен и круг лиц, которым это «нечто» неизвестно.

Правовое понятие тайны выделяет следующие ее признаки:

• тайна есть, прежде всего, информация;

• информация должна быть известна или доверена узкому кругу лиц;

• информация может быть известна или доверена конкретным субъектам в силу их профессиональной или служебной деятельности, осуществления определенных поручений;

• информация не подлежит разглашению (огласке);

• разглашение информации может повлечь наступление негативных последствий (материальный и моральный ущерб ее обладателю, пользователю или иному лицу);

• на лицах, которым доверена информация, не подлежащая оглашению и распространению, лежит правовая обязанность и ответственность ее хранение и защиту;

• за разглашение этой информации законом устанавливается юридическая ответственность [284].

Держать в тайне, в секрете – значит защищать информацию от чего-либо, определять степень секретности и конфиденциальности информации. Понятие «тайна» можно определить так: *тайна, или секретность и конфиденциальность информации, – это состояние информации в определенный период времени, которое характеризуется ограничением на ее распространение и доступ к ней в связи с ее защитой и охраной государством или иным обладателем документированной информации. Конфиденциальная информация (документы), составляющая тайну, за исключением государственной, – информация ограниченного доступа и распространения.*

Ограничение доступа к информации, составляющей государственную тайну, определяет режим секретности информации, ее защиту органами, уполномоченными государством, применяемыми ими мероприятиями и средствами.

Ограничение доступа к информации и ограничение ее распространения определяет режим конфиденциальности информации, который предполагает ее охрану обладателем информации мерами и средствами, не противоречащими законодательству.

1.2. Персональные данные

В соответствии с Федеральным законом «О персональных данных»: «Персональные данные – это любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация» [22].

Указанный Федеральный закон установил критерии законности действий, связанных с обработкой персональных данных, а также пределы ограничения прав физических лиц – субъектов персональных данных в связи с обеспечением общественных интересов, безопасности государства и общества.

Следует отметить, что действие этого закона не распространяется на отношения, возникающие при организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда Российской Федерации и других архивных документов, а также при обработке персональных данных, отнесенных к сведениям, составляющим государственную тайну. Более подробно о доступе к архивным конфиденциальным документам – персональным данным изложено в разд. 4.5.

Существуют специальные категории персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни и т.д.

Биометрические персональные данные – это сведения, характеризующие физиологические особенности человека, на основе которых можно установить его личность, например дактилоскопические данные (отпечатки пальцев); информация, полученная на полиграфе (детекторе лжи), и др. Биометрические персональные данные, за некоторым исключением (например, отпечатки пальцев преступников и т.д.), могут обрабатываться только при наличии согласия в письменной форме физического лица.

Технологии обработки персональных данных. *Обработка персональных данных* – это действия (операции или технологии) с ними, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование и их уничтожение.

Использование персональных данных – действия с ними, совершаемые оператором в целях принятия решений, или иные действия, порождающие юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающие права и свободы этого субъекта или других физических лиц.

Распространение персональных данных – действия, направленные на их передачу определенному кругу лиц либо ознакомление с ними неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к ним каким-либо иным способом.

Обезличивание персональных данных – действия, в результате которых невозможно определить их принадлежность конкретному физическому лицу.

Блокирование персональных данных – временное прекращение их сбора, систематизации, накопления, использования, распространения, в том числе их передачи.

Уничтожение персональных данных – действия, в результате которых либо невозможно восстановить их содержание в АИС, либо уничтожаются материальные носители персональных данных.

Организация обработки персональных данных осуществляется оператором. Помимо организации и непосредственно обработки персональных данных, операторы определяют цели и содержание обработки. *Оператор* – это государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание их обработки.

Не допускается обработка персональных данных, избыточных по отношению к целям, заявленным при их сборе, а также объединение созданных для несовместимых между собой целей баз данных АИС.

Обработка персональных данных может осуществляться оператором только с согласия субъектов персональных данных. Однако в отдельных случаях согласия субъекта на обработку не требуется, например при обработке кадровой документации в организации, где работает этот субъект.

Хранение персональных данных должно осуществляться в форме, позволяющей определять физическое лицо, не дольше, чем этого требуют цели обработки этих данных. По достижении целей обработки или в случае утраты необходимости в достижении этих целей последние подлежат уничтожению.

Обработка персональных данных должна осуществляться при следующих двух условиях.

Первое условие: оператор может выполнять ее только с согласия субъектов персональных данных, за исключением случаев, когда обработка осуществляется:

• в целях исполнения договора, одной из сторон которого является субъект персональных данных (например, трудового договора или служебного контракта – для государственных служащих);

• для статистических или иных научных целей при условии обязательного их обезличивания – действия, в результате которых невозможно определить их принадлежность к конкретному субъекту персональных данных;

• для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, при невозможности получения согласия субъекта;

• для доставки почтовых отправлений организациями почтовой связи, для осуществления операторами электросвязи расчетов с пользователями за оказанные услуги связи, а также для рассмотрения претензий пользователей услугами связи;

• в целях профессиональной деятельности журналиста либо в целях научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

• в целях опубликования в соответствии с законодательством о государственной службе, в том числе персональных данных о замещающих государственные должности, или должности государственной гражданской службы, а также о кандидатах на выборные государственные или муниципальные должности.

Второе условие: если оператор на основании договора поручает обработку персональных данных другому лицу, существенным условием договора является обязанность обеспечения указанным лицом конфиденциальности этих данных и безопасности при их обработке.

Особенности технологий обработки персональных данных, осуществляемой без использования средств автоматизации. Обработка персональных данных, содержащихся в АИС персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как их использование, уточнение, распространение, уничтожение в отношении каждого из физических лиц – субъектов персональных данных, осуществляются при непосредственном участии человека [78].

Правила работы (обработки) с документированными персональными данными, осуществляемой без использования средств автоматизации, должны быть установлены нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами организаций – государственных и негосударственных структур и применяться с учетом изложенных требований Постановления Правительства Российской Федерации «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» [Там же].

Персональные данные при их обработке должны обособляться от иной документированной информации, в частности путем фиксации их на отдельных материальных носителях, в специальных разделах или на полях форм (бланков) документов.

При фиксации персональных данных на материальных носителях не допускается фиксация на одном носителе данных, цели обработки которых заведомо не совместимы. При обработке различных категорий персональных данных для каждой категории должен использоваться отдельный материальный носитель.

Лица, осуществляющие обработку персональных данных (в том числе сотрудники организации-оператора или лица, осуществляющие такую обработку по договору с оператором), должны быть проинформированы о факте обработки ими указанных данных, их категориях, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами государственных и негосударственных структур и локальными правовыми актами организации (при их наличии).

При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее – типовая форма), должны соблюдаться следующие условия:

- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес физического лица – субъекта персональных данных, источник их получения, сроки обработки, перечень действий, которые будут совершаться в процессе обработки этих данных, общее описание используемых оператором способов их обработки;
- типовая форма должна предусматривать поле, в котором физическое лицо при необходимости получения письменного согласия может поставить отметку о своем согласии на обработку своих персональных данных, осуществляемую без использования средств автоматизации, – на обработку персональных данных (см. разд. 4.4.1);
- типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими данными, содержащимися в документе, не нарушая прав и законных интересов других субъектов персональных данных – физических лиц;
- типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо несовместимы.

При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска физического лица на территорию, на которой находится оператор, или в иных аналогичных целях, должны соблюдаться следующие условия:

• необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена актом оператора, содержащим сведения о цели обработки персональных данных, способы фиксации и состав информации, запрашиваемой у физических лиц, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных, а также сведения о порядке пропуска на территорию, на которой находится оператор, без подтверждения подлинности персональных данных, сообщенных физическим лицом;

• копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;

• персональные данные каждого физического лица могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска его на территорию, на которой находится оператор.

При невозможности обработки персональных данных, зафиксированных на материальном носителе, который не позволяет осуществлять их обработку отдельно от других размещенных на том же носителе данных, должны быть приняты меры по обеспечению их раздельной обработки, в частности:

• при необходимости использования или распространения конкретных персональных данных отдельно от находящихся на том же материальном носителе других данных осуществляется их копирование способом, который исключает одновременное копирование персональных данных, не подлежащих распространению и использованию, и в дальнейшем используется (распространяется) эта копия;

• в случае необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель, но предварительно производится копирование сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование тех данных, которые подлежат уничтожению или блокированию.

Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может выполняться способом, исключающим дальнейшую их обработку с сохранением возможности обработки иных данных, зафиксированных на этом носителе (удаление, вымарывание).

Уточнение персональных данных производится путем обновления или изменения их на материальном носителе, а если это не допускается его техническими особенностями, то с помощью фиксации на нем сведений о вносимых изменениях либо изготовления нового носителя (документа) с уточненными персональными данными.

Обработка персональных данных должна осуществляться таким образом, чтобы в отношении каждой категории этих данных можно было определить места их хранения (материальных носителей) и установить перечень лиц, осуществляющих их обработку либо имеющих к ним доступ. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются оператором.

При обработке биометрических персональных данных**,** осуществляемой без использования средств автоматизации и вне информационных систем, для каждой их категории должен использоваться отдельный материальный носитель [79].

Материальный носитель должен обеспечивать:

• защиту от несанкционированной повторной и дополнительной записи информации после извлечения из АИС биометрических персональных данных;

• возможность доступа к персональным данным, записанным на материальный носитель оператора и лиц, уполномоченных на работу с ними;

• возможность идентификации автоматизированной информационной системы персональных данных, в которую произведена их запись, а также оператора, осуществившего такую запись;

• невозможность несанкционированного доступа к персональным данным, содержащимся на материальном носителе.

Конфиденциальность персональных данных. Операторы, обеспечивающие обработку персональных данных, и третьи лица, получающие доступ к персональным данным, обязаны соблюдать их конфиденциальность, за исключением случаев:

• обезличивания персональных данных – действий, в результате которых становится невозможным определение принадлежности персональных данных конкретному физическому лицу;

• использования общедоступных персональных данных, доступ к которым определен неограниченным кругом лиц и предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Общедоступными источниками персональных данных являются также источники, созданные в целях информационного обеспечения, например справочники, адресные книги. В них, с письменного согласия субъекта персональных данных, могут быть указаны его фамилия, имя и отчество, год и место рождения, адрес, абонентский номер и иная предоставленная им информация. В любое время эти сведения могут быть исключены из общедоступных источников персональных данных по требованию физического лица либо по решению суда или иных уполномоченных государственных органов.

Конфиденциальность персональных данных – это обязательное для соблюдения оператором или иным получившим доступ к ним лицом требование не допускать их распространения без согласия физического лица или наличия иного законного основания. В случае, если оператор на основании договора поручает обработку персональных данных другому лицу, существенным требованием договора является обязанность обеспечения указанным лицом регламентированного доступа к персональным данным, их конфиденциальности и защиты при обработке.

Федеральным законом «О персональных данных» установлен запрет на обработку персональных данных в целях продвижения товаров, работ, услуг на рынке путем установления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации без получения предварительного согласия физического лица – субъекта персональных данных.

При выявлении неправомерных действий с персональными данными в обязанности оператора входит устранение допущенных нарушений в срок, не превышающий трех рабочих дней с даты такого выявления. Если нарушения устранить невозможно, то оператор в указанный срок обязан уничтожить персональные данные. Если цель обработки персональных данных была достигнута, оператор обязан незамедлительно прекратить их обработку и уничтожить в срок, не превышающий трех рабочих дней с даты достижения цели их обработки.

О своем намерении начать обработку персональных данных оператор обязан уведомлять уполномоченный орган по защите прав субъектов персональных данных (согласно закону таким органом является федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи). Более подробно это рассмотрено в разд. 4.4.2.

В Уголовном кодексе Российской Федерации [14] (УК РФ) предусмотрена ответственность за незаконное собирание и распространение сведений о частной жизни лица, составляющих его личную и семейную тайну (ст. 137), тайну переписки, телефонных переговоров и иных сообщений (ст. 138), тайну голосования (ст. 142), тайну усыновления (ст. 155). Более подробно указанные статьи изложены в приложении 6. Юридические и физические лица, владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством за нарушение режима защиты, обработки и порядка использования этой информации.

Меры по обеспечению защиты персональных данных при их автоматизированной обработке. Оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры для защиты данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий [14].

Контроль и надзор за выполнением в АИС установленных Правительством Российской Федерации требований обеспечения безопасности персональных данных при их обработке осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности (ФСБ России) [48, 65], и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, – Федеральной службой по техническому и экспортному контролю (ФСТЭК России) [63]. Обе службы осуществляют свою деятельность в пределах их полномочий и без права ознакомления с персональными данными в обрабатываемых их АИС.

Правительство Российской Федерации установило требования и меры по защите и обеспечению безопасности персональных данных при их обработке в АИС [82], которые подробно изложены в разд. 8.3.4.

Персональные данные работника. Составной частью личной тайны являются персональные данные работника. Работодателю – владельцу персональных данных физического лица (или потенциальному владельцу, в случае оформления на работу гражданина, по каким-либо причинам не принятого на работу) эти данные необходимы для осуществления трудовых отношений. Организации, владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством за нарушение режима ее защиты, обработки, передачи и использования.

Признание тех или иных сведений конфиденциальными является прерогативой правообладателя информации. *Правообладателем информации* – персональных данных является сам гражданин, он же и определяет доступ к данной информации, необходимый для осуществления своих прав. Гражданин имеет право вступать во взаимоотношения с различными организациями. Для осуществления этих взаимоотношений гражданин – собственник информации о себе должен предоставить эту информацию организации (учреждению, предприятию), которая становится обладателем сведений о гражданине. Организация обязана защищать данную информацию. Среди документов и информации организации-работодателя, используемой ею в связи с трудовыми отношениями, особое место занимают документы о составе семьи работника, необходимые для предоставления ему гарантий, связанных с выполнением семейных обязанностей (см. далее о семейной тайне).

В настоящее время Трудовым кодексом Российской Федерации [8] определен один из видов персональных данных, а именно персональные данные работника – информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника. Соответственно, обработкой персональных данных работника (получением, хранением, комбинированием, передачей, использованием и т.д.) занимается Кадровая служба организации-работодателя. Информация о личной жизни работника, не связанная с трудовыми отношениями, в понятие персональных данных работника не входит и собирать ее работодатель не имеет права.

Личное дело также является персональными данными работника. В него включаются следующие документы:

- трудовой договор, отвечающий требованиям, установленным в Трудовом кодексе Российской Федерации (ст. 57);
- трудовая книжка работника, которая должна находиться в его личном деле в период действия трудового договора;
- приказ (распоряжение) о приеме на работу;

• приказы (распоряжения) об изменении условий трудового договора, его прекращении; приказы (распоряжения) о поощрениях и дисциплинарных взысканиях, примененных к работнику.

Персональные данные государственного гражданского служащего. В Федеральном законе «О государственной гражданской службе Российской Федерации» [30, ст. 42], а также в Указе Президента Российской Федерации «Об утверждении Положения о персональных данных государственного гражданского служащего и ведении его личного дела» [61] определены персональные данные государственного гражданского служащего (госслужащего). Этими правовыми актами также определены основные требования к порядку их защиты, обработки, хранения и передачи. Под *персональными данными государственного гражданского служащего* понимаются сведения о фактах, событиях и обстоятельствах жизни госслужащего служащего, позволяющие идентифицировать его личность и содержащиеся в его личном деле либо подлежащие включению в личное дело.

На основе персональных данных госслужащего формируются и ведутся, в том числе на электронных носителях, реестры гражданских госслужащих, которые, в свою очередь, являются информацией конфиденциального характера.

Акты гражданского состояния – действия граждан или события, влияющие на возникновение, изменение или прекращение прав и обязанностей, а также характеризующие правовое состояние граждан.

Государственная регистрация актов гражданского состояния производится органами записи актов гражданского состояния, образованными органами государственной власти субъектов Российской Федерации (далее – органы записи актов гражданского состояния). Государственной регистрации в порядке, установленном Федеральным законом «Об актах гражданского состояния», подлежат следующие акты: рождение, заключение брака, расторжение брака, усыновление (удочерение), установление отцовства, перемена имени и смерть [43, ст. 3, 12, 47].

Совершенные по религиозным обрядам до образования или восстановления органов записи этих актов гражданского состояния приравниваются к актам, совершенным в органах их записи в соответствии с действовавшим на момент их совершения законодательством, и не требуют последующей государственной регистрации.

Сведения, ставшие известными работнику органа записи актов гражданского состояния в связи с его государственной регистрацией, являются персональными данными, относятся к категории конфиденциальной информации, имеют ограниченный доступ и разглашению не подлежат.

Руководитель органа записи актов гражданского состояния должен сообщить в органы социальной защиты населения и налоговый орган, осуществляющий государственную регистрацию юридических лиц и индивидуальных предпринимателей, а также в органы Пенсионного фонда Российской Федерации и Фонда социального страхования Российской Федерации сведения о государственной регистрации смерти. Также руководитель обязан сообщить сведения о государственной регистрации акта гражданского состояния по запросу суда (судьи), органов прокуратуры, дознания или следствия либо Уполномоченного по правам человека в Российской Федерации и в других случаях, установленных федеральными законами.

Семейная тайна – сведения, касающиеся семьи и по моральным соображениям скрываемые от посторонних семьей, под которой в социальном аспекте понимается союз лиц, основанный на браке, родстве, принятии детей на воспитание, характеризующийся общностью жизни, интересов, а в юридическом смысле – круг лиц, связанных правами и обязанностями, вытекающими из брака, родства, усыновления или иной формы принятия детей на воспитание. Эта информация и документы составляют другой вид конфиденциальной информации, которая тесно связана с личной тайной, но не тождественна ей по составу защищаемой информации. Семейную тайну возможно определить так: это информация ограниченного доступа нескольких физических лиц, ограниченная членами семьи (составом семьи).

Семейная и личная тайны тесно связаны между собой и во многом совпадают. Различия между ними усматриваются в одном: если личная тайна непосредственно касается интересов лишь конкретного индивидуума, то семейная тайна затрагивает интересы нескольких лиц, находящихся друг с другом в отношениях, регулируемых Семейным кодексом Российской Федерации [16].

Тайна усыновления – сведения о факте усыновления ребенка, информация об отказе от него действительных родителей, иных обстоятельствах усыновления. Предание этих сведений огласке, т.е. предоставление их третьим лицам, которым не было известно о факте усыновления, означает разглашение тайны усыновления. Тайну усыновления возможно отнести к семейной тайне. Тайна усыновления охраняется законом [43, ст. 3, 12, 47]. Работники органа записи актов гражданского состояния не вправе без согласия усыновителей (усыновителя) сообщать какие-либо сведения об усыновлении и выдавать документы, из содержания которых видно, что усыновители (усыновитель) не являются родителями (одним из родителей) усыновленного ребенка.

Тайна голосования – зафиксированные в бюллетене для голосования и раскрывающие отношение гражданина к выбору того или иного кандидата [35, ст. 7].

Тайна исповеди охраняется законом. Священнослужитель не может быть привлечен к ответственности за отказ от дачи показаний по обстоятельствам, которые стали известны ему из исповеди. Никто не обязан сообщать о своем отношении к религии и не может подвергаться принуждению при определении своего отношения к религии, к исповеданию или отказу от исповедания религии, к участию или неучастию в богослужениях, других религиозных обрядах и церемониях, в деятельности религиозных объединений, в обучении религии. Запрещается вовлечение малолетних в религиозные объединения, а также обучение малолетних религии вопреки их воле и без согласия их родителей или лиц, их заменяющих [44, ст. 3, п. 7].

Партийная тайна – это «информация о членах политической партии, представляемая для сведения в уполномоченные органы, относится к информации с ограниченным доступом. Разглашение информации без согласия соответствующих членов политической партии влечет за собой ответственность, установленную законодательством Российской Федерации» [41, ст. 19, п. 6].

Таким образом, анализ нормативных источников позволяет нам предложить следующую схему информации ограниченного доступа, составляющей персональные данные, выделить характеризующие их конкретные признаки и сформулировать их определение.

С позиций научной дисциплины как документоведения персональные данные гражданина – это конфиденциальная документированная информация, составляющая следующие виды тайн: частной жизни, семейной, голосования, исповеди, партийной, а также персональные данные гражданина как работника, как государственного служащего (кадровая документация о нем), как жителя или владельца недвижимости и т.д.

В ряде случаев персональные данные (личная тайна) составляют врачебную, адвокатскую, нотариальную, налоговую тайны, тайну почтово-телеграфных отправлений и др., которые одновременно считаются служебной и профессиональной тайнами (см. разд. 1.4, 1.5). Нарушение установленного Федеральным законом «О персональных данных» порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) влечет за собой административную ответственность в соответствии со ст. 13.1 Кодекса Российской Федерации об административных нарушениях (см. приложение 6).

Учитывая изложенное, определение персональных данных (тайны частной жизни) можно сформулировать следующим образом: *персональные данные физического лица (гражданина) или личная тайна (тайна частной жизни)* – это конфиденциальная документированная информация, незаконное собирание или распространение которой причиняет вред правам и законным интересам этого лица и предоставляет ему право на защиту в соответствии с законодательством Российской Федерации.

Следующий комплекс информации ограниченного доступа, в соответствии с Перечнем сведений конфиденциального характера, утвержденным Указом Президента Российской Федерации [68], – сведения, составляющие тайну следствия и судопроизводства, а также сведения о защищаемых лицах и мерах государственной защиты.

1.3. Тайна следствия и судопроизводства

Тайна следствия связана с интересами законного производства предварительного расследования по уголовным и гражданским делам. В силу Уголовного процессуального кодекса Российской Федерации [10, ст. 161] (УПК РФ) данные предварительного расследования не подлежат разглашению. Такая информация может касаться как характера производимых следственных действий, так и доказательной базы, перспектив расследования, круга лиц, участвующих в расследовании.

Следователь или дознаватель должен предупредить участников уголовного судопроизводства о недопустимости разглашения без соответствующего разрешения ставшей им известной информации предварительного расследования, о чем у них берется подписка с предупреждением об ответственности. Данные предварительного расследования могут быть преданы гласности лишь с разрешения следователя, дознавателя и только в том объеме, в каком ими будет признано это допустимым, если разглашение не противоречит интересам предварительного расследования и не связано с нарушением прав и законных интересов участников уголовного судопроизводства.

Разглашение сведений о частной жизни участников уголовного судопроизводства без их согласия не допускается, ибо они относятся к персональным данным (см. разд. 1.2).

Важно отметить, что в законе отсутствует перечень сведений, составляющих следственную тайну. Это означает, что прокурор, следователь или лицо, производящие дознание, могут по своему усмотрению устанавливать, какая информация о предварительном расследовании может быть специально охраняемой, а какая – нет.

В ряде случаев информация, составляющая тайну следствия и судопроизводства, содержит государственную, коммерческую, банковскую и иные тайны, охраняемые законами. УПК РФ определяет, какие обстоятельства исследуются на закрытом судебном заседании [Там же, ст. 241]. Разбирательство дел во всех судах открытое, за исключением случаев, когда это противоречит интересам защиты государственной тайны или иной охраняемой федеральным законом.

Закрытое судебное разбирательство, кроме того, допускается по мотивированному определению суда или постановлению судьи по делам о преступлениях лиц, не достигших шестнадцатилетнего возраста, по делам о половых преступлениях, а также по другим делам в целях предотвращения разглашения информации об интимных сторонах жизни участвующих в деле лиц. Приговоры судов во всех случаях провозглашаются публично.

Федеральным законом «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства» [28, ст. 9] определена необходимость обеспечения конфиденциальности сведений о защищаемом лице. По решению органа, осуществляющего меры безопасности, может быть наложен запрет на выдачу сведений о защищаемом лице из государственных и иных информационно-справочных фондов, а также могут быть изменены номера его телефонов и государственные регистрационные знаки используемых им или принадлежащих ему транспортных средств.

В исключительных случаях, связанных с производством по другому уголовному либо гражданскому делу, сведения о защищаемом лице могут быть представлены в органы предварительного расследования, прокуратуру или суд на основании письменного запроса прокурора или суда (судьи) с разрешения органа, принявшего решение об осуществлении государственной защиты.

Следующий комплекс информации, которая рассматривается в качестве тайны, относится к государственным и общественным интересам. Здесь, в первую очередь, рассматривается вопрос о служебной тайне.

1.4. Служебная тайна

Как ранее говорилось, в действующем законодательстве не определено однозначно понятие служебной тайны. Проект Федерального закона «О служебной тайне» рассматривался в Государственной Думе с 2004 г., но до настоящего времени не принят.

Необходимость правового регулирования института служебной тайны вызвана рядом причин, в их числе: отсутствие в законодательстве единого подхода к соответствующей категории документированной информации ограниченного доступа; многочисленные примеры незаконного распространения (продажи) информации, аккумулируемой в органах государственной власти и относящейся либо к личности, либо к деятельности хозяйствующих субъектов; ограничения на распространение информации, накладываемые по своему усмотрению руководителями органов государственной власти и государственными (муниципальными) служащими на предоставление информации гражданам, общественным организациям, средствам массовой информации.

Вместе с тем для служебной тайны как системы защиты сведений появились и другие сферы применения. В частности, ряд органов исполнительной власти в силу выполняемых ими функций получает от различных субъектов значительное количество конфиденциальной информации (налоговые, антимонопольные, правоохранительные органы и т.д.). Речь идет о сведениях, составляющих коммерческую и банковскую тайну, персональные данные.

В деятельности государственных структур, помимо всего указанного, образуется значительное количество внутрисистемной информации, которая в силу законодательных ограничений не может быть отнесена к государственной тайне, однако и не может быть свободно распространяемой.

В качестве примера можно привести комплекс мер, предпринимаемых для обеспечения защиты судей, иных работников правоохранительных органов, планы Минфина России и Банка России, связанные с изменениями курса национальной валюты, планы использования подразделений правоохранительных органов для осуществления контртеррористической и иной оперативно-служебной деятельности, а также информацию разнообразного характера, которая в настоящее время не имеет адекватной правовой защиты.

Единственный нормативный акт, регулирующий данную группу правоотношений, – «Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти», утвержденное постановлением Правительства Российской Федерации от 03.11.1994 № 1233 (ДСП). Данное Положение распространяется только на деятельность федеральных органов исполнительной власти, хотя образование и поступление аналогичных сведений характерны для любых органов как государственной власти, так и органов местного самоуправления.

Многие условия, определяющие порядок отнесения сведений к категории служебной информации, не установлены в Положении, а определяются руководителями федеральных органов исполнительной власти, что нельзя признать правильным, поскольку введение ограничений на доступ к информации должно устанавливаться только федеральным законом. На уровне Положения выстроить долговременную и стабильную систему защиты информации, имеющей продолжительный срок хранения, невозможно.

Несмотря на практически полное отсутствие нормативного регулирования в сфере отнесения информации к служебной тайне, ее защиты и установления санкций за противоправное распространение такой информации, данная категория присутствует в большом количестве федеральных законов (около 40), в том числе в федеральных законах: «Об основах государственной службы Российской Федерации», «О Правительстве Российской Федерации», «О службе в таможенных органах Российской Федерации», «О Центральном банке Российской Федерации (Банке России)», «Об основах муниципальной службы Российской Федерации», «О рынке ценных бумаг» и др.

Защита служебной информации не имеет в законодательстве однозначного отражения. По-разному решается в законодательстве вопрос о структуре конфиденциальной информации и соотношении различных видов тайн.

На электронных рынках России и с помощью рассылки сообщений электронной почты бесконтрольно распространяются CD, содержащие базы данных с информацией о персональных данных и организациях. Например, базы данных: «Таможня», ГИБДД, БТИ (Бюро технической инвентаризации), «Прописка», «Внешнеэкономическая деятельность», ЕГРП (Единая государственная регистрация предприятий), «Собственники квартир», «Доходы физических лиц», «Картотека МВД» (судимости и др.), ОВИР (зарегистрированные паспорта) и ряд других баз данных.

По данным ряда исследований, большинство зарубежных стран используют систему ограничения в доступе к информации с таким (или схожим) названием для защиты внутрисистемной информации в своих государственных администрациях. К таким странам, в частности, относятся Испания, Германия, Франция и США. В этих странах за неправомерное распространение таких сведений установлена уголовная ответственность.

Должностные лица, работники различных учреждений и организаций в силу служебных обязанностей не должны давать информацию, которая подпадает под категорию служебной тайны. Сведения,

содержащие служебную тайну, могут относиться к гражданину, его жизни и деятельности (см. разд. 1.2), а могут затрагивать деятельность госучреждения, предприятия, организации.

Для работников соответствующих предприятий, учреждений и организаций сведения о тайне усыновления, вкладах граждан в различного рода банки, характере заболеваний пациентов и т.д. представляют собой служебную либо профессиональную, например, врачебную тайну, обусловленную выполнением ими своих трудовых и служебных функций (см. разд. 1.5). Служебная тайна не подлежит разглашению, кроме тех случаев, когда те или иные сведения запрашиваются правоохранительными органами.

Согласно Указу Президента Российской Федерации «Об утверждении перечня сведений конфиденциального характера» разница между служебной и коммерческой тайнами состоит в том, что коммерческая тайна – это информация, связанная с коммерческой деятельностью, а служебная тайна – это служебная информация, доступ к которой ограничен государственными структурами.

По общему смыслу понятия «служебная тайна» можно предположить то, что ее носителями должны быть субъекты, которые относятся к категории служащих. Таким образом, можно утверждать, что потенциальными носителями служебной тайны являются как минимум все служащие, которые работают в государственных органах, органах законодательной, исполнительной и судебной властей, а также в подведомственных им предприятиях, учреждениях и организациях.

Лица, получившие незаконными методами информацию, которая составляет служебную тайну, обязаны возместить причиненные убытки. Такая же обязанность возлагается на работников или служащих, разгласивших служебную тайну вопреки трудовому договору или служебному контракту, в том числе контракту, и на контрагентов, сделавших это вопреки гражданско-правовому договору.

Между юридическими лицами, а также между юридическими и физическими лицами могут складываться отношения, при которых нежелательно разглашение определенной информации. Иными словами, они должны сохраняться в тайне. Нераспространение физическим лицом информации о другом физическом лице достигается на основе взаимной договоренности, а также нравственного поведения лица, знающего ту или иную информацию о другом лице.

В государственных и негосударственных структурах существует определенный порядок для выполнения целей, функций и задач конкретной организации: система планирования, отчетности, контроля, технологии документооборота и т.д. Информацию такого рода можно

отнести к служебной тайне или секретам производства (см. разд. 1.7). Перечень данной информации устанавливается руководителем организации – обладателя информации. Информацией, относящейся к служебной тайне, могут обладать любые организации независимо от организационно-правовой формы, формы собственности и видов деятельности. Примером служебной тайны является налоговая.

В соответствии с Налоговым кодексом Российской Федерации [12, ст. 102] налоговую тайну составляют любые полученные налоговым органом, а также органами внутренних дел, государственного внебюджетного фонда и таможенным органом сведения о налогоплательщике. Информация о налогоплательщике, если он является физическим лицом, – это одновременно его личная тайна, т.е. относится к персональным данным. Исключение составляет информация, которая не может быть налоговой тайной (см. приложение 1).

Налоговая тайна не подлежит разглашению налоговыми органами, органами внутренних дел, государственных внебюджетных фондов и таможенными, их должностными лицами и привлекаемыми специалистами, экспертами, за исключением случаев, предусмотренных федеральным законом.

Сведения, поступившие в налоговые органы, органы внутренних дел, государственных внебюджетных фондов или таможенные, составляющие налоговую тайну, имеют специальный режим хранения и доступа (см. разд. 4.2; 7.4).

Доступ к сведениям, составляющим налоговую тайну, имеют должностные лица, определяемые федеральными органами исполнительной власти, уполномоченными по контролю и надзору в области налогов и сборов, внутренних дел, таможенного дела.

Утрата документов, содержащих налоговую тайну, либо разглашение сведений, составляющих налоговую тайну, влечет ответственность, предусмотренную ст. 183 УК РФ (см. приложение 6).

К разглашению налоговой тайны относится, в частности, использование или передача другому лицу секрета производства (ноу-хау), служебного секрета производства или коммерческой тайны налогоплательщика – юридического и физического лица, а также персональных данных налогоплательщика, т.е. информации, которая стала известна должностному лицу налогового органа, а также органов внутренних дел, государственного внебюджетного фонда или таможенного, привлеченному специалисту или эксперту при исполнении ими своих обязанностей.

В данном случае налоговую тайну можно отнести к информации ограниченного доступа, составляющей служебную, профессиональную и коммерческую тайны, персональные данные, секрет производства (см. разд. 1.2; 1.5–1.7).

Поступившая в налоговые органы информация, составляющая налоговую тайну, имеет специальный режим хранения и доступа и, соответственно, технологии ее защиты. Доступ к информации, составляющей налоговую тайну, имеют должностные лица по перечням, которые определены Федеральной налоговой службой России (ФНС России).

Положением о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, утвержденным постановлением Правительства Российской Федерации от 03.11.1994 № 1233, к служебной информации ограниченного распространения отнесена несекретная информация, касающаяся деятельности организаций, <...> ограничения на распространение информации диктуются служебной необходимостью [110].

Положение определяет общий порядок обращения с документами и другими материальными носителями информации – документами, содержащими служебную информацию ограниченного распространения в федеральных органах исполнительной власти, а также на подведомственных им предприятиях, в учреждениях и организациях. Требования Положения распространяются на порядок обращения с иными материальными носителями служебной информации ограниченного распространения (фото-, кино-, видео- и аудиопленки, машинные носители информации и др.).

Положением определен перечень информации, в соответствии с которым служебная информации не может быть ограниченного распространения (см. приложение 1). Руководители федеральных органов исполнительной власти в пределах своей компетенции определяют:

- категории должностных лиц, уполномоченных относить служебную информацию к разряду ограниченного распространения;
- порядок передачи служебной информации ограниченного распространения другим органам и организациям;
- порядок снятия пометки: «для служебного пользования» с носителей информации ограниченного распространения;
- организацию защиты служебной информации ограниченного распространения.

Должностные лица, принявшие решение об отнесении служебной информации к разряду ограниченного распространения, несут персональную ответственность за обоснованность принятого решения и за соблюдение ограничений, в соответствии с которыми служебная информация не может быть ограниченного распространения. Служебная информация без санкции соответствующего должност-

ного лица не подлежит разглашению (распространению). За разглашение служебной информации ограниченного распространения, а также нарушение порядка обращения с документами, содержащими такую информацию, государственный служащий (работник организации) может быть привлечен к дисциплинарной или иной предусмотренной законодательством ответственности (см. приложение 6).

Положения об обязанностях по неразглашению служебной информации ограниченного распространения должны быть включены также в государственные контракты, трудовые и иные договоры, заключаемые государственными органами, органами местного самоуправления или иными организациями, обладающими данной информацией [219]. Обязанности по неразглашению сведений и информации ограниченного распространения возникают:

- у должностных лиц и иных работников государственных органов и органов местного самоуправления, подведомственных им организаций – с момента их приема на работу, если не установлен особый порядок допуска к сведениям;
- у работников иных организаций, иных лиц, осуществляющих работы по государственному контракту или трудовому договору в органах и организациях, – с момента заключения государственного контракта, иного договора с соответствующим органом или организацией;
- у лиц, получивших сведения ограниченного распространения, – с момента получения таких сведений.

В случае ликвидации федерального органа исполнительной власти (организации) решение о дальнейшем использовании служебной информации ограниченного распространения принимает ликвидационная комиссия. Срок исполнения обязанностей по неразглашению сведений ограниченного распространения устанавливается в положениях о порядке доступа к сведениям, составляющим служебную тайну (см. гл. 4). Срок не может быть ограничен, если такие сведения были получены государственными органами и органами местного самоуправления, а равно подведомственными им организациями в процессе осуществления их деятельности в соответствии с установленной компетенцией и если такие сведения составляют охраняемую законом информацию ограниченного доступа иных лиц.

Перечень сведений о деятельности Правительства Российской Федерации и федеральных органов исполнительной власти, обязательных для размещения в Интернете, утвержден Постановлением Правительства Российской Федерации [95] и является перечнем ин-

формации, которую нельзя относить к конфиденциальной (см. приложение 1). В субъекте Российской Федерации – Москве утвержден Перечень категорий организаций и предприятий города Москвы, для которых создание и ведение информационных ресурсов о своей деятельности является обязательным, и Перечень сведений о деятельности Правительства Москвы и комплексов городского управления, подлежащих обязательному размещению в общедоступных информационных ресурсах в сети Интернет.

Определение понятий «служебная тайна» и «персональные данные», вероятно, должно распространяться на всю конфиденциальную информацию, циркулирующую не только в государственных структурах, подведомственных им предприятиях, учреждениях и организациях, но и в негосударственных структурах, включая коммерческие организации.

В соответствии с Постановлением Правительства Российской Федерации «О подписании Соглашения между Правительством Российской Федерации и Правительством Итальянской Республики о взаимном обеспечении сохранности засекреченных сведений» [97], гриф секретности (конфиденциальности) «Для служебного пользования» означает, что это несекретные сведения, касающиеся деятельности предприятий, учреждений и организаций, содержащие служебную информацию [301]. В этом смысле несекретная информация, составляющая служебную тайну, – это конфиденциальная информация учреждения, предприятия, организации вне зависимости от организационно-правовой формы и формы собственности. Соответственно, служебная тайна может быть также у негосударственных структур и иметь соответствующую отметку «Для служебного пользования». Но для этого необходимо составить перечень информации, составляющей служебную тайну, который бы входил как подраздел в Перечень конфиденциальной информации, составляющей коммерческую тайну, секрет производства (ноу-хау) и служебный секрет производства организации (см. приложение 2).

Более подробно определение степени ограничения доступа к документам и использование отметки конфиденциальности при оформлении документов рассматривается в разд. 2.2.

Сведения, относящиеся к служебной информации, не являются обычно предметом самостоятельных сделок, однако их разглашение может причинить имущественный ущерб организации и вред ее деловой репутации. Как видно из примеров, служебная тайна не является синонимом государственной тай-

ны, однако ее правовой режим устанавливается государственными и негосударственными структурами – обладателями информации [222].

К служебной тайне, за исключением сведений, составляющих государственную тайну, относится информация о деятельности государственных органов и их служащих, представляющая государственный интерес, а также иная информация ограниченного доступа, составляющая частную, коммерческую тайну субъекта, полученная государственным органом в пределах своей компетенции для выполнения возложенных на него функций. Следовательно, информация может являться служебной тайной, если она отвечает следующим требованиям:

- отнесена федеральным законом к служебной информации о деятельности государственных органов, доступ к которой ограничен по закону или в силу служебной необходимости;
- является конфиденциальной информацией другого лица (коммерческая тайна, банковская тайна, секрет производства (ноу-хау), служебный секрет производства, персональные данные);
- не является государственной тайной и не попадает под перечень сведений, составляющих государственную тайну;
- получена представителем государственного органа или органа местного самоуправления только в силу исполнения обязанностей по службе в случаях и в порядке, установленных федеральным законодательством, и имеет действительную или потенциальную ценность в силу неизвестности ее третьим лицам.

Сопоставление и анализ норм права позволяют предложить обобщающее определение служебной тайны.

Служебная тайна – это охраняемая законом информация ограниченного доступа о деятельности государственных и негосударственных структур, доступ к которой ограничен в силу служебной необходимости, за исключением информации, составляющей государственную тайну, а также информация ограниченного распространения, ставшая известной в государственных и негосударственных структурах на законном основании, для исполнения служебных обязанностей, имеющая действительную или потенциальную ценность в силу неизвестности ее третьим лицам. Обладатель информации, составляющей служебную тайну, принимает меры к ее конфиденциальности, незаконному ее получению или разглашению и предоставляет ему право на защиту и охрану в соответствии с законодательством Российской Федерации.

1.5. Профессиональная тайна

Федеральным законом «Об информации...» определено, что «информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации» [23, ст. 9, п. 5].

Информация, составляющая профессиональную тайну, может быть предоставлена третьим лицам в соответствии с федеральными законами и (или) по решению суда. Срок исполнения обязанностей по соблюдению конфиденциальности информации, составляющей профессиональную тайну, может быть ограничен только с согласия гражданина (физического лица – субъекта персональных данных), предоставившего такую информацию о себе (см. разд. 1.2).

В соответствии с признаком профессиональной принадлежности из действующего законодательства можно выделить такие виды профессиональных тайн, как: врачебная, адвокатская, аудиторская, нотариальная, тайна переписки, телефонных и иных переговоров, тайна страхования и ряд других [68, п. 4]. Например, в содержание адвокатской тайны входят сведения, сообщенные адвокату гражданином в связи с оказанием ему юридической помощи [36, ст. 8]. Кредитные организации, например коммерческие банки, гарантируют тайну операций, счетов и вкладов своих клиентов и корреспондентов [55, ст. 26]. Нотариальная тайна – это сведения, доверенные нотариусу в связи с совершением нотариальных действий [20, ст. 5, 16].

Доступ к информации, связанной с профессиональной деятельностью, ограничен в соответствии с Конституцией Российской Федерации и соответствующими федеральными законами. Рассмотрим более подробно некоторые виды профессиональной тайны.

Тайна связи. В соответствии с Федеральным законом «О почтовой связи» [42, ст. 14], «информация об адресных данных пользователей услуг почтовой связи, о почтовых отправлениях, почтовых переводах денежных средств, телеграфных и иных сообщениях, входящих в сферу деятельности операторов почтовой связи, а также сами эти почтовые отправления, переводимые денежные средства, телеграфные и другие сообщения являются тайной связи и могут выдаваться только отправителям (адресатам) или их представителям».

Данное утверждение также можно отнести к профессиональной деятельности почтовых и других операторов связи. В этом случае персональные данные адресата (отправителя) становятся профессиональной тайной или служебной тайной оператора почтовой связи. Должностные

лица, работники организаций почтовой связи, допустившие нарушения указанных положений, привлекаются к ответственности в порядке, установленном в УК РФ, ст. 138 (см. приложение 6).

То же прописано в Федеральном законе «О связи»:

«1. Сведения об абонентах и оказываемых им услугах связи, ставшие известными операторам связи в силу исполнения договора об оказании услуг связи, являются конфиденциальной информацией и подлежат защите в соответствии с законодательством. К сведениям об абонентах относятся фамилия, имя, отчество или псевдоним абонента-гражданина, наименование (фирменное наименование) абонента – юридического лица, фамилия, имя, отчество руководителя и работников этого юридического лица, а также адрес абонента или адрес установки оконечного оборудования, абонентские номера и другие данные, позволяющие идентифицировать абонента или его оконечное оборудование, сведения баз данных систем расчета за оказанные услуги связи, в том числе о соединениях, трафике и платежах абонента.

2. Операторы связи вправе использовать созданные ими базы данных об абонентах для осуществления информационно-справочного обслуживания, в том числе для подготовки и распространения информации различными способами, в частности на магнитных носителях и с использованием средств телекоммуникаций» [32, ст. 53].

При подготовке данных для информационно-справочного обслуживания могут быть использованы только фамилия, имя, отчество абонента-гражданина и его абонентский номер, наименование (фирменное наименование) абонента – юридического лица, указанные ими абонентские номера и адреса установки оконечного оборудования.

Информация об абонентах-гражданах без их согласия в письменной форме не может включаться в данные для информационно-справочного обслуживания и использоваться для оказания справочных и иных информационных услуг оператором связи или третьими лицами. Предоставление третьим лицам сведений об абонентах-гражданах может осуществляться только с согласия в письменной форме абонентов. Операторы связи обязаны обеспечить соблюдение тайны связи или, как уже говорилось, личной тайны абонента. Осмотр почтовых отправлений лицами, не являющимися уполномоченными работниками оператора связи, вскрытие почтовых отправлений, осмотр вложений, ознакомление с информацией и документальной корреспонденцией, передаваемыми по сетям электросвязи и сетям почтовой связи, осуществляются только на основании решения суда.

Информация о передаваемых по сетям электросвязи и почтовой связи сообщениях и т.д., а также сами эти сообщения, почтовые отправления и переводимые денежные средства могут выдаваться только отправителям и получателям или их уполномоченным представителям.

В соответствии с Федеральным законом «Об оперативно-розыскной деятельности», разрешается проводить оперативно-розыскные мероприятия, связанные с контролем почтовых отправлений, телеграфных и иных сообщений, прослушиванием телефонных переговоров с подключением к станционной аппаратуре предприятий, учреждений и организаций независимо от организационно-правовых форм и форм собственности, физических и юридических лиц, органами Федеральной службы безопасности и органами внутренних дел в порядке, определяемом межведомственными нормативными актами или соглашениями между органами, осуществляющими оперативно-розыскную деятельность [47].

Проведение оперативно-розыскных мероприятий, которые ограничивают конституционные права человека и гражданина на тайну переписки и т.д., допускается на основании судебного решения (ранее – при санкции прокуратуры).

Врачебная тайна. Основы законодательства Российской Федерации об охране здоровья граждан определяют врачебную тайну так: «Врачебная тайна: информация о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иные сведения, полученные при его обследовании и лечении» [19, ст. 61]. В содержание врачебной тайны входит следующая информация:

- о примененных методах лечения и их эффективности;
- о лице, обратившемся за помощью, его физических, психических недостатках, привычках, наклонностях, интимных связях и т.д., т.е. персональные данные пациента и его биометрические персональные данные (см. разд. 1.1.2);
- о семье больного и укладе жизни в доме и на работе (семейная тайна).

Исходя из этого информацию, относящуюся к врачебной тайне, можно разделить на две группы:

1) медицинские данные или биометрические персональные данные;

2) информация о частной жизни больного, полученная в процессе исполнения профессиональных (служебных) врачебных обязанностей.

Гражданину должна быть подтверждена гарантия конфиденциальности передаваемой им информации.

Не допускается разглашение информации, составляющей врачебную тайну, лицами, которым она стала известна при обучении, исполнении профессиональных, служебных и иных обязанностей. С согласия гражданина или его законного представителя допускается передача информации, составляющей врачебную тайну, другим

гражданам, в том числе должностным лицам, в интересах обследования и лечения пациента, для проведения научных исследований, публикации в научной литературе, использования этих сведений в учебном процессе и в иных целях.

Лица, которым в установленном законом порядке переданы сведения, составляющие врачебную тайну, наравне с медицинскими и фармацевтическими работниками с учетом причиненного гражданину ущерба несут в соответствии с законодательством юридическую ответственность за разглашение врачебной тайны. В УК РФ нет конкретных статей, предусматривающих ответственность за разглашение врачебной тайны, но это не значит, что это действие ненаказуемое. Согласно ст. 137 УК РФ нарушение неприкосновенности частной жизни, разглашение врачебной тайны наказуемо (см. приложение 6).

В случае разглашения врачебной тайны другие лица, получившие информацию о гражданине, больном, несут ответственность за злоупотребление должностными полномочиями и их превышение.

Аудиторская тайна. В соответствии с Федеральным законом «Об аудиторской деятельности» аудиторские организации и индивидуальные аудиторы обязаны хранить тайну об операциях аудируемых лиц и лиц, которым оказывались сопутствующие аудиту услуги [40, ст. 8]. Аудиторские организации и индивидуальные аудиторы обязаны обеспечивать сохранность информации и документов, получаемых и (или) составляемых ими при осуществлении аудиторской деятельности, и не вправе передавать эту информацию (документы) или их копии третьим лицам либо разглашать их без письменного согласия предприятий, организаций, в отношении которых осуществлялся аудит, и оказывались сопутствующие аудиту услуги. Федеральный орган исполнительной власти, осуществляющий государственное регулирование аудиторской деятельности, и иные лица, получившие доступ к информации, составляющей аудиторскую тайну, обязаны сохранять конфиденциальность в отношении такой информации.

Журналистская тайна. Среди разновидностей профессиональной тайны существует также такое понятие, как журналистская, или редакционная тайна.

Не допускается использование средств массовой информации в целях совершения уголовно наказуемых деяний, для разглашения сведений, составляющих государственную или иную специально охраняемую законом тайну, для распространения материалов, содержащих публичные призывы к осуществлению террористической деятельности или публично оправдывающих терроризм, других экстремистских материалов, а также материалов, пропагандирующих порнографию, культ насилия и жестокости [53, ст. 4].

Редакция не вправе разглашать в распространяемых сообщениях и материалах сведения, предоставленные гражданином, субъектом персональных сведений с условием сохранения их в тайне. Также редакция обязана сохранять в тайне источник информации и не вправе называть лицо, предоставившее сведения с условием неразглашения его имени, за исключением случая, когда соответствующее требование поступило от суда в связи с находящимся в его производстве делом [53, ст. 41]. Это положение касается персональных данных гражданина, которые рассмотрены в разд. 1.2.

Профессиональная тайна характеризуется конкретными признаками. Первым признаком отнесения информации к данному виду тайны выступает профессия, в силу которой лицу доверяется или становится известной информация ограниченного доступа. Другой общий признак – информация доверяется лицу, исполняющему профессиональные обязанности, добровольно по выбору владельца этой информации и, как правило, затрагивает частную жизнь последнего. Третий признак – лицо, которому в силу его профессии была доверена информация, обязано по закону обеспечить ее сохранность как профессиональной тайны под страхом наступления ответственности в соответствии с действующим законодательством.

Таким образом, *профессиональная тайна* – это охраняемая законом информация ограниченного доступа, за исключением информации, составляющей государственную тайну, доверенная или ставшая известной лицу исключительно в силу исполнения им своих профессиональных обязанностей, не связанных с государственной или муниципальной службой, незаконное получение или распространение которой может повлечь за собой вред правам и законным интересам другого лица, доверившего эту информацию.

1.6. Коммерческая тайна

Точно назвать дату появления в человеческом обществе коммерческой тайны невозможно. Однако бесспорен тот факт, что еще в древности мастера своего дела, а также торговые люди надежно хранили секреты своей профессии, причем так надежно, что даже для нашего поколения некоторые технологии прошлого еще остаются тайной.

Первое официальное нормативно-правовое закрепление понятия «коммерческая тайна» состоялось после принятия Закона СССР «О предприятиях в СССР» [56]*. Дополнением к указан-

* Прекратил действие с 1 января 1991 г.

ному определению понятия явилось принятие Закона РСФСР «О предприятиях и предпринимательской деятельности» [54]*, в котором было указано следующее: «Предприятие имеет право не предоставлять информацию, содержащую коммерческую тайну. Перечень сведений, составляющих коммерческую тайну, определяется руководителем предприятия. Перечень сведений, которые не могут составлять коммерческую тайну, определяется Советом Министров РСФСР».

До 2004 г. термин «коммерческая тайна» упоминался в нескольких десятках российских законов, однако содержание этого понятия было дано только в ст. 139 ГК РФ (статья утратила силу). В этой статье не проводится различие между служебной и коммерческой тайнами, хотя в жизни употребляются оба этих понятия. Коммерческая тайна связана с интересами обеспечения законной предпринимательской деятельности.

Федеральный закон «О коммерческой тайне» определил понятие «коммерческая тайна» [29, ст. 3]. Однако с принятием Четвертой части ГК РФ закон претерпел значительные изменения. В настоящее время федеральный закон регулирует отношения, связанные с установлением, изменением и прекращением режима коммерческой тайны в отношении информации, составляющей секрет производства (ноу-хау), о которых более подробно изложено в разд. 1.7.

В новой редакции от 24.07.2007 Федерального закона определено: «Коммерческая тайна – режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Информация, составляющая коммерческую тайну (секрет производства), – сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны» [Там же, п. 2].

---

* Утратил силу 21 марта 2002 г. с принятием Федерального закона «О приведении законодательных актов в соответствие с Федеральным законом “О государственной регистрации юридических лиц”».

Перечень информации, которая не может составлять коммерческую тайну, состоит из 11 позиций (более подробный перечень дан в приложении 1).

По мотивированному требованию органа государственной власти предприятие, организация должны предоставлять ему на безвозмездной основе информацию, в том числе составляющую коммерческую тайну. Мотивированное требование должно быть составлено в письменной форме, подписано уполномоченным должностным лицом, содержать указание цели и правового основания затребования информации, составляющей коммерческую тайну, и срок предоставления этой информации. В случае отказа обладателя информации предоставить ее органам государственной власти они вправе затребовать эту информацию только в судебном порядке.

За невыполнение обладателем информации, составляющей коммерческую тайну, невыполнение законных требований органов государственной власти, иных государственных органов, органов местного самоуправления о предоставлении им информации, составляющей коммерческую тайну, а равно воспрепятствование получению должностными лицами этих органов указанной информации влечет за собой ответственность в соответствии с законодательством Российской Федерации [Там же, ст. 15].

Одной из мер по установлению режима охраны и установлению конфиденциальности коммерческой тайны является нанесение на материальные носители (документы) грифа «Коммерческая тайна» (более подробно о нанесении грифа на документы см. в разд. 2.2).

Возможно выделить конкретные признаки, характеризующие коммерческую тайну, и сформулировать определение ее понятия:

1. Коммерческая тайна – это документированная информация ограниченного доступа, составляющая секрет производства (ноу-хау), имеющая действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам. К ней нет свободного доступа. Обладатель этой информации на законном основании принимает меры к ее конфиденциальности.

2. Неприкосновенность документированной информации ограниченного доступа, составляющей коммерческую тайну, охраняется законом.

3. Незаконное получение, использование или разглашение информации ограниченного доступа, составляющей коммерческую тайну, причиняет вред их обладателю.

4. Информация ограниченного доступа, составляющая коммерческую тайну, может быть известна или доверена лицам, работающим в коммерческих или государственных структурах, на которых возлагается обязанность неразглашения этой информации.

5. За незаконное получение, использование или разглашение информации, составляющей коммерческую тайну, законодательством Российской Федерации устанавливается уголовная ответственность (см. приложение 6) [14, ст. 183].

Таким образом, с позиций такой дисциплины, как документоведение, определение «коммерческая тайна» можно сформулировать следующим образом: *коммерческая тайна – это охраняемая законом документированная информация ограниченного доступа или конфиденциальная информация, составляющая секрет производства (ноу-хау), за исключением информации, составляющей государственную тайну, в любой деятельности организации (государственной и негосударственной структур) и физического лица – обладателя информации, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам и в отношении которой ее обладателем введен режим коммерческой тайны.*

Банковская тайна. Возможны различные модификации конфиденциальной информации, составляющей коммерческую тайну. Одним из видов последней является банковская тайна, которая относится, как правило, к финансово-кредитной деятельности и едина для всех кредитных организаций (коммерческих банков). Но содержание коммерческой тайны, как правило, индивидуально для каждого предприятия или учреждения и относится к производству и распределению (торговле).

Кредитная организация, Банк России или организация, осуществляющая функции по обязательному страхованию вкладов, гарантируют тайну операций, счетов и вкладов своих клиентов и корреспондентов. Все служащие кредитной организации обязаны хранить тайну операций, счетов и вкладов ее клиентов и корреспондентов, а также иных сведений, устанавливаемых кредитной организацией, если это не противоречит федеральному закону [216].

Справки по операциям и счетам юридических лиц и граждан, осуществляющих предпринимательскую деятельность без образования юридического лица, выдаются кредитной организацией им самим, судам и арбитражным судам (судьям), Счетной палате Российской Федерации, налоговым органам, таможенным органам, органам принудительного исполнения судебных актов, органам предварительного следствия по делам, находящимся в их производстве, органам внутренних дел при осуществлении ими функций по выявлению, предупреждению и пресечению налоговых преступлений и др.

Справки по счетам и вкладам в случае смерти их владельцев выдаются кредитной организацией лицам, указанным владельцем счета или вклада в сделанном кредитной организации завещательном распоряжении, нотариальным конторам по находящимся в их про-

изводстве наследственным делам о вкладах умерших вкладчиков, а в отношении счетов иностранных граждан – иностранным консульским учреждениям [215].

Информация по операциям юридических лиц и граждан, занимающихся предпринимательской деятельностью без образования юридического лица, а также физических лиц предоставляется кредитными организациями в уполномоченный орган, осуществляющий меры по противодействию легализации (отмыванию) доходов, полученных преступным путем, в случаях, порядке и объеме, предусмотренных Федеральным законом «О противодействии легализации (отмыванию) доходов, полученных преступным путем» [39, ст. 7, 9].

Как Банк России, так и организация, осуществляющая функции по обязательному страхованию вкладов, не вправе разглашать сведения о счетах, вкладах, а также сведения о конкретных сделках и об операциях кредитных организаций, полученные ими в результате исполнения лицензионных, надзорных и контрольных функций.

Уполномоченный орган, осуществляющий меры по противодействию легализации (отмыванию) доходов, полученных преступным путем, не вправе раскрывать третьим лицам информацию, полученную от кредитных организаций в соответствии с Федеральным законом «О противодействии легализации (отмыванию) доходов, полученных преступным путем».

Организация, осуществляющая функции по обязательному страхованию вкладов, не вправе раскрывать третьим лицам информацию, полученную в соответствии с данным Федеральным законом «О страховании вкладов физических лиц в банках Российской Федерации» [31, ст. 31]. Страховое агентство вправе получать необходимую ему для осуществления функций информацию, составляющую служебную, коммерческую и банковскую тайны банка, в отношении которого наступил страховой случай [Там же].

Агентство обязано предоставить ставшую ему известной информацию об операциях банка, в отношении которого наступил страховой случай, по счетам и вкладам, о его финансовом состоянии, а также иную информацию, являющуюся коммерческой и банковской тайнами указанного банка, по запросу суда, а также Банка России. В случае разглашения страховым агентством или его должностными лицами информации, составляющей служебную, коммерческую и банковскую тайны, агентство обязано возместить причиненные убытки лицу, права которого были нарушены. Организация, осуществляющая функции по обязательному страхованию вкладов, не вправе раскрывать третьим лицам полученную информацию о страховании вкладов физических лиц в кредитных организациях.

В соответствии с Федеральным законом «О кредитных историях» определено: «Информация по операциям юридических лиц, граждан, осуществляющих предпринимательскую деятельность без образования юридического лица, и физических лиц, с их согласия, предоставляется кредитными организациями в целях формирования кредитных историй в бюро кредитных историй в порядке и на условиях, которые предусмотрены заключенным с бюро кредитных историй договором» [26, ст. 5].

За разглашение банковской тайны Банк России, организация, осуществляющая функции по обязательному страхованию вкладов, кредитные, аудиторские и иные организации, уполномоченный орган, осуществляющий меры по противодействию легализации (отмыванию) доходов, полученных преступным путем, а также их должностные лица и их работники несут уголовную ответственность, включая возмещение нанесенного ущерба [14, ст. 183] (см. приложение 6).

Коммерческие банки гарантируют тайну операций, счетов и вкладов своих клиентов и корреспондентов. Персонал банка обязан хранить эту тайну, а также другой информации, устанавливаемой банком, если это не противоречит законодательству о банковской деятельности. Информация, составляющая банковскую тайну, – персональные данные клиентов – может быть предоставлена только самим клиентам или их представителям.

Государственные структуры, которым предоставляется информация, обязаны хранить банковскую тайну. В этом случае банковская тайна становится служебной тайной. Банки обязаны публиковать по формам и в сроки, которые устанавливаются Центральным банком России, следующую информацию о своей деятельности:

- ежеквартально – бухгалтерский баланс, отчет о прибылях и убытках, информацию об уровне достаточности капитала, о величине резервов на покрытие сомнительных ссуд и иных активов;
- ежегодно – бухгалтерский баланс и отчет о прибылях и убытках с заключением аудиторской фирмы (аудитора) об их достоверности.

Фактически это перечень информации, которую нельзя отнести к банковской тайне.

Банки ежегодно публикуют свои консолидированные бухгалтерские отчеты и консолидированные отчеты о прибылях и убытках в форме, порядке и сроки, которые устанавливаются Центральным банком России, после подтверждения их достоверности заключением аудиторской фирмы (аудитора). Указанная информация, хотя и характеризует финансовое положение банка, к банковской тайне не относится. Так, банковская тайна кредитной организации выступает как частный случай коммерческой тайны, однако при ее передаче в судебные органы, Счетную палату Российской Федерации, налоговым, таможенным и следственным органам она становится частным случаем коммерческой тайны.

Банковская тайна в структурных подразделениях Центрального банка России – это уже частный случай служебной тайны. Возможно рассмотрение правового регулирования банковской тайны и в другом аспекте – исходя из субъекта информации. Соответственно, если субъектом информации выступает клиент банка, то это – банковская тайна. В случае, когда субъектом информации выступает сам банк – это коммерческая тайна банка [215; 216].

1.7. Секрет производства (ноу-хау) и служебный секрет производства

В ст. 1465, 1470 Четвертой части ГК РФ появилось новое понятие конфиденциальной информации: секрет производства (ноу-хау) и служебный секрет производства. Секретом производства (ноу-хау) признаются сведения любого характера (производственные, технические, экономические, организационные и др.), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны [5, ст. 1465] (см. разд. 1.6).

Исключительное право на секрет производства, созданный работником в связи с выполнением своих трудовых обязанностей или конкретного задания работодателя (служебный секрет производства), принадлежит работодателю [Там же, ст. 1470].

Гражданин, которому в связи с выполнением его трудовых обязанностей или конкретного задания работодателя стал известен секрет производства, обязан сохранять конфиденциальность полученных сведений до прекращения действия исключительного права на секрет производства.

В государственных, а также негосударственных структурах существует определенный порядок для выполнения целей, функций и задач конкретной организации: система планирования, финансирования, отчетности, контроля, технологий документооборота, конфиденциального делопроизводства и т.д. Информацию такого рода ранее можно было отнести, в соответствии с Положением о порядке обращения со служебной информацией ограниченного распространения, к несекретной информации, касающейся деятельности организаций, ограничения на распространение диктуются служебной необходимостью. На сегодняшний день это секрет производства (ноу-хау). Перечень

данной информации устанавливается руководителем организации – обладателя информации. Информацией, относящейся к секрету производства и служебному секрету производства, могут обладать любые организации, государственные и негосударственные структуры независимо от организационно-правовой формы, формы собственности и видов деятельности.

Обладателю секрета производства принадлежит исключительное право его использования любым не противоречащим закону способом (исключительное право на секрет производства), в том числе при изготовлении изделий и реализации экономических и организационных решений. Обладатель секрета производства может распоряжаться указанным исключительным правом.

Гражданин или юридическое лицо, обладающие исключительным правом на результат интеллектуальной деятельности или на средство индивидуализации (правообладатель), вправе использовать такой результат или такое средство по своему усмотрению любым не противоречащим закону способом. Исключительное право на секрет производства действует до тех пор, пока сохраняется конфиденциальность сведений, составляющих его содержание. С момента утраты конфиденциальности соответствующих сведений исключительное право на секрет производства прекращается у всех правообладателей.

Существует три вида договоров, регулирующих конфиденциальность секрета производства:

1) договор об отчуждении исключительного права на секрет производства;

2) лицензионный договор о предоставлении права использования секрета производства;

3) секрет производства, полученный при выполнении работ по договору подряда.

По договору об отчуждении исключительного права на секрет производства одна сторона (правообладатель – юридическое или физическое лицо, которым может быть государственная либо негосударственная структура) передает или обязуется передать принадлежащее ей исключительное право в полном объеме другой стороне – приобретателю этого права. При этом лицо, распорядившееся своим правом, обязано сохранять конфиденциальность секрета производства до прекращения действия исключительного права.

По лицензионному договору одна сторона – обладатель исключительного права на секрет производства (лицензиар) предоставляет или обязуется предоставить другой стороне (лицензиату) право использования соответствующего секрета производства в установленных договором пределах. Лицензионный договор может быть заключен как

с указанием, так и без указания срока его действия. В случае, когда срок, на который заключен лицензионный договор, не указан в этом договоре, любая из сторон вправе в любое время отказаться от договора, предупредив об этом другую сторону не позднее, чем за шесть месяцев, если договором не предусмотрен более длительный срок. При предоставлении права использования секрета производства лицо, распорядившееся своим правом, обязано сохранять конфиденциальность секрета производства в течение всего срока действия лицензионного договора. Лица, получившие соответствующие права по этому договору, обязаны сохранять конфиденциальность секрета производства до прекращения действия исключительного права.

В случае, когда секрет производства получен при выполнении договора подряда, договора на выполнение научно-исследовательских, опытно-конструкторских (НИОКР) или технологических работ либо по государственному или муниципальному контракту для государственных или муниципальных нужд, исключительное право на такой секрет принадлежит подрядчику (исполнителю), если соответствующим договором (государственным или муниципальным контрактом) не предусмотрено иное [248].

В случае, когда секрет производства получен при выполнении работ по договору, заключаемому главным распорядителем или распорядителем бюджетных средств с государственными структурами, исключительное право на такой секрет производства принадлежит подрядчику (исполнителю), если договором не установлено, что это право принадлежит Российской Федерации.

Нарушителями секрета производства являются: лицо, которое неправомерно получило информацию и сведения, составляющие секрет производства, и разгласило или использовало эти сведения; лицо, нарушившее конфиденциальность секрета производства в течение всего срока действия лицензионного договора, и лицо, которому в связи с выполнением его трудовых обязанностей или конкретного задания работодателя стал известен секрет производства и которое не сохранило конфиденциальность полученных сведений и информации до прекращения срока действия исключительного права на секрет производства.

Обладателем информации, составляющей секрет производства на законном основании, может быть введен режим коммерческой тайны. Поэтому ответственность за нарушение секретов производства сопоставима с ответственностью за незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайны [14, ст. 183] (см. приложение 6).

ГЛАВА 2

ДОКУМЕНТИРОВАНИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

2.1. Особенности документирования конфиденциальной информации

Документирование информации – одно из обязательных условий включения информации и документов в информационные ресурсы любой организации, государственной или негосударственной структуры (далее – организации).

В соответствии с Федеральным законом «Об информации...», законодательством Российской Федерации или соглашением сторон могут быть установлены требования к документированию информации [23, ст. 11, п. 2].

В федеральных органах исполнительной власти документирование информации осуществляется в порядке, установленном Правительством Российской Федерации в Правилах делопроизводства и документооборота (далее – Правила делопроизводства) [76]. Требования, установленные в Правилах делопроизводства, распространяются не только на федеральные органы исполнительной власти, но и другие государственные органы, органы местного самоуправления, т.е. государственные структуры. Эти требования могут распространяться и на другие организации и предприятия – негосударственные структуры.

В утвержденных Правилах делопроизводства определены «документирование информации, фиксация информации на материальных носителях в установленном порядке». Под документом понимается официальный документ, созданный государственным органом, органом местного самоуправления, юридическим или физическим лицом, оформленный в установленном порядке и включенный в документооборот федерального органа исполнительной власти [Там же, разд. 2].

Действие Правил делопроизводства не распространяется на организацию работы с документами и процессами документирования информации, содержащей государственную тайну.

Документирование информации ограниченного доступа является важнейшей составной частью конфиденциального делопроизводства, поскольку от количества, состава и правильности оформления конфиденциальных документов зависят качество и эффективность управленческой и производственной деятельности, достоверность и юридическая сила документов, трудоемкость их обработки и качество организации делопроизводства и документооборота, включая защищенный электронный документооборот, обмен электронными сообщениями.

Электронное сообщение – это информация, переданная или полученная пользователем информационно-телекоммуникационной сети [23, ст. 2]. Электронное сообщение, подписанное электронной цифровой подписью или иным аналогом собственноручной подписи, признается электронным документом, равнозначным документу, подписанному собственноручной подписью, в случаях, если федеральными законами или иными нормативными правовыми актами не устанавливается или не подразумевается требование о составлении такого документа на бумажном носителе [Там же, ст. 11].

Объем и содержание создаваемых конфиденциальных документов, в том числе и электронных, существенно влияют на организацию работ по их защите, защите электронного документооборота и в целом по информационной безопасности организации.

Документирование – длительный и системный процесс сбора и обработки информации в целях хранения, классификации, поиска, использования или передачи. Документированной информацией является информация, зафиксированная на материальном носителе путем ее документирования, с реквизитами, позволяющими определить такую информацию, или в установленных законодательством Российской Федерации случаях ее материальный носитель [23, ст. 2].

В силу своих особенностей технологии документирования конфиденциальной информации предполагают оформление реквизитов документов при их создании, которое имеет свою специфику и включает в себя:

- определение и использование реквизита конфиденциального документа – отметки о конфиденциальности документа или степени ограничения доступа и распространения (см. разд. 2.2);
- определение состава конфиденциальных документов – разработку Перечня конфиденциальной документированной информации, необходимого для определения степени ограничения доступа к документам (см. разд. 2.3);
- учет бумажных носителей, включая бланки документов (см. разд. 2.4, 2.7);

• учет проектов конфиденциальных документов и черновиков документов (см. разд. 2.5);

• учет носителей создаваемых электронных документов (сообщений) (см. разд. 3.7).

В данной главе не рассматривается оформление реквизитов конфиденциальных документов при документировании информации в соответствии с ГОСТ Р 6.30–2003 [151]. Существует достаточное количество научной литературы по данному вопросу [285; 295; 313]. Более подробно в этой главе освещено оформление такого реквизита, как отметка об ограничении доступа к документу или его конфиденциальности. Это связано еще с тем, что в ГОСТ Р 6.30–2003 требования к оформлению реквизита «отметка об ограничении к доступу» отсутствуют, несмотря на то что в практике оформления конфиденциальных документов данный реквизит применялся и применяется, например, в соответствии с Положением о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, утвержденным Постановлением Правительства Российской Федерации [94] или Федеральным законом «О коммерческой тайне» [29]. В Правилах делопроизводства [76, разд. III, п. 9] одним из обязательных реквизитов создаваемых документов является «отметка о конфиденциальности».

Более подробно особенности определения степени ограничения доступа к конфиденциальной информации, составляющей служебную, профессиональную, коммерческую тайны, а также секрет производства, рассмотрены в разд. 2.2.2. Технологии создания конфиденциальных документов с помощью СВТ, их печатания, копирования и тиражирования рассмотрены в разд. 2.6.

2.2. Определение степени ограничения доступа к документам и использование отметки конфиденциальности при оформлении документов

2.2.1. Общие положения

Порядок отнесения сведений к информации ограниченного доступа аналогичен порядку отнесения сведений о государственной тайне. Общедоступные технологии делопроизводства, относящиеся к государственной тайне, можно использовать при организации работы с конфиденциальными документами.

Степень конфиденциальности может быть присвоена документу:

• исполнителем на стадии подготовки документа;

• руководителем структурного подразделения или руководителем организации на стадии согласования или подписания документа;

• адресатом (получателем) документа на стадии его первичной обработки в Службе делопроизводства или Службе конфиденциального делопроизводства, если в организации существует такая отдельно выделенная служба (далее – Служба делопроизводства).

Определение необходимости проставления грифа (отметки) конфиденциальности на документах, в соответствии с утвержденным Перечнем конфиденциальной документированной информации организации (см. разд. 2.3), осуществляется исполнителем или должностным лицом, подписывающим документ, а на издании – автором (составителем) и руководителем, утверждающим издание к печати.

Изменение отметки конфиденциальности документа производится при изменении степени конфиденциальности содержащихся в нем сведений. Основанием для изменения или снятия отметки являются:

• соответствующая корректировка Перечня конфиденциальной документированной информации;

• истечение установленного срока действия конфиденциальности информации в соответствии с Перечнем конфиденциальной документированной информации;

• наличие события, при котором отметка конфиденциальности должна быть изменена или снята, например, окончание действия договора между организациями.

В зависимости от возможной степени ущерба, наносимого организации в случае разглашения информации, применяются две степени конфиденциальности информации: «конфиденциально» и «строго конфиденциально» [208; 245].

Использование перечисленных отметок для ограничения доступа и распространения информации, не относящейся к конфиденциальной, не допускается. Также не допускается, в соответствии со ст. 8 Закона Российской Федерации «О государственной тайне», использование грифов ограничения доступа, относящихся к государственной тайне: «Особой важности», «Совершенно секретно», «Секретно» [50].

На документы, дела, издания, а также другие носители информации наносится отметка конфиденциальности, включающая следующие реквизиты: степень конфиденциальности информации со ссылкой на соответствующий пункт действующего в организации Перечня конфиденциальной документированной информации; название организации, осуществившей ограничение доступа к конфи-

денциальной документированной информации; регистрационный номер; дату или условие снятия степени конфиденциальности или ограничение доступа.

Отметка о конфиденциальности наносится без кавычек в правом верхнем углу первого листа документа (при необходимости дополняется номером экземпляра документа, дела, издания), на обложке и титульном листе издания, а также на первой странице сопроводительного письма к этим материалам. Например:

Строго конфиденциально
Экз. № 1

или

Для служебного пользования
Экз. № 3

Для нанесения регистрационного номера, который должен включать в обязательном порядке данные о конфиденциальности документа, на регистрационно-контрольных карточках, а также в электронных картотеках допускается сокращение написания отметки: «Строго конфиденциально» – СКФД, «Конфиденциально» – КФД, «Для служебного пользования» – ДСП.

Руководители структурных подразделений, должностные лица имеют право снимать отметку конфиденциальности информации с документов и изданий, подготовленных в данном структурном подразделении, руководствуясь при этом Перечнем конфиденциальной документированной информации структурного подразделения организации.

После снятия отметки конфиденциальности документ передается в Службу делопроизводства. Об изменении или снятии конфиденциальности делается отметка на самом документе, удостоверяемая визой руководителя, подписавшего этот документ. О внесении в документ такой отметки сообщается заинтересованным лицам, учреждениям, предприятиям и организациям.

В целях своевременного изменения или снятия отметки конфиденциальности с документов необходимо регулярно просматривать учетные картотеки (перечни, журналы, списки и т.д.), в том числе электронные, и выявлять те документы, которые могут быть удалены из этих картотек.

Если созданный конфиденциальный документ подлежит отправлению с сопроводительным письмом, то оно регистрируется за самостоятельным номером, на нем проставляется отметка конфиденциальности, соответствующая отметке конфиденциальности приложения, независимо от того, содержит или нет сопроводительное письмо конфиденциальные данные.

При наличии нескольких приложений с разными степенями конфиденциальности отметка конфиденциальности сопроводительного письма устанавливается по наивысшей степени конфиденциальности приложений. Необходимость проставления на сопроводительном письме отметки конфиденциальности вызвана также тем обстоятельством, что без соблюдения этого требования подавляющее большинство сопроводительных писем будут не конфиденциальными, а открытыми. Однако поскольку документы отправляются за номерами сопроводительных писем, то формально и конфиденциальные приложения окажутся открытыми [208].

2.2.2. Особенности определения степени ограничения доступа к информации, составляющей служебную, коммерческую тайны, секрет производства (ноу-хау)

Для служебной информации ограниченного распространения, в том числе для информации, составляющей служебную тайну, за исключением информации, относящейся к государственной тайне, установлена одна степень конфиденциальности – «Для служебного пользования». Наименование данной отметки и его сокращенное название определены Положением о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, утвержденным Постановлением Правительства Российской Федерации [110].

В соответствии с п. 5 ст. 10 закона отнесение информации к конфиденциальной осуществляется в порядке, установленном законодательством Российской Федерации, за исключением случаев, предусмотренных ст. 11 данного закона. Использование в приведенной норме закона двух терминов, а именно «законодательство Российской Федерации» и «федеральный закон» позволило Суду сделать вывод о том, что отнесение информации к конфиденциальной в случаях, не подпадающих под действие ст. 11 закона, может осуществляться в порядке, установленном не только федеральными законами, но и иными актами законодательства (указами Президента Российской Федерации, постановлениями Правительства Российской Федерации).

Применение грифа «Для служебного пользования» также более подробно рассмотрено в разд. 1.4.

На практике негосударственные структуры, обладающие информацией, составляющей служебную тайну или секрет производства, применяют наименование отметки конфиденциальности «Для

служебного пользования» совместно со степенями конфиденциальности документов: «Конфиденциально» и «Строго конфиденциально».

В Федеральном законе «О коммерческой тайне» установлена одна степень конфиденциальности – «Коммерческая тайна», свидетельствующая лишь о принадлежности информации к коммерческой тайне. Установление одной степени (одного грифа) конфиденциальности информации, составляющей коммерческую тайну, обусловлено, вероятно, тем, что степень конфиденциальности определяется обладателями информации, которые могут иметь разные подходы к определению степени конфиденциальности однотипной по содержательной части информации в соответствии с Федеральным законом «О коммерческой тайне» (см. приложение 2).

При рассмотрении дел о неправомерном получении информации, составляющей коммерческую тайну, в судебном порядке (см. приложение 6) сложно определить, кто из обладателей установил правильную степень конфиденциальности информации, так как критерии отнесения информации к той или другой степени конфиденциальности, а также запрет на отнесение документированной информации к конфиденциальной (см. приложение 1) устанавливает ее обладатель. В Федеральном законе «О коммерческой тайне» об этом ничего не сказано, но содержится указание на то, что наряду с мерами по установлению режима коммерческой тайны обладатель информации вправе применять при необходимости средства и методы технической защиты конфиденциальности этой информации и другие не противоречащие законодательству Российской Федерации меры.

Меры по охране конфиденциальности информации, принимаемые ее обладателем, должны включать в себя:

- определение перечня информации, составляющей коммерческую тайну (см. приложение 2);
- ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка, а также принятия нормативного документа (положения, инструкции) по конфиденциальному делопроизводству;
- учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана (см. разд. 4.7);

• регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров (см. гл. 4);

• нанесение на материальные носители (документы), содержащие информацию, составляющую коммерческую тайну, грифа «Коммерческая тайна» с указанием обладателя этой информации (для юридических лиц – полное наименование и место нахождения, для индивидуальных предпринимателей – фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства) [29, ст. 10].

Без применения данных мер, в том числе такой основной, как нанесение грифа «Коммерческая тайна» или отметки о конфиденциальности, режим коммерческой тайны нельзя считать установленным.

В то же время придание информации, требующей разного уровня защиты, одной степени конфиденциальности не позволяет выделить наиболее значимую информацию в целях установления для нее более усиленного, чем для менее значимой информации, режима защиты.

Решение этой проблемы состоит в разделении информации по степеням конфиденциальности – на создаваемую и отправляемую документированную информацию. Документированная информация, не подлежащая отправлению в другие организации, может иметь две степени и два наименования конфиденциальности – «Конфиденциально», «Строго конфиденциально», а отправляемая – одну степень и наименование «Коммерческая тайна». Для информации ограниченного доступа, составляющей коммерческую тайну, используется гриф «Коммерческая тайна». В соответствии с Федеральным законом «О коммерческой тайне», гриф должен содержать сведения об обладателе указанной информации. В данном случае это означает, что право собственности на информацию, составляющую коммерческую тайну, охраняется законодательством Российской Федерации. Гриф «Коммерческая тайна» можно дополнять соответствующим внутренним грифом степени конфиденциальности: «Конфиденциально» и «Строго конфиденциально» или грифом «Для служебного пользования» [209; 238].

В новой редакции Федеральный закон «О коммерческой тайне» регулирует отношения, связанные с установлением, изменением и прекращением режима коммерческой тайны в отношении информации, составляющей секрет производства (ноу-хау). Поэтому все, что определено выше, касается документированной информации, составляющей секрет производства (ноу-хау) и служебный секрет производства.

2.2.3. Особенности определения степени ограничения доступа к информации, составляющей профессиональную тайну

Профессиональной тайной является информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (см. разд. 1.5). Фактически получается, что профессиональная тайна – это персональные данные клиентов, пациентов и т.д., а также служебная и коммерческая тайны других организаций.

В Федеральном законе «Об информации...», в котором дано определение профессиональной тайны, и в Федеральном законе «О персональных данных» про степень конфиденциальности и, соответственно, об отметке конфиденциальности ничего не говорится. И на практике на кадровой документации организаций или банковской документированной информации о клиентах банка (банковская тайна), или медицинских картах (врачебная тайна) отметка конфиденциальности на документах не проставляется. Об этом упоминается в содержании данного документа.

Документы и информация, отнесенные к профессиональной тайне (в некоторой мере профессиональная тайна относится к персональным данным), например документация кадровая, банковская (банковская тайна), адвокатская и аудиторская (адвокатская и аудиторская тайны), как правило, грифа ограничения доступа не имеют, потому что в полном объеме являются конфиденциальными в связи с тем, что профессиональная тайна в любом случае сводится к соблюдению неразглашения (конфиденциальности) персональных данных клиентов, пациентов и других физических лиц – субъектов персональных данных в соответствии с Федеральным законом «О персональных данных».

2.3. Разработка Перечня конфиденциальной документированной информации

2.3.1. Общие положения

Одной из особенностей документирования конфиденциальной информации является регламентирование состава создаваемых конфиденциальных документов. Конфиденциальная документиро-

ванная информация должна создаваться только при действительной необходимости в письменном удостоверении наличия и содержания управленческих, коммерческих, производственных и иных действий, передаче информации, хранении и использовании ее в течение конкретного времени и в определенном количестве экземпляров. При этом решение задач конфиденциальной деятельности должно обеспечиваться минимальным количеством конфиденциальных документов при сохранении полноты требуемой информации.

Требование регламентирования создаваемой КДИ обусловлено необходимостью предотвращения не только необоснованного, но и неконтролируемого ее создания, которое может привести к утечке содержащейся в документах информации.

Перечень конфиденциальной документированной информации организации (далее – Перечень) является основой организации конфиденциального делопроизводства и документооборота и зависит от компетенции и функций организации, характера ее деятельности, взаимосвязей с другими предприятиями и организациями, порядка разрешения вопросов. В свою очередь, Перечень влияет на качество соответствующей области деятельности, организацию и надежность обработки и защиты документированной информации, а также служит основанием для создания Классификатора автоматизированной информационной системы и циркулирующей в системе информации ограниченного доступа, или, другими словами, системы защищенного электронного документооборота [246].

Целями разработки такого Перечня должны являться не только определение состава конфиденциальной документированной информации, необходимой и достаточной для деятельности организации, но и установление конкретных лиц, имеющих право создавать, составлять, визировать и подписывать (утверждать) документы, а также предотвращение необоснованной рассылки этих документов.

Состав конфиденциальной документированной информации определяется организацией (ее обладателем) и фиксируется в Перечне, который нуждается в регулярном обновлении, корректировке.

При составлении Перечня необходимо исходить из трех основных принципов: законности, обоснованности и своевременности придания документированной информации конфиденциальности, т.е. отнесения ее к какой-либо тайне (коммерческой, профессиональной, служебной, банковской, персональным данным и т.д.), за исключением государственной тайны.

Принцип законности заключается в соблюдении мер по охране конфиденциальности информации и запрету относить информацию к какой-либо тайне в соответствии с законодательством Российской Федерации и нормативными правовыми документами (см. приложение 1).

Принцип обоснованности устанавливается экспертной оценкой целесообразности придания конфиденциальности конкретной информации исходя из вероятных последствий – нанесения ущерба (экономического, финансового и др.) – и баланса экономической выгоды и безопасности организации, включая информационную безопасность.

Принцип своевременности заключается в установлении ограничения доступа и распространения информации с момента ее получения, разработки или до разработки.

В каждой позиции Перечня рекомендуется указывать отметку конфиденциальности, фамилии работников, имеющих право доступа и несущих ответственность за сохранность конфиденциальной документированной информации, срок действия грифа или наименование события, снимающего это ограничение, виды документов и баз данных, в которых эти сведения фиксируются и хранятся.

Важной задачей Перечня является дробление информации на отдельные информационные элементы, известные разным должностным лицам. В свою очередь, закрепление информации с ограниченным доступом за конкретными документами позволяет исключить возможность необоснованного создания документов или включения в них избыточных данных.

Аналогичные перечни в качестве разделов, входящих в общий Перечень конфиденциальной документированной информации, могут иметь структурные подразделения организации. Перечень информации, которую запрещено относить к документированной информации с ограниченным доступом, приведен в приложении 1. Примерный перечень информации, составляющей коммерческую, служебную тайны, секрет производства (ноу-хау) организации, приведен в приложении 2.

Организации в начальной стадии разработки Перечня необходимо создать Примерный перечень документированной информации ограниченного доступа, который следует включить в Инструкцию по конфиденциальному делопроизводству или отдельным разделом в общую Инструкцию по делопроизводству, регулирующую информационные взаимосвязи режима конфиденциальности информа-

ции. Затем этот Перечень можно будет наполнить конкретной информацией при изменении внешних и внутренних условий работы организации [246].

2.3.2. Особенности составления позиций Перечня конфиденциальной документированной информации, составляющей коммерческую тайну

В данные позиции Перечня включается информация:

• составляющая коммерческую тайну (секрет производства) – сведения любого характера (производственные, технические, экономические, организационные и др.), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности (см. приложение 2);

• имеющая, согласно определению самого обладателя информации, действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, у которых нет свободного доступа к данной информации на законном основании и в отношении которой обладателем таких сведений введен режим коммерческой тайны.

Исключение составляет информация, которая не может быть коммерческой тайной, а также информация, которую не разрешается ограничивать в допуске и распространении в соответствии с российским законодательством и правовыми нормативными документами (см. приложение 1).

Кроме того, правомерным считается получение конфиденциальной информации от ее обладателя на основании договора или в результате правопреемства (см. разд. 1.7).

Особое внимание следует уделять такому виду документов, как договора и контракты, в связи с тем, что в данном виде документов отражена информация, составляющая коммерческую тайну: финансовая, торговая, снабженческая, научно-техническая, производственная и другая, включая ноу-хау (секреты производства). Причем в некоторых случаях в Перечень необходимо включать не только информацию договора, но и сам факт его заключения. Примерный перечень информации, составляющей коммерческую и служебную тайны, секрет производства (ноу-хау), приведен в приложении 2.

2.3.3. Основные этапы разработки Перечня конфиденциальной документированной информации

Первый этап. На основе анализа задач, функций, компетенции, направлений деятельности организации необходимо установить весь состав циркулирующей в организации информации, отображенной на любом носителе, любым способом, в любом виде и в любой автоматизированной информационной системе или отдельном компьютере. Также необходимо учитывать перспективы развития организации и ее взаимоотношений с партнерами и заранее определять характер дополнительной информации, которая может возникнуть в результате деятельности организации. Данная информация классифицируется по тематическому признаку.

Второй этап. Определяется, какая из установленной информации должна быть ограниченного доступа и относиться к какому-либо виду тайн, за исключением государственной. Базовым критерием при этом является возможность получения преимуществ от использования информации за счет неизвестности ее третьим лицам. Этот критерий имеет две составляющие: неизвестность информации третьим лицам и получение преимуществ в силу этой неизвестности. Конфиденциальная документированная информация взаимосвязана и взаимообусловлена, поскольку, с одной стороны, неизвестность информации третьим лицам сама по себе ничего не значит, если не обеспечивает преимуществ, с другой – преимущества можно получить только за счет такой неизвестности. Конфиденциальность информации является правовой формой и одновременно инструментом обеспечения ее неизвестности.

Преимущества от использования информации, неизвестной третьим лицам, могут состоять в получении выгоды или предотвращении ущерба, иметь в зависимости от областей и видов деятельности экономические, моральные и другие характеристики, выражаться количественными и качественными показателями. Названный критерий является объективным показателем возможности отнесения информации к какой-либо тайне, мерилом придания информации статуса конфиденциальной. Это означает, что при отсутствии данного критерия нет оснований для перевода информации в категорию конфиденциальной – информации ограниченного доступа. Но это не означает, что при его наличии информация во всех случаях может и должна быть отнесена к конфиденциальной [209].

Третий этап. После установления состава информации определяется степень ее конфиденциальности. Степень конфиденциальности – это показатель уровня закрытости информации. Уровень закрытости зависит от величины ущерба, который может наступить при утечке информации. Чем больше этот ущерб, тем выше должна быть и степень конфиденциальности информации. Более подробно определение и использование отметки конфиденциальности на документах рассмотрено в разд. 2.2.

Четвертый этап. Это этап определения конкретных сроков конфиденциальности информации либо обстоятельств и событий, при наступлении которых она снимается. Продолжительность конфиденциальности информации должна соответствовать срокам действия условий, необходимых и достаточных для признания данной информации конфиденциальной.

Результаты всех этапов работы оформляются Перечнем конфиденциальной документированной информации (форма 1).

При значительном объеме конфиденциальной информации она классифицируется в Перечне по разделам, соответствующим сферам деятельности организации, или по перечням конфиденциальной документированной информации структурных подразделений организации.

Руководством организации должна быть утверждена Экспертная комиссия по защите конфиденциальной информации (далее – Экспертная комиссия), одними из основных функций которой являются согласование и утверждение Перечня.

Перечень подписывается председателем и всеми членами Экспертной комиссии, утверждается и вводится в действие приказом руководителя организации. В приказе должны быть определены мероприятия по обеспечению функционирования Перечня и контролю за его выполнением. С приказом и Перечнем необходимо ознакомить под расписку всех сотрудников организации, работающих с информацией ограниченного доступа, за исключением той, которая представляет государственную тайну.

Копии Перечня или выписки из него должны быть направлены обладателям данной информации как в самой организации, так и вне ее. Ими являются физические или юридические лица, которым в силу служебного положения, договора либо на ином законном основании информация известна.

Дополнения и изменения состава включенных в Перечень сведений, а также изменение степени их конфиденциальности могут осуществляться с разрешения руководителя организации и вноситься в Перечень за подписями руководителей структурного подразде-

ления по принадлежности информации, Службы безопасности организации (если такая служба предусмотрена в штатном расписании организации) и Службы делопроизводства. При существенном изменении состава сведений Перечень должен составляться заново.

В сферу конфиденциального делопроизводства входят наряду с документированной информацией (документами на бумажном носителе) базы данных, электронные документы и т.д., поэтому из всей совокупности информации, включенной в Перечень сведений, необходимо выделить состав документируемой информации и установить виды документов, в которых она должна быть зафиксирована.

Например, базой данных является представленная в объективной форме совокупность самостоятельных материалов (статей, расчетов, нормативных актов, судебных решений и иных подобных материалов), систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью электронной вычислительной машины (ЭВМ) [5, ст. 1260].

В рамках критериев документирования определение состава документируемой информации должно увязываться с решением конкретных задач. В зависимости от назначения этой информации определяются конкретные виды документов. Виды КДИ необходимо устанавливать с учетом оптимального объема содержащейся в ней информации, исключающей избыточную, в том числе дублетную, информацию, поскольку избыточная информация – это конфиденциальные данные, утечка которых может нанести ущерб организации.

После установления состава документов определяется круг лиц, имеющих право создавать (составлять) и подписывать (утверждать) каждый вид документа, а также предприятий и организаций, которым этот документ должен направляться. На данном этапе дополнительно определяется Перечень создаваемой конфиденциальной документированной информации (форма 2).

В Перечень может быть включена также графа «ФИО лиц, визирующих (согласовывающих) документы».

Грифы и сроки конфиденциальности документов должны соответствовать степеням и срокам конфиденциальности включаемой в документы информации.

Если документ подлежит утверждению, то в графе 6 сначала проставляются ФИО лица (лиц), подписывающего документ, затем, после слова «утв.» – ФИО лица, утверждающего документ. При значительном количестве утверждаемых документов графа 6 может быть разделена на две графы: «ФИО лиц, имеющих право подписывать документы» и «ФИО лиц, имеющих право утверждать документы».

Форма 1

№ п/п	Наименование информации	Степень конфиденциальности	Срок конфиденциальности
1	2	3	4

Форма 2

№ п/п	Наименование документов	Гриф конфиден-циальности	Срок конфиден-циальности	ФИО лиц, имеющих право создавать документ	ФИО лиц, имеющих право подписывать документ	Количество составляемых экземпляров документа	Куда направляется	Примечание
1	2	3	4	5	6	7	8	9

Если при направлении конфиденциальных документов другим предприятиям и организациям каждый адресат не должен знать, кому еще направлен данный документ, то в графе 8 по соответствующему виду документа после внесения адресатов делается пометка «Раздельное адресование», означающая, что на каждом экземпляре документа должен проставляться лишь адресат, которому направляется данный экземпляр.

Графу 9 следует использовать (при необходимости) для указания периодичности составления документов, а также для пометки о проставлении оттиска печати на соответствующих документах.

Перечень создаваемой конфиденциальной информации утверждается руководителем организации. Под расписку с ним должны быть ознакомлены все лица, наделенные правом создавать, оформлять, визировать, подписывать и утверждать документы. Внесение в Перечень возможных последующих частичных уточнений или изменений может быть возложено на руководителей Службы безопасности и Службы делопроизводства организации, а также Экспертной комиссии.

При изменении Перечня конфиденциальной документированной информации соответствующие изменения вносятся и в Перечень создаваемой конфиденциальной документированной информации. О снятии грифа конфиденциальности информации с отправленных документов должны быть письменно оповещены организации и предприятия – адресаты.

В случаях необходимости создания разовых документов, не включенных в Перечень создаваемой конфиденциальной документированной информации, или дополнительных экземпляров документов, не предусмотренных Перечнем, их изготовление может производиться по совместному разрешению руководителей соответствующего структурного подразделения, Службы безопасности и Службы делопроизводства. Одновременно определяется целесообразность включения таких документов (дополнительных экземпляров) в Перечень конфиденциальной документированной информации. Служба делопроизводства совместно с руководителями соответствующих подразделений, а также Службой безопасности должна осуществлять контроль за соответствием создаваемых документов Перечню конфиденциальной документированной информации. Необходимость такого контроля обусловлена тем, что исполнители документов нередко допускают некоторые отступления от Перечня, например:

• завышение или занижение отметки конфиденциальности документов;

• проставление отметки конфиденциальности на документах, не содержащих конфиденциальной информации;

• необоснованное включение конфиденциальной информации в документы и превращение тем самым открытых документов в конфиденциальные;

• неправильное адресование документов;

• непроставление отметки конфиденциальности на документах, содержащих конфиденциальную информацию.

Сведения Перечня конфиденциальной документированной информации необходимо использовать для ведения Реестра конфиденциальной информации, циркулирующей в АИС (конечно, при наличии в организации такой системы), или, иначе, системы конфиденциального электронного документооборота. Организация и технологии разработки такого Реестра, необходимые для обеспечения режима конфиденциальности информации в данных системах, более подробно рассматриваются в разд. 3.7.

2.4. Учет бумажных носителей конфиденциальной информации

Создание конфиденциальных документов должно начинаться с учета, оформления и выдачи исполнителям бумажных носителей информации, на которых будут составляться черновики или проекты конфиденциальных документов. Эти технологии не всегда являются обязательными, поскольку они усложняют процесс документирования конфиденциальной информации и понижают оперативность подготовки документов. Для рассмотрения вопроса о применении технологии учета бумажных носителей всегда следует помнить о балансе их учета – одной из форм защиты конфиденциальной информации – и оперативности создания и прохождения конфиденциальных документов. В связи с этим разд. 2.4 и 2.5, которые были созданы по материалам книги А.И. Алексенцева «Конфиденциальное делопроизводство» [209], носят рекомендательный характер.

Бумажными носителями могут быть: спецблокноты, отдельные листы бумаги, типовые формы документов, стенографические и рабочие тетради. *Спецблокнот* предназначен для составления

черновиков конфиденциальных документов и представляет собой сброшюрованные и пронумерованные листы бумаги с линией отрыва и контрольным листом, в котором проставляются номера листов блокнота. *Стенографическая тетрадь* используется для стенограмм, *рабочая тетрадь* (сброшюрованные листы бумаги без линии отрыва), как правило, – для различных рабочих справочных записей, хотя в ней допускается составлять черновики отдельных больших по объему документов. Остальные носители могут использоваться как для составления черновиков, так и для печатания или рукописного изготовления проектов документов.

Бумажные носители, предназначенные для составления черновиков конфиденциальных документов, в некоторых организациях не учитываются, а лишь производится отметка об их уничтожении в учетных формах соответствующих документов после печатания проектов документов. Однако это нередко приводит к тому, что при составлении нескольких вариантов черновика с отметкой в учетных формах уничтожается только вариант, с которого печатался проект документа, остальные варианты просто выбрасываются или хранятся у составителя.

Все это, помимо необходимости последующего проведения поиска черновика, которое зачастую не приводит к положительным результатам, создает возможности для утечки содержащейся в черновике конфиденциальной информации. Поэтому все носители, предназначенные для составления черновиков и проектов конфиденциальных документов, следует учитывать предварительно, до внесения в них записей. Такой учет позволяет предотвращать неправомерное обращение с носителями и, кроме того, обеспечивать контроль за подготовкой документов и их соответствием Перечню конфиденциальной документированной информации. Учет носителей осуществляется Службой делопроизводства, контроль за состоянием учета – Службой безопасности организации.

Перед взятием на учет носители должны быть соответствующим образом оформлены.

На обложках спецблокнотов сотрудник Службы делопроизводства пишет или проставляет штампом (если не проставлено типографским способом) слово «Спецблокнот» и в правом верхнем углу гриф конфиденциальности. Если листы спецблокнота не пронумерованы типографским способом, то они нумеруются.

На обложках рабочих и стенографических тетрадей указываются вид носителя, гриф конфиденциальности, инициалы и фамилия исполнителя. Листы тетрадей нумеруются, оборот последнего листа

подписывается сотрудником Службы делопроизводства с указанием количества листов в тетради. Листы типовых форм документов нумеруются исполнителем, на первом листе проставляется гриф конфиденциальности.

На отдельных листах бумаги в соответствующих графах основных надписей штампов или других установленных местах исполнителем проставляются отметка конфиденциальности и номера листов. На любом носителе, предназначенном для составления одного конкретного документа, указывается наименование этого документа.

Учет бумажных носителей в зависимости от их количества и продолжительности хранения может осуществляться в пределах года или нескольких лет. В последнем случае учетные номера каждого года продолжают номера предыдущих лет. По окончании непрерывного учета заводится новый учет за новыми номерами. Числящиеся по предыдущему учету носители перерегистрируются по новому учету с отметкой о перерегистрации в предыдущей учетной форме.

Носители конфиденциальной информации учитываются в журналах или карточках (форма 3).

Если в организации носители не переводятся на инвентарный (выделенный) учет документов, дел и носителей конфиденциальной документированной информации (см. разд. 3.6), то графа 9 называется«Отметка об уничтожении носителя».

При постановке на учет заполняются графы 1–6.

В графе 1 рядом с номером носителя начальными буквами (аббревиатурой) проставляется его отметка конфиденциальности: СТ – служебная тайна; ПД – персональные данные; ПТ – профессиональная тайна; КТ – коммерческая тайна; СКФД – строго конфиденциально; КФД – конфиденциально; ДСП – для служебного пользования.

В графе 2 арабскими цифрами проставляется дата: в карточке – с указанием числа, месяца и года, в журнале – числа и месяца (год проставляется перед началом регистрации носителей за этот год). В графе 3 пишется: спецблокнот, листы, типовая форма, рабочая тетрадь и др. В графе 4 указывается наименование носителя, если он предназначен для составления конкретного документа, или его назначение, если в него будет вноситься различная информация, например по спецблокноту – «для черновиков», по рабочей тетради – «для рабочих записей».

Форма 3

Учетный номер и отметка конфиденциальности носителя	**Дата регистрации**	**Вид носителя**	**Наименование или назначение носителя**	**Количество листов**	**ФИО лиц, получивших носитель**	**Подпись, дата в получении носителя**	**Подпись, дата возврата носителя**	**Отметка об уничтожении носителя или переводе на инвентарный учет документов**
1	2	3	4	5	6	7	8	9

Одновременно на самих носителях проставляется:

• на спецблокнотах – в верхнем левом углу лицевой стороны обложки штамп с указанием учетного номера носителя и количества листов, на каждом листе в верхнем левом углу – учетный номер;

• на рабочих и стенографических тетрадях – в верхнем левом углу лицевой стороны обложки (а при невозможности в верхнем левом углу форзаца) такой же штамп с указанием учетного номера носителя и количества листов;

• на отдельных листах документа в верхней части левого поля первого листа проставляется такой же штамп с указанием учетного номера носителя и количества листов; на левом поле остальных листов – штамп «К носителю № __» или сокращенно «К Н № __» с указанием номера.

После постановки на учет носитель передается исполнителю под подпись в графе 7 журнала учета носителей.

При необходимости постановки на учет дополнительных листов носителя (при нехватке ранее взятых листов для составления черновика документа или для замены испорченных листов) они нумеруются от последнего листа, ранее учтенного по этому номеру носителя, регистрируются в журнале учета носителей под тем же номером, что и ранее взятые листы, отдельной строкой под ними (при этом заполняются графы 2, 5), на левом поле каждого листа проставляется штамп «К Н № __» с указанием номера, а на первом листе всего носителя прежнее количество листов зачеркивается и проставляется новое с учетом дополнительных листов. Исправление заверяется подписью сотрудника Службы делопроизводства. Выдача дополнительных листов производится под отдельную подпись в графе 7 журнала учета носителей.

2.5. Учет проектов конфиденциальной документированной информации

Проекты конфиденциальных документов могут изготавливаться рукописным способом, на пишущей машинке или с помощью печатающих устройств (принтеров) средств вычислительной техники. Особенности изготовления конфиденциальной документированной информации на средствах ЭВМ рассмотрены в разд. 2.6. Также могут изготавливаться отдельные рукописные текстовые документы, авторами которых являются должностные лица (докладные записки, справки, заявления и др.), если это предусмотрено Инструкцией по делопроизводству организации.

Документы не рекомендуется диктовать, наговаривать на диктофон. Проекты других текстовых документов изготавливаются печатным способом под диктовку или со звуковоспроизводящих устройств либо в два этапа: составление на бумажном носителе черновика проекта документа рукописным способом и последующее печатание проекта документа с черновика. Также возможен вариант внесения переменной части текста в типовые формы документов, хранимые в памяти компьютера, и их дальнейшего распечатывания на принтере.

Проекты документов, изготовляемые рукописным способом, и составляемые на учтенных бумажных носителях черновики проектов текстовых документов должны отвечать требованиям, предъявляемым к соответствующим видам документов, как по способу воспроизведения информации, так и по порядку оформления. Они должны содержать все необходимые на стадии подготовки данного вида документа реквизиты, соответствующие ГОСТ 6.30–2003, а также особенности, предъявляемые к оформлению конфиденциальных документов, иметь отметку о конфиденциальности (см. разд. 2.1).

Кроме того, на первом листе черновика текстового документа должны быть проставлены количество необходимых экземпляров проекта документа и фамилия исполнителя. Если подлежащий изданию документ не предусмотрен Перечнем конфиденциальной документированной информации, то на черновике должны быть представлены визы руководителей соответствующего структурного подразделения, Службы безопасности и Службы делопроизводства.

Черновики и проекты текстовых документов должны также отвечать существующим нормам по содержательной части и способу изложения. Такие нормы в определенной степени зависят от конкретного вида документа, однако существуют и общие требования, которые необходимо учитывать при составлении любого вида текстовых документов.

При наличии черновика, составленного на любом бумажном носителе, проверяются соответствие черновика Перечню конфиденциальной документированной информации, наличие и правильность оформления необходимых реквизитов, а также:

- если черновик составлен в виде спецблокнота, просчитывается количество листов черновика с изъятием их из спецблокнота;
- если черновик составлен на отдельных листах бумаги или в типовой форме документа, просчитывается количество листов черновика;
- если черновик составлен в виде стенографической или рабочей тетради, проверяются наличие листов тетради и соответствие их количества заверительной надписи.

После проведения этих операций данные о черновике вносятся в журнал или карточку учета проектов созданных/изданных конфиденциальных документов (форма 4).

Если издаваемые организацией документы не переводятся на инвентарный, выделенный (списочный) учет (см. разд. 3.6), то графа 17 опускается.

При приеме черновика заполняются графы 1, 3–5. В графе 1 проставляются очередной порядковый номер документа, который будет напечатан с данного черновика, и аббревиатурой отметка конфиденциальности. Внутренние документы и документы, подлежащие отправлению в другие организации и предприятия, учитываются по единой валовой нумерации.

В графе 5 проставляются номер носителя, присвоенный ему по журналу учета носителей, и через дробь номера листов носителя, являющихся черновиком данного документа (при последовательности номеров листов – через тире, при непоследовательности – через запятую).

Учетный номер будущего документа указывается и на черновике, а при составлении черновика в спецблокноте – дополнительно в соответствующей графе контрольного листа спецблокнота напротив изъятых для печатания листов черновика с проставлением подписи сотрудника Службы делопроизводства и даты. Спецблокнот возвращается исполнителю, а за получение отдельных листов бумаги, типовой формы документа, стенографической или рабочей тетради сотрудник Службы делопроизводства выдает разовую расписку по форме 5.

Форма 5

РАСПИСКА

Дана _____ *в том, что мною* _____
(инициалы, фамилия) (инициалы, фамилия)
получены во временное пользование документы, носители информации за № _____,
всего на _____ *л.*

Подпись

Дата

После печатания проекта документа заполняются графы 6–7 журнала учета созданных/ изданных документов, проект документа вместе с черновиком передается исполнителю под подпись в графе 8. Разовая расписка, выданная ранее исполнителю за получение носителя (черновика), возвращается сотруднику Службы конфиденциального делопроизводства и уничтожается.

Форма 4

Учетный номер и отметка конфиден-циальности	Дата документа	Вид и заголовок документа	ФИО исполнителя	Номера носителя и листов черновика	Количество экземпляров документов	Количество листов в экземпляре	Подпись за получение черновика и проекта документа	Подпись за возврат, дата
1	2	3	4	5	6	7	8	9

Окончание

Отметка об уничтожении черновика	Отметка об уничтожении проектов или лишних экземпляров документа	Куда отправлен документ	Номера экземпляров	Наименование, номер и дата сопроводитель-ного документа	Отметка о возврате	Индекс (номер) дела, номера листов дела	Номер по учету документов выделенного хранения, количество экземпляров
10	11	12	13	14	15	16	17

При необходимости перепечатывания отдельных листов проекта документа без изменения общего количества листов от исполнителя принимаются по разовой расписке все экземпляры подлежащих перепечатыванию листов. Вновь отпечатанные листы передаются исполнителю взамен разовой расписки.

В случае необходимости перепечатывания проекта документа с изменением количества листов перепечатывание производится за новым учетным номером. От исполнителя принимаются исправленный и все другие экземпляры проекта, а также черновик с погашением подписи исполнителя в графе 9 журнала учета изданных документов. Технология учета и выдачи вновь отпечатанного проекта аналогична технологии учета и выдачи проекта документа, печатаемого с черновика, с той лишь разницей, что в графе 5 вместо номера носителя указывается «С № __» с проставлением номера перепечатываемого проекта без указания номеров листов в нем.

При изготовлении дополнительных экземпляров проекта документа или дополнительных экземпляров уже подписанного (утвержденного) документа (в случае возникновения необходимости в них) в графе 6 журнала учета созданных/изданных документов под ранее сделанной записью через знак «+» проставляется количество дополнительных экземпляров. Нумерация дополнительно изготовленных экземпляров производится от последнего номера ранее пронумерованных экземпляров. Подпись за получение таких экземпляров производится отдельно от предыдущей.

При рукописном изготовлении проекта текстового документа на отдельных листах или рукописном заполнении типовой формы документа, а также при разработке чертежно-графических документов носители могут учитываться или по журналу учета носителей, или сразу по журналу учета созданных/изданных документов. В последнем случае заполняются графы 1, 3–7 (в графе 5 пишется слово «Рукопись»).

Если проект текстового документа печатался под диктовку, то заполняются те же графы (в графе 5 проставляется «б/ч» – без черновика).

Эти же графы заполняются при печатании проекта документа со звуковоспроизводящих устройств (в графе 5 проставляются вид и номер носителя речевой информации). Прием/возврат носителя осуществляется по разовой расписке.

Если проект документа был отпечатан как открытый, а в процессе визирования или подписания было принято решение о переводе его в разряд конфиденциальных, то исполнителем должны быть пред-

ставлены в Службу делопроизводства все экземпляры отпечатанного проекта и черновик. На обороте последнего экземпляра проекта исполнитель указывает, сколько экземпляров отпечатано и сколько листов в черновике, заверяя это своей подписью. При отсутствии черновика или отдельных экземпляров проекта документа руководителем организации назначается комиссия для их поиска. Если они не будут найдены, то об этом делается отметка на обороте последнего экземпляра проекта за подписью председателя комиссии. Об обстоятельствах утраты докладывается руководителю организации для принятия соответствующих решений.

Фактически представленные экземпляры проекта документа и черновик регистрируются в журнале учета созданных/изданных документов в графах 1, 3–7. В графе 5 при наличии черновика пишется «Конфиденциально ___ л.» с указанием количества листов черновика, на черновике проставляются отметка конфиденциальности и учетный номер проекта документа. При отсутствии черновика в графе 5 указывается «б/ч» – без черновика.

Проект документа выдается вместе с черновиком (при наличии) исполнителю под подпись в графе 8.

После отработки проекта текстового документа исполнитель должен проставить номера экземпляров, завизировать остающийся в организации экземпляр, получить визы соответствующих должностных лиц, подписать (а при необходимости и утвердить) проект у соответствующего руководителя и передать все экземпляры документа, в том числе и оказавшиеся по каким-либо причинам лишними, вместе с черновиком (если документ печатался с черновика) в Службу делопроизводства. Если проект документа по каким-либо причинам не был подписан, то все его экземпляры вместе с черновиком также передаются в Службу делопроизводства.

В целях упорядочения визирования конфиденциальных документов целесообразно разработать Перечень визируемых документов с указанием по каждому документу визирующих должностных лиц, если в Перечне конфиденциальной документированной информации отсутствует соответствующая графа (см. разд. 2.3.3). При этом следует иметь в виду, что визирования не требуют лишь некоторые внутренние документы (докладные и объяснительные записки, справки по определенным вопросам и др.).

Сотрудник Службы делопроизводства расписывается за получение конфиденциального документа (проекта) черновика в графе 9 журнала учета созданных/изданных документов, одновременно проставляя в графе 2 дату документа, которая должна соответствовать дате его подписания (утверждения).

Черновик, проект (как неподписанный, так и перепечатанный), лишние экземпляры документа уничтожаются.

В графе 10 журнала учета созданных/изданных документов пишется «Уничтожен» или проставляется аналогичный штамп, заверяемый подписью сотрудника Службы делопроизводства с проставлением даты. В графе 11 при уничтожении проекта документа пишется «Проект уничтожен» или проставляется аналогичный штамп, а при уничтожении лишних экземпляров документа – «Экз. № ___ уничтожены» с указанием номеров экземпляров. Эти отметки заверяются подписью сотрудника Службы делопроизводства с проставлением даты.

В графе 9 журнала учета носителей производится отметка об уничтожении носителя (кроме спецблокнотов) в качестве черновика изданного документа (проекта). Отметка оформляется следующим образом: «Уничтожен как черновик № ___» с указанием номера изданного документа (проекта). Если носитель не являлся черновиком, а уничтожается по каким-либо другим причинам, то в графе 9 пишется «Уничтожен» или проставляется соответствующий штамп, заверяемый подписью сотрудника Службы делопроизводства с указанием даты.

Испорченные, не являющиеся черновиком листы спецблокнота, если он предназначен для использования несколькими исполнителями, должны изыматься из спецблокнота и уничтожаться после возврата спецблокнота каждым исполнителем с отметкой об уничтожении в контрольном листе спецблокнота, заверяемой подписью сотрудника Службы делопроизводства. Такой порядок обусловлен необходимостью исключения необоснованного ознакомления других исполнителей с конфиденциальной информацией, зафиксированной на испорченных листах данным исполнителем. Таким же способом испорченные листы могут уничтожаться и при использовании спецблокнота одним исполнителем. Однако в этом случае допускается уничтожение испорченных листов вместе с обложкой и корешками изъятых листов спецблокнота после использования всех листов.

При уничтожении использованного спецблокнота в контрольном листе проверяются наличие отметок и подписей о номерах документов или об уничтожении испорченных листов, обложка спецблокнота с корешками изъятых листов и с испорченными листами, если они не были уничтожены ранее, а в графе 9 журнала учета носителей пишется слово или проставляется штамп «Уничтожен», заверяемый подписью сотрудника Службы делопроизводства с указанием даты.

Об уничтожении бумажных носителей по решению руководителя организации может составляться акт по форме 6.

Форма 6

АКТ

Мы, нижеподписавшиеся, _____
(должности, инициалы, фамилии

_____
сотрудников Службы делопроизводства)

составили настоящий акт в том, что нами « » 20... г. произведено уничтожение путем сжигания макулатуры за период с « » по « » 20... г.,

(подпись, инициалы, фамилия)

(подпись, инициалы, фамилия)

Бумажные носители могут уничтожаться и с помощью бумагорезательной машины, как правило также после проведения квартальной проверки наличия документов. При уничтожении таким способом тоже может составляться акт об уничтожении с заменой в тексте слова «Сжигание» на слова «Измельчение машиной».

2.6. Особенности создания и изготовления конфиденциальных документов с помощью средств ЭВТ, их печатания, тиражирования, размножения

Конфиденциальные документы, создаваемые в организации, оформляются на бланках, на стандартных листах бумаги формата А4 (210 × 297 мм) или А5 (148 × 210 мм) либо в виде электронных документов, т.е. документов, в которых информация представлена в электронно-цифровой форме [37] или в виде электронных сообщений – информации, переданной или полученной пользователем информационно-телекоммуникационной сети [23, ст. 2]. Они должны иметь установленный состав реквизитов, а также расположение и оформление в соответствии с ГОСТ Р 6.30–2003.

Бланки организации разрабатываются на основе углового или продольного варианта расположения реквизитов. При угловом варианте реквизиты бланка располагаются в верхнем левом углу листа, при продольном варианте – посередине листа вдоль верхнего поля. Требования к учету использования и хранения бланков, печатей, штампов, необходимых для оформления конфиденциальных документов, изложены в разд. 2.7.

Каждый лист документа, оформленный как на бланке, так и на стандартном листе бумаги, должен иметь поля не менее 20 мм – левое, 10 мм – правое, 20 мм – верхнее и 20 мм – нижнее.

Состав реквизитов конфиденциального документа определяется его видом и назначением. Согласование конфиденциального документа в организации оформляется визой уполномоченного должностного лица. Согласование документа, созданного в организации, с другими учреждениями, организациями, предприятиями оформляется грифом (листом) согласования, протоколом или письмом о согласовании.

Конфиденциальные документы составляются на средствах ЭВМ (компьютере) и распечатываются с помощью принтера, в зависимости от степени защиты технических средств и программного обеспечения, непосредственным исполнителем. В случае необходимости распечатка документов производится технической службой (секретарь, инспектор, оператор и т.д.) под ответственность исполнителя конфиденциальных документов.

Окна в помещении, где изготавливаются конфиденциальные документы, целесообразно тонировать или зашторивать. Экран монитора необходимо разворачивать в сторону от окна и входной двери.

На первом листе лицевой стороны документа в левом нижнем углу (допускается на обороте первого листа) указываются количество отпечатанных экземпляров, фамилия исполнителя, фамилия ответственного за распечатку и дату печатания документа. Дополнительно указывается наименование файла, в котором набиралась информация.

Отпечатанные, завизированные и подписанные отправляемые и организационно-распорядительные документы ограниченного доступа (приказы, распоряжения, протоколы и т.д.) вместе с их черновиками и вариантами передаются в Службу делопроизводства. Кадровая документация (персональные данные) передается в Службу кадров для ее регистрации.

Черновики и варианты уничтожаются с подтверждением факта уничтожения записью на копии отправляемого (исходящего) письма или подлиннике организационно-распорядительного документа: «Черновик (и варианты) уничтожены. Дата. Подпись». Запись производится непосредственно исполнителем или сотрудником структурного подразделения в зависимости от того, где были уничтожены черновики и варианты документа (более подробно см. в разд. 2.5).

Организация работы по изготовлению электронных конфиденциальных документов. Изготовление электронных аналогов бумажных конфиденциальных документов сопровождается дополнительными

требованиями к системе их защиты. Для сотрудников централизованно разрабатывается иерархическая система идентифицирующих паролей, кодов и ключей для обеспечения разграничения доступа к информации.

Любое санкционированное или несанкционированное обращение к информации должно регистрироваться (протоколироваться). Рекомендуется систематически проверять используемое пользователями программное обеспечение в целях обнаружения неутвержденных или необычных программ. Применение персоналом неутвержденных (незарегистрированных) защитных мер при работе с компьютером не допускается. При несанкционированном входе в конфиденциальный файл информация должна немедленно автоматически стираться.

Закончив работу на компьютере, сотрудник обязан:

- проверить наличие электронных носителей информации (вне компьютера) по внутренней описи и сдать их в Службу делопроизводства;
- блокировать компьютер персональным ключом и отключить электропитание в помещении;
- запереть и опечатать помещение, сдать его под охрану.

После изготовления конфиденциального документа на принтере и при необходимости переноса текста на дискету (флеш-память) информация в компьютере также должна быть стерта. Факт уничтожения информации подтверждается подписями исполнителя и сотрудника Службы делопроизводства в карточке учета созданного/изданного документа или соответствующей отметкой в электронной карточке.

В Службе делопроизводства должны храниться регулярно обновляемые копии используемых исполнителями электронных носителей. Работа с электронными конфиденциальными документами разрешается только при наличии в организации сертифицированной системы защиты компьютеров и локальной сети.

Размножение и тиражирование конфиденциальных документов. Допускается копирование (тиражирование) исполнителем непосредственно в подразделениях, имеющих копировальную технику, небольших по объему конфиденциальных документов. Порядок использования имеющейся копировальной техники в подразделениях устанавливается их руководителями. Учет выполненных копировальных работ ведется в журналах, которые выдаются Службой делопроизводства сотрудникам, принявшим копировальную технику на ответственное хранение. Дополнительно размноженные экземпля-

ры учитываются в Службе делопроизводства за номером подлинника и в той же учетной форме. Выписки из документов делаются также с разрешения руководителя подразделения и учитываются за новыми номерами на карточках регистрации созданных/изданных документов.

Целевое использование сотрудниками копировальной техники следует строго контролировать.

Централизованное копирование (тиражирование) производится по разрешению руководства структурного подразделения и Службы делопроизводства только для служебных документов по оформленному заказу на бланке установленной формы 7.

Форма 7

сшить
с обложкой
с оборотом
уменьшить
увеличить
(необходимое подчеркнуть)

ЗАКАЗ
на копирование документов

Индекс или наименование
подразделения _____

Исполнитель _____

Телефон _____

Наименование документа (полностью) _____
_____

Стр. _____ Экз. _____
Дата _____ Время _____

Подпись _____

Оператор _____ Дата _____ Время _____

Подпись исполнителя, получившего заказ _____

Дата _____ Время _____

На копирование передаются, как правило, первые, четко напечатанные экземпляры (подлинники) документов в несброшюрованном виде. Заказы выполняются в порядке очередности их поступления. Тираж изготовленных копий должен соответствовать заказу и выдаваться исполнителю вместе с первым экземпляром (подлинником) документа. О выполнении заказа делается соответствующая отметка. Учет выполненных работ по копированию конфиденциальных документов ведется на основании заказов.

Изготовление брошюр производится с разрешения руководства Службы делопроизводства. Копирование (тиражирование) бланков документов, используемых в организации, не разрешается. Запрещается также использовать для копирования документов копировальную технику, не оборудованную техническими средствами защиты от излучений ими электромагнитных волн.

Тиражирование и размножение конфиденциальных документов и изданий в типографии производится с разрешения Службы делопроизводства (если такая служба существует в организации) и под контролем Службы безопасности. В типографиях учет тиражируемых документов и изданий может осуществляться с учетом других открытых материалов.

По окончании печатания документов и изданий набор должен быть разобран, а печатные формы аннулированы, о чем составляется акт за подписями представителя организации – заказчика и типографии.

2.7. Учет использования и хранения печатей, штампов, бланков, необходимых для оформления конфиденциальных документов

2.7.1. Печати и штампы

Печать – это устройство, содержащее клише для нанесения оттисков на бумагу [154].

Федеральные органы власти применяют печати с изображением Государственного герба Российской Федерации. Порядок применения гербовых печатей устанавливается российским законодательством. Порядок применения печатей с изображением Государственного герба регулируется Федеральным конституционным законом «О Государственном гербе Российской Федерации» [3]. Негосударственные организации применяют печать с наименованием самой организации в соответствии с уставом организации.

Штамп – устройство прямоугольной формы для проставления отметок справочного характера о получении, регистрации, прохождении, исполнении документов и др. Согласно ГОСТ Р 6.30–2003 оттиск печати заверяет подлинность подписи должностного лица на документах, удостоверяющих права лиц, фиксирующих факты, связанные с финансовыми средствами и обязательствами, а также на иных документах, предусматривающих заверение подлинности подписи.

В соответствии с уставом в организации могут использоваться круглые печати структурных подразделений и печати для отдельных категорий документов («Для пакетов», «Для договоров», «Для копий»), металлические выжимные печати для опечатывания помещений и удостоверения специальных пропусков. Печати изготавливаются в строго ограниченном количестве и исключительно в служебных целях. Решение о необходимости изготовления печатей и их количестве принимает руководство организации по согласованию с руководителем Службы делопроизводства и Службы безопасности. Заявка на изготовление печати и ее эскиз оформляется в соответствующих подразделениях и передается в Административно-хозяйственную службу, которая размещает заказ на предприятии – изготовителе печатей.

Печатью заверяются подписи руководителя, его заместителей, финансовой службы, главного бухгалтера, а также других должностных лиц, которым доверенностью или распорядительным документом руководителя предоставлены соответствующие полномочия. Передача печатей посторонним лицам и вынос их за пределы территории организации не допускаются.

Служба делопроизводства ведет общий учет имеющихся в организации печатей и штампов в специальном журнале (форма 8) с проставлением их оттисков. Выдача печатей и штампов осуществляется под расписку работникам, персонально ответственным за их использование и хранение. Листы журнала учета печатей и штампов нумеруются, прошнуровываются и опечатываются.

Печати хранятся в надежно запираемых шкафах. Ответственность за законность использования и хранение главной печати организации возлагается на руководителя. Ответственность за хранение, законность использования других печатей возлагается на руководителей соответствующих подразделений. Порядок хранения печатей и штампов, правильность их использования в структурных подразделениях проверяется подразделением, ответственным за учет печатей. В случае служебной необходимости по решению руководителя организации допускается изготовление дополнительных экземпляров печати.

Форма 8

Журнал учета печатей и штампов

№ п/п	Оттиск печати (штампа)	Наименование печати (штампа)	Дата получения печати (штампа) от изготовителя	Предприятие-изготовитель, дата и номер сопроводительного документа	Кому выдана (должность, подразделение)
1	2	3	4	5	6

Окончание

Подпись работника	Дата возврата печати	Подпись работника	Дата уничтожения печати	Дата, номер акта
7	8	9	10	11

Пришедшие в негодность и утратившие значение печати и штампы подлежат возврату по месту выдачи, где они уничтожаются по акту с соответствующей отметкой в журнале учета.

2.7.2. Бланки документов

Бланки документов, тетрадей и блокнотов для записей служат одним из средств защиты конфиденциальных документов, в том числе от подделки, а также являются полиграфической продукцией, подлежащей учету.

Бланки изготавливаются только полиграфическими и штемпельно-граверными предприятиями, имеющими лицензии на соответствующий вид деятельности и сертификаты о наличии технических и технологических возможностей для изготовления указанного вида продукции на качественном уровне.

В организациях используются бланки документов, изготовленные типографским способом. В случае применения компьютерного шаблона бланка последний должен иметь неизменяемый формат.

Не разрешено тиражирование бланков документов средствами оперативной полиграфии (ксерокопии) с помощью компьютерной техники при распечатке на принтере. Допускается тиражирование средствами оперативной полиграфии (ксерокопирование) документов на бланке, предназначенных для рассылки, при условии заверения каждой копии документа печатью Службы делопроизводства.

Организация работы по изготовлению бланков возлагается на Административно-хозяйственную службу, которая:

- получает от Службы делопроизводства заявки на изготовление бланков документов, а также, при необходимости, их образцы (макеты);
- оформляет заказы на изготовление в типографии печатно-бланочной продукции;
- получает и ведет учет и выдачу в Службу делопроизводства изготовленных бланков документов.

Изготовленные бланки документов нумеруются типографским способом или нумератором в Службе делопроизводства. Порядковый номер проставляется в нижней части оборотной стороны бланка. Учет бланков ведется раздельно по их видам в журнале (форма 9).

Бланки выдаются работникам, ответственным за делопроизводство в подразделениях, под роспись в журнале учета выдачи бланков (форма 10).

Форма 9

Журнал учета бланков

Наименование вида бланка	Дата поступления	Дата и номер сопроводительного документа	Наименование организации — поставщика бланков	Количество экземпляров бланков	Серия и номера гербовых бланков
1	2	3	4	5	6

Форма 10

Журнал учета выдачи бланков в структурные подразделения

Наименование вида гербового бланка	Количество экземпляров бланков	Серия и номера гербовых бланков	Наименование подразделения, ФИО получателя	Расписка в получении	Примечание
1	2	3	4	5	6

В структурных подразделениях бланки документов должны использоваться строго по назначению и храниться в надежно запираемых шкафах. Передача бланков другим организациям и лицам не допускается. Ответственность за обеспечение сохранности бланков и правильность их использования несут работники, ответственные за делопроизводство в подразделениях, и руководители подразделений. Уничтожение бланков, не требующих обращения, осуществляют по акту с отметкой в учетно-регистрационной форме, в том числе электронной.

Контроль за изготовлением, использованием и хранением бланков возлагается на Службу делопроизводства.

Лица, персонально ответственные за учет, использование и хранение бланков, назначаются распорядительным документом руководителя организации. Регистрационно-учетные формы необходимо включать в номенклатуру дел.

Проверку наличия, использования и хранения бланков проводят не реже одного раза в год Экспертной комиссией, назначаемой распорядительным документом руководителя организации. О проведенных проверках делают отметки в учетно-регистрационных формах после последней записи. В случае обнаружения нарушений при изготовлении, учете, хранении и использовании бланков комиссия проводит служебное расследование, результаты которого оформляют актом и доводят до сведения руководства организации.

ГЛАВА 3

ОРГАНИЗАЦИЯ КОНФИДЕНЦИАЛЬНОГО ДОКУМЕНТООБОРОТА

3.1. Особенности учета и регистрации конфиденциальной документированной информации

Документооборот – движение документов с момента их создания или получения до завершения исполнения, помещения в дело и (или) отправки [76, разд. II, п. 4]. В документообороте организации выделяются следующие документопотоки:

- поступающая документация (входящая);
- отправляемая документация (исходящая);
- внутренняя документация (создаваемая/издаваемая).

Основой организации конфиденциального документооборота является учет конфиденциальной документированной информации на каждом этапе ее прохождения.

Регистрация документа – присвоение документу регистрационного номера и запись в установленном порядке сведений о документе [Там же]. Регистрацией документа является также запись учетных данных о документе по установленной форме, фиксирующая факт его получения, создания или отправления [163].

Основной целью организации конфиденциального документооборота является учет и регистрация конфиденциальных документов с целью формирования контрольной и справочно-информационной базы для оперативного нахождения, контроля исполнения, представления необходимых справок о конфиденциальных документах, а также для проверки их наличия, обеспечивающей постоянный мониторинг сохранности и защиты каждого документа и своевременное фиксирование его местонахождения.

Учет и регистрация конфиденциальных документов включает следующие этапы:

- фиксирование факта поступления документа;
- фиксирование создания/издания документа;
- фиксирование отправления документа;
- фиксирование местонахождения документа;

• обеспечение поиска документов при проверке их наличия или необходимости обращения к документу;

• обеспечение справочно-информационной и контрольной работы по документам;

• предупреждение утраты копий и экземпляров документа, черновиков и редакций, приложений и отдельных листов;

• предотвращение утери черновиков и вариантов документа;

• подтверждение факта уничтожения всех черновых материалов, возникших в процессе исполнения документа;

• подтверждение факта передачи документа на отправку или исполнение сотрудникам Службы делопроизводства.

Для решения этих задач целесообразно вести следующие виды учета конфиденциальной документированной информации:

• поступивших пакетов с документированной информацией (см. разд. 3.2.1);

• поступивших документов с их регистрацией (см. разд. 3.2.2);

• созданных/изданных (внутренних) документов с их регистрацией (см. разд. 3.3);

• отправляемых документов (см. разд. 3.5.1);

• распределения внутренних (созданных/изданных) документов (см. разд. 3.5.2);

• отправляемых пакетов с документированной информацией (см. разд. 3.5.2);

• документов и дел инвентарного (выделенного) хранения (инвентарным учетом также называют списочный учет – см. разд. 3.6);

• информации и ее носителей при ее автоматизированной обработке с помощью Реестра конфиденциальной информации и АИС (см. разд. 3.7).

Данные о конфиденциальном документе заносятся в журнал или карточку учета поступивших документов (форма 1).

Учету подлежат все без исключения внутренние (созданные/изданные в организации), а также полученные от других организаций, предприятий и отправляемые в другие организации конфиденциальные документы.

Регистрация конфиденциальных документов включает присвоение и проставление в учетных, а также регистрационно-контрольных формах и на самом документе регистрационных номеров и запись учетных и поисковых данных о конфиденциальных документах (учетном и регистрационном номере, дате, авторе, заголовке, количестве листов, степени конфиденциальности, местонахождении и др.).

Форма 1

Регистрационный номер и отметка конфиденциальности документа	Дата поступления	Вид и заголовок документа	Откуда поступил	Номер и дата документа организации-отправителя	Количество листов основного документа	Количество листов приложений
1	2	3	4	5	6	7

Окончание

Кому выдан	Количество листов	Подпись за получение и дата	Подпись за возврат и дата	Индекс (номер) дела, номера листов дела	Номер по инвентарному (выделенному) учету	Примечание
8	9	10	11	12	13	14

Допускается ведение регистрации в журналах или на карточках отдельно от регистрации другой открытой документации. При незначительном объеме конфиденциальных документов допускается вести регистрацию в массиве открытой документации.

Документы на бумажном носителе учитываются по количеству листов, а издания (книги, журналы, брошюры, диски) – поэкземплярно.

Учет конфиденциальных документов предусматривает не только учет факта их создания/издания или получения и отправления, но и обязательную фиксацию всех перемещений по структурным подразделениям организации, руководителям и исполнителям в процессе рассмотрения, использования и исполнения этих документов.

Учет, регистрация и хранение конфиденциальных документов, как правило, осуществляются централизованно в Службе делопроизводства.

Внутренние (созданные/изданные) конфиденциальные документы должны учитываться и регистрироваться независимо от того, направляются они в другие организации или являются внутренними (см. разд. 3.3). Учет внутренних конфиденциальных документов ведется отдельно от их регистрации.

Порядок исполнения конфиденциальных документов предполагает в качестве одной из задач исполнителя ведение их учета (см. разд. 3.4).

Экспедиционные технологии обработки отправляемой конфиденциальной документированной информации и пакетов предполагают их регистрацию и учет (см. разд. 3.5). Учет отправляемых конфиденциальных документов ведется отдельно от их регистрации.

Порядок инвентарного или списочного (выделенного) учета конфиденциальных документов (дел и носителей конфиденциальной документированной информации) рассмотрен в разд. 3.6. Этот вид конфиденциальной документированной информации невозможно либо нецелесообразно подшивать в дела в соответствии с режимом доступа к информации, внешними особенностями и другими делопроизводственными условиями (вид носителя, например формат, сброшюрованность и т.д.).

Независимо от вида учета и регистрации конфиденциальной документированной информации ее возможно учитывать в журналах или карточках, в том числе в электронных картотеках (автоматизированной системе учета конфиденциальных документов и их регистрации). При большом объеме документов целесообразно использовать карточный, а также автоматизированный способ учета, так как он сокращает время на поиск документов, дает возможность осуществлять контроль исполнения документов без изготовления специаль-

ных контрольных карточек, ускоряет и повышает качество проведения проверок наличия документов.

При карточном способе учета конфиденциальной документированной информацией (как и ее носителей) необходимо вести контрольный журнал, предназначенный для учета, обеспечения последовательности проставления номеров и контроля за местонахождением этой информации, находящейся в обращении, ускорения ее поиска, а также для проставления отметок о проверках на ее наличие.

Контрольный журнал заводится по каждому виду карточного учета и регистрации документов (поступающие, внутренние, отправляемые) и отдельно для носителей. Журнал заполняется по форме 2.

При обработке конфиденциальной документированной информации (переводе на другой вид учета, регистрации, отправлении, подшивке в дело, уничтожении, передаче на архивное хранение) соответствующий учетный номер в контрольном журнале округляется без указания окончательного местонахождения документа. Возможно вместо контрольного журнала вести карточную форму учета или автоматизировать данный процесс с помощью электронных картотек.

Журналы или картотеки учета внутренних, поступивших и отправляемых конфиденциальных документов ведутся в течение календарного года. Конфиденциальные документы, не исполненные в текущем году, подлежат переводу на учет следующего года (кроме организационно-распорядительных документов и протоколов) с отметкой об этом в учетных формах текущего года.

В учетных формах не разрешается делать какие-либо исправления с помощью корректирующей жидкости или подчистки бритвой. Исправления аккуратно вписываются работником Службы делопроизводства рядом с ошибочной записью или выше ее и заверяются его подписью.

Журналы и картотеки содержат в совокупности конфиденциальную информацию, поэтому их следует хранить в условиях, исключающих доступ к ним посторонних лиц. По окончании рабочего дня сотрудник Службы делопроизводства проверяет правильность учета документов и их наличие. Перемещение конфиденциальных документов между сотрудниками фиксируется в передаточном журнале Службы делопроизводства.

Листы журналов должны быть перед заведением пронумерованы, прошиты и опечатаны печатью Службы делопроизводства. На оборотной стороне последнего листа журналов проставляется заверительная надпись с указанием количества листов, подписываемая сотрудником, ответственным за ведение журнала.

Форма 2

Учетный и регистрационный номер документа (носителя), дата учета и регистрации	Вид и наименование носителя, номера экземпляров, количество листов в экземпляре	Местонахождение документа (носителя)	Отметки о проведении проверки наличия документов (носителей)
1	2	3	4

Заверительная надпись на картотеку учета конфиденциальных документов с указанием количества карточек в ней составляется по окончании года на отдельной карточке и помещается в конце картотеки.

Если содержащиеся в регистрационно-контрольной форме сведения по совокупности являются конфиденциальными, то журналам и картотекам должен присваиваться гриф конфиденциальности (отметка конфиденциальности). На карточках учета и регистрации отметка конфиденциальности не проставляется, поскольку отметка находится в регистрационном номере. При регистрации конфиденциальных документов к их регистрационному номеру добавляется краткий гриф ограничения доступа, например ДСП, КФД, СКФД (см. разд. 2.2).

Реферативные информационные издания в журнальном или сброшюрованном карточном исполнении, в которых содержатся сведения конфиденциального характера, выпускаются с той же отметкой об ограничении доступа к информации или отметкой конфиденциальности документа. Изъятые из этих изданий реферативные информационные листы и карточки, не содержащие конфиденциальной информации, учитываются и хранятся как открытые материалы. Факт изъятия карточек и листов заверяется подписями двух лиц на обложке издания [209].

Для того чтобы отличить номер созданного документа от номера документа инвентарного (выделенного) учета, целесообразно на конфиденциальном документе инвентарного учета перед номером проставлять индекс, например И, что означает «инвентарный», или В – «выделенный». В журнале (карточке) инвентарного (выделенного) учета конфиденциальных документов индекс не проставляется.

Электронные конфиденциальные документы, базы данных, содержащие эти документы, создаются, обрабатываются и хранятся в автоматизированных информационных системах, или, иными словами, в системе защищенного электронного документооборота организации.

Бумажный учет и регистрацию конфиденциальных документов можно перевести на технологию автоматизированного (электронного) учета и регистрации в АИС. Электронный учет и регистрация включают в себя следующие технологии:

- ввод в систему исходных сведений о конфиденциальной документированной информации и формирование электронных форм журналов или картотек (см. формы в следующих подразделах);
- контроль правильности внесения записей и их соответствия учитываемым документам;

• вывод выходных форм (возможна разработка аналитических выходных форм) на монитор или распечатку (при необходимости) на бумажном носителе введенных записей отдельно по каждому конфиденциальному документу или по всем документам за рабочий день;

• распечатка при необходимости учетной формы (листа журнала, карточки) выдачи документа.

В электронные формы журналов и картотек данные о документах вносятся в хронологической последовательности их поступления в Службу делопроизводства. Бумажные распечатки записей исходных сведений о документах, внесенных в электронную форму, выполняют учетную функцию удостоверения факта поступления, отправления или создания/издания документа, его местонахождения и места хранения. Распечатки в комплексе формируют традиционный журнал (картотеку), в котором записи о документах располагаются в валовом порядке. Журнал является одновременно:

• описью конфиденциальной документированной информации;

• страховым массивом учетных данных о документах на случай порчи или уничтожения электронных форм.

Электронная система учета реализует функцию контрольного, справочного и поискового обслуживания пользователей и исполнителей.

Сведения об изменении местонахождения конфиденциальной документированной информации вносятся в электронные формы, которые выполняют в данном случае роль контрольной картотеки. По окончании исполнения делается новая распечатка полных сведений о документе, которая помещается в традиционную картотеку вместо находившейся там распечатки исходных сведений о документе.

Выдача конфиденциальных документов исполнителям осуществляется по распечаткам учетного журнала (карточек учета) документов, в которых фиксируется роспись за получение и возврат документов, или отметкам в электронных картотеках. Документы, например, инвентарного (выделенного) учета могут также выдаваться под роспись в распечатке учета выдачи документа (см. разд. 3.6).

Учет конфиденциальной информации, циркулирующей в АИС или системах электронного документооборота, производится с помощью Реестра конфиденциальной информации и автоматизированной информационной системы организации (см. разд. 3.7). Более подробно организация системы защищенного электронного документооборота рассмотрена в гл. 8.

3.2. Обработка поступающих конфиденциальных документов, их учет и регистрация

3.2.1. Экспедиционные технологии обработки и учета поступающих пакетов с конфиденциальными документами

Конфиденциальные документы должны пересылаться (доставляться) между организациями в запечатанных пакетах, оформленных соответствующим образом. В процессе экспедиционной обработки поступивших документов необходимо выполнять следующие меры по защите конфиденциальной информации и ее носителей:

- не допускать попадания в организацию конфиденциальных документов других предприятий и организаций;
- проверять целостность конвертов, пакетов, упаковок (далее – пакетов) с документами, т.е. убедиться, что они не вскрывались на пути следования от отправителя до адресата;
- предотвращать утрату документов после вскрытия пакета;
- исключать возможность ознакомления с конфиденциальными документами технических работников организации, не имеющих к ним доступа;
- исключать возможность ознакомления любых работников организации с информацией, имеющей пометку «Лично»;
- не допускать утерю документов и их частей за счет неполного изъятия их из пакетов;
- проверять комплектность конфиденциального документа, наличие всех листов, экземпляров и иных частей, отсутствие факта подмены документа.

Пакеты, содержащие конфиденциальные документы, поступают из почтового отделения связи (ценные, заказные и простые отправления) с помощью фельдъегерской связи (если такая связь в организации существует), от курьеров предприятий и организаций, от посетителей. Конфиденциальная документированная информация может также приходить по факсимильной связи, электронной почте, по телеграфной и телетайпной связи. При получении пакетов сотрудник экспедиционного подразделения Службы делопроизводства обязан:

- проверить на пакете соответствие адресата, проставление номеров документов и организации-отправителя, целостность упаковки, сохранность прошивки и оттиска печати;
- убедиться, что содержимое пакета не просматривается;

• проверить на пакете и сопроводительном документе на него (реестре, описи и др.) соответствие наименований адресата и отправителя, номеров документов, номеров экземпляров (если указаны);

• расписаться в сопроводительном документе за принятые пакеты с проставлением даты и, при необходимости, печати или специального штампа.

Следует учитывать ту особенность, что на пакетах, а часто на самих конфиденциальных документах не ставится гриф ограничения доступа. Это объясняется нежеланием отправителя обращать внимание посторонних лиц на отметку о конфиденциальности. Поэтому предварительное рассмотрение и распределение всей поступающей документированной информации должно выполняться квалифицированным сотрудником Службы делопроизводства, обладающим знаниями структуры организации, функций структурных подразделений и обязанностей работников, состава и Перечня конфиденциальной документированной информации и таких же перечней структурных подразделений организаций (см. разд. 2.3).

Документы, поступающие централизованно по линиям факсимильной связи, электронной почты, также просматриваются этим сотрудником в целях определения возможной их конфиденциальности. Сотрудник вскрывает все пакеты (кроме имеющих пометку «Лично»), проверяет правильность адресования и комплектность документов.

Первичная обработка поступивших конфиденциальных документов включает проверку правильности доставки документов, их наличия и приложений к ним, а также распределение документов на регистрируемые и не подлежащие регистрации. Поскольку поступившие документы делятся также на имеющие отметку конфиденциальности и не имеющие такой отметки, то при вскрытии пакетов проверяется соответствие на пакете и документе отправителя и адресата отметки конфиденциальности, номеров документов, номеров экземпляров документа (если указаны на пакете). Пакеты должны быть вскрыты таким образом, чтобы можно было убедиться, что в них не осталось каких-либо вложений.

В документах проверяется наличие листов, а в документах, имеющих приложения, кроме того, соответствие учетных номеров, отметки конфиденциальности, номеров экземпляров, количества листов приложения записям в отметке о наличии приложения, содержащейся в основном документе (сопроводительном письме).

Пакеты с пометкой «Лично» вскрываются работником, которому они адресованы, или уполномоченным им лицом. По усмотрению лица, вскрывшего пакеты, перечисленные выше данные проверяются им самим или сотрудником Службы делопроизводства.

Документы, не отнесенные к разряду конфиденциальной информации, повторно внимательно просматриваются и передаются сотруднику, занятому обработкой и регистрацией открытой документации [209].

Все поступающие пакеты в момент их получения целесообразно учитывать, с тем чтобы можно было обнаружить их возможную утрату до регистрации содержащихся в них документов. Для этого следует вести журнал учета поступивших конфиденциальных пакетов, который предназначен, кроме того, для проставления отметок о взятии поступивших документов на различные виды учета, а также о возврате ошибочно присланных документов. Журнал ведется по форме 3.

Если на пакетах указан другой адресат, то они не принимаются.

При нарушении оформления пакетов, несоответствии данных на пакете и в сопроводительном документе, а также повреждении упаковки составляется акт в двух экземплярах, который подписывается сотрудником Службы делопроизводства и лицом, доставившим пакеты. Второй экземпляр акта направляется отделению связи, доставившему пакет, или организации – отправителю пакета, если он доставлен, минуя отделение связи. Если повреждение пакета позволяет изъять документ или прочесть его, то об этом сообщается руководству организации и Службы делопроизводства, а пакет не принимается до принятия решения.

После проставления подписи за принятые пакеты сотрудник Службы делопроизводства заполняет графы 1–3 журнала учета поступивших пакетов, при этом в графе 3 количество пакетов указывается прописью, а лицо, доставившее пакеты, заверяет эти данные своей подписью в графе 4. Дата поступления пакетов может проставляться перед началом их учета за каждый день. В этом случае графа 1 в журнал не включается.

Затем до вскрытия пакетов заполняются графы 5–6 журнала (графа 6 заполняется, если на пакете есть номера документов). Порядковые номера пакетов ежедневно начинаются с № 1. Рядом с номером пакета, имеющего пометку «Лично», проставляется слово «Лично». Если на пакете рядом с номером документа указаны номера экземпляров, то они переносятся в журнал.

Форма 3

Дата поступления пакетов	Откуда поступили	Количество пакетов	Подпись лица, доставившего пакеты	Порядковые номера пакетов
1	2	3	4	5

Окончание

Номера и отметки конфиденциальности вложенных в пакеты документов	Номера, присвоенные поступившим документам	Учетные номера возвращенных и взятых на учет инвентарного (выделенного) хранения документов	Отметка о возврате ошибочно присланных документов	Отметка о проверке наличия
6	7	8	9	10

При несоответствии на пакете и документе или на документе и приложении учетных номеров, недостаче или излишке листов и экземпляров документа, а также в случае, если документ направлен в организацию ошибочно, руководителем Службы делопроизводства и сотрудником, вскрывшим пакет, составляется в двух экземплярах акт, второй экземпляр которого вместе с лицевой стороной пакета (при несоответствии данных на пакете и документе) немедленно направляется отправителю. О недостаче листов или экземпляров сообщается, кроме того, руководителю Службы делопроизводства данной организации-отправителя.

Ошибочно присланные документы, лишние листы и экземпляры вместе с актом направляются с сопроводительным письмом организации-отправителю. В графе 9 журнала учета поступивших пакетов производится отметка о возврате с указанием того, сколько листов или какие экземпляры и почему возвращаются, номера и даты сопроводительного письма, например: «Пять листов (экз. № __) возвращены как лишние с № 23 КТ от 14.09.2010 г.» или (при возврате документа полностью) «Документ возвращен как ошибочно присланный с № ПК от 20.08.2010 г.».

Ошибочно присланные документы могут по согласованию с организацией-отправителем пересылаться по назначению, под их учетными номерами, в новых пакетах с вложением в них лицевой стороны пакета организации-отправителя. В этом случае в графе 9 журнала учета поступивших пакетов делается отметка о пересылке с указанием организации, которой направлен документ, номера и даты сопроводительного письма.

О несоответствии на пакете и документе и приложении отметки конфиденциальности или номеров экземпляров организации-отправителю сообщается письмом. Журнал учета пакетов можно вести в автоматизированном режиме – в автоматизированной информационной системе, если такая система существует в организации или будет разработана.

3.2.2. Учет и регистрация поступивших (входящих) конфиденциальных документов

После вскрытия пакета и проверки правильности вложений поступившей конфиденциальной документированной информации присваивается очередной регистрационный входящий номер, который также проставляется в графе 7 журнала учета поступивших пакетов.

Учет и регистрация поступивших конфиденциальных документов осуществляются одновременно в единой форме (см. разд. 3.1, форма 1), как правило, в день поступления.

Как отмечалось ранее, допускается ведение регистрации в журналах или на карточках отдельно от регистрации другой открытой документации. При этом в регистрационно-контрольных формах, в том числе электронных, к входящему регистрационному номеру документа добавляется гриф ограничения допуска к документу в краткой форме, например: ДСП – «Для служебного пользования». Для документов, поступивших из других организаций, имеющих другое обозначение грифа ограничения доступа, во входящих регистрационно-контрольных формах к регистрационному входящему номеру добавляется обозначение отметки в краткой форме, например: КФД – конфиденциально или СКФД – строго конфиденциально. Более подробно особенности применения отметки конфиденциальности рассмотрены в разд. 2.2.

В момент регистрации заполняются графы 1–7. В графе 1 проставляется регистрационный номер, присвоенный документу, и аббревиатурой отметки конфиденциальности документа. В графе 5 указываются номер, присвоенный документу в организации-отправителе, и дата подписания (утверждения) документа. Если документ прислан без сопроводительного письма, то в графе 6 проставляется количество его листов, а в графе 7 делается прочерк. Если документ имеет сопроводительное письмо, то в графе 6 проставляется количество листов сопроводительного письма, а в графе 7 – количество листов приложений. При этом, если все приложения имеют гриф конфиденциальности, указывается общее количество листов всех приложений; если часть приложений не имеет отметки конфиденциальности, то количество их листов проставляется через «+» к листам конфиденциальных приложений, например: 7+3 н/к (н/к означает «не конфиденциальные»).

При поступлении документа в двух и более экземплярах проставляется общее количество листов всех экземпляров. При этом на одном экземпляре проставляется входящий штамп, а на первых листах других экземпляров – отметка «К вх. №.__».

При учете документов, присланных для согласования, подписания, утверждения, ознакомления, т.е. всех документов, подлежащих возврату, отметка о поступлении проставляется на обороте последнего листа основного документа и каждого приложения.

Если в организацию возвращены отправленные ранее без сопроводительного письма все или часть экземпляров документа, то производится отметка об их возвращении без присвоения входяще-

го номера. Эта отметка проставляется в графе 8 журнала учета поступивших пакетов напротив возвращенного номера вложенного в пакет документа, например: № 12 (при возврате документа), № 2 (при возврате документа выделенного хранения), вх. № 15 (при возврате документа, зарегистрированного по входящему номеру). Одновременно в графе 15 журнала учета созданных/изданных документов или в графе 11 журнала (карточки) учета документов инвентарного (выделенного) хранения (см. разд. 3.6) делается запись: «Экз. № __ возвращены, п/ж № __ з а __» с проставлением номеров экземпляров, порядкового номера и даты поступления пакета, в котором находились возвращенные экземпляры. В графе 14 журнала учета поступивших документов (под отметкой об отправлении) производится запись: «Возвращен, п/ж № __ за __» с проставлением порядкового номера и даты поступления пакета с возвращаемым документом (п/ж означает «журнал поступивших пакетов», см. форму 3 в разд. 3.2.1).

Если документ отправлялся и (или) возвращен с сопроводительным письмом, то он регистрируется за очередным входящим номером конфиденциального документа, подлежащего выделенному хранению, переводится затем без сопроводительного письма на учет документов инвентарного (выделенного) хранения (см. разд. 3.6). Сопроводительное письмо подшивается в дело.

3.3. Учет и регистрация внутренних (созданных/изданных) конфиденциальных документов

Учет и регистрация внутренних (созданных/изданных) конфиденциальных документов начинается на стадии подготовки их проектов. Учет проектов конфиденциальной документированной информации изложен в разд. 2.5 [209].

Для регистрации внутренних конфиденциальных документов исполнитель сдает сотруднику Службы делопроизводства:

- все экземпляры подписанного руководителем документа;
- приложения к документу (при наличии);
- черновики основного документа и приложений, редакции и варианты документа, рабочие записи.

О сдаче и уничтожении указанных материалов сотрудник Службы делопроизводства делает отметку в учетной карточке документов, находящихся у исполнителя (см. разд. 3.4). Отметка заверяется подписями сотрудника Службы и исполнителя. Факт уничтожения

черновика и других материалов подтверждается также отметкой на копии документа, остающейся в деле Службы делопроизводства, например: «Черновик уничтожен. Дата. Подпись сотрудника делопроизводства». Черновики и другие материалы уничтожаются путем измельчения, исключающего возможность восстановления текста. Попытки исполнителей оставить в своем распоряжении какие-либо неучтенные материалы по исполненному документу должны рассматриваться руководством организации как грубое нарушение работы с конфиденциальными документами и трудовой дисциплины [209].

Внутренние (создаваемые/издаваемые в организации) конфиденциальные распорядительные документы – постановления, распоряжения, приказы, указания, решения, а также протоколы – имеют регистрационный номер, который состоит из ежегодной валовой нумерации в пределах каждого из этих видов документов, с добавлением отметки конфиденциальности.

Регистрация конфиденциальных распорядительных документов ведется отдельно от их учета. Для обеспечения последовательности проставления таких номеров, ускорения их поиска журналы учета или карточки (электронные карточки в АИС) созданных конфиденциальных документов необходимо вести по каждому их виду отдельно. Журнал или карточка заполняются по форме 4.

В графе 3 проставляется учетный номер документа, присвоенный ему на стадии учета его проекта до основной регистрации по журналу учета созданных/изданных документов (см. разд. 2.5). Графы 1–4 обязательны, целесообразность включения граф 5–7 должна определяться главным образом объемом и характером справочной работы по конфиденциальным распорядительным документам.

Приложения к созданным (изданным) документам являются самостоятельными документами и имеют свои номера по соответствующим видам учета.

3.4. Технологии исполнения и контроля за исполнением конфиденциальных документов

В соответствии с разрешительной системой доступа к конфиденциальной информации (см. гл. 4) после учета и регистрации конфиденциальных документов осуществляется их рассмотрение и передача для исполнения.

Форма 4

Порядковый регистрационный номер и отметка конфиденциальности	Дата	Учетный номер	Заголовок	Количество экземпляров	Количество листов в экземпляре	Отметка о местонахождении	Отметка о проверке наличия
1	2	3	4	5	6	7	8

При большом объеме поступающих документов целесообразно их предварительно рассмотреть и распределить по уровням принятия решений по ним. С этой целью разрабатывается Перечень поступивших документов, направляемых на исполнение без доклада руководителю организации. В этом Перечне полномочия по принятию решений по исполнению документов делегируются на соответствующий уровень управления. В Перечень включаются конкретные наименования поступающих документов, которые имеют, как правило, типовой и повторяющийся характер и адресуются заместителям руководителя организации, руководителям структурных подразделений или непосредственным исполнителям без рассмотрения их руководителем организации (форма 5). Разработку Перечня целесообразно возлагать на постоянно действующую Экспертную комиссию по защите конфиденциальной информации (см. разд. 4.1.2). При его подготовке необходимо учитывать требования разрешительной системы доступа к конфиденциальной информации в части обеспечения правомерности доступа к документам в процессе делегирования полномочий по их рассмотрению.

Перечень подписывается председателем и членами экспертной комиссии и вводится в действие приказом руководителя организации. В приказе определяется должностное лицо, которому предоставляется право адресования документов, включенных в Перечень. Ими могут быть руководители Службы делопроизводства и Службы безопасности или помощник (референт) руководителя организации. Это лицо, в соответствии с Перечнем, лишь адресует документы без указания порядка и сроков их исполнения, поскольку руководители различных уровней при адресовании им документов в резолюции определяют их характер и сроки исполнения. При адресовании документов непосредственным исполнителям последние знают, что нужно сделать по исполнению документа и в какие сроки, так как такие документы являются типовыми и характер их исполнения однотипен.

Перечень позволяет сократить путь и время движения документов до непосредственных исполнителей и, следовательно, ускорить процесс их исполнения, освободить руководство от рассмотрения вопросов, которые могут быть решены непосредственными исполнителями документов, уменьшить трудозатраты на рассмотрение, исполнение и обработку документов, обеспечить выполнение требований разрешительной системы доступа к поступившим конфиденциальным документам (см. гл. 4).

Не включенные в Перечень документы, подлежащие рассмотрению непосредственно руководителем организации, передаются ему (его помощнику, секретарю) под подпись в журнале передачи конфиденциальных документов (форма 6), если они не рассматриваются в присутствии сотрудника Службы делопроизводства, ответственного за их учет.

Форма 5

№ п/п	Наименование адресуемых документов	Должность, ФИО лица, которому адресуются документы	Должность, ФИО лица, которому адресуются документы при временном отсутствии основных адресатов
1	2	3	4

Форма 6

Номер документа	Количество листов	Подпись за получение и дата	Подпись за возврат и дата
1	2	3	4

При одновременном получении и возврате нескольких документов может проставляться одна подпись за все документы. Если часть документов, рассматриваемых в присутствии сотрудника Службы делопроизводства, остается у руководителя, то в журнал передачи конфиденциальных документов вносится только эта часть.

После рассмотрения и нанесения на них резолюций документы передаются исполнителям (см. разд. 3.1). Требующие исполнения внутренние конфиденциальные распорядительные документы (приказы, протоколы и решения коллегиальных органов и др.) также передаются исполнителям. Если исполнителей несколько, то документ в первую очередь передается ответственному исполнителю, указанному в резолюции, а при отсутствии указания – поставленному в резолюции первым.

При получении документа исполнитель должен проверить соответствие учетного и регистрационного номеров документа и количества его листов (с пересчетом) записям в регистрационных и учетных формах. Если в процессе исполнения документа выявится, что исполнителю требуется лишь часть документа, то документ полностью сдается в Службу делопроизводства с погашением подписи исполнителя за получение, а исполнителю под новую расписку в регистрационно-учетных формах выдается необходимая ему часть документа.

Передача документов между исполнителями должна производиться через Службу делопроизводства или Службу контроля исполнения (если такая отдельная служба предусмотрена штатным расписанием организации) при возврате в течение рабочего дня, по разовой расписке.

При карточном учете в случае изменения местонахождения документа в контрольном журнале карандашом проставляется новое его местонахождение, а карточка перемещается в соответствующую ячейку картотеки [209].

Если документ одновременно выдается по частям нескольким исполнителям, то при карточном учете подписи за получение документа проставляются на основной карточке, которая ставится в ячейку картотеки по фамилии одного из исполнителей, в ячейки остальных исполнителей помещаются сигнальные карточки, которые могут быть либо дубликатом основной карточки с указанием количества листов (экземпляров), выданных исполнителю, либо содержать лишь сведения об учетном номере документа, фамилию соответствующего исполнителя, количестве полученных им листов (экземпляров). Применение автоматизированных электронных картотек АИС контроля исполнения упрощает данный процесс.

Документы, требующие подготовки ответа или принятия решения, подлежат контролю. Организация контроля должна обеспечивать качественное и своевременное исполнение конфиденциальных документов. Ответственность за качество исполнения документов несут исполнители и руководители подразделений, в которых работают исполнители. Контроль за сроками исполнения конфиденциальных документов осуществляет наряду с руководителями соответствующих структурных подразделений Служба делопроизводства.

Если исполнение документа поставлено на контроль, то при карточном способе учета используются дополнительные экземпляры регистрационно-учетных карточек, в которых для перенесения резолюции руководителя и контрольных отметок используются графы, отражающие движение документов в ходе их исполнения. При карточном учете для контроля за исполнением документов изготавливаются специальные контрольные карточки, содержащие следующие реквизиты:

- регистрационный номер документа и отметку конфиденциальности;
- дату документа;
- вид и заголовок документа;
- резолюцию;
- контрольные отметки;
- отметку о снятии документа с контроля.

В контрольных карточках не должны содержаться конфиденциальные сведения.

При контроле документов, которые имеют отдельные пункты и самостоятельного исполнителя, отвечающего за выполнение и за свой срок исполнения, на каждый из пунктов заполняется отдельный экземпляр карточки учета (контрольной карточки). Из карточек контролируемых документов формируется контрольная картотека по срокам исполнения документов. В пределах каждого срока карточки могут систематизироваться по видам регистрации документов, исполнителям, видам документов и др.

При автоматизированном контроле исполнения документов соответствующие данные вводятся в автоматизированную информационную систему контроля исполнения.

В процессе контроля исполнения документа Служба делопроизводства должна периодически (в установленные в организации сроки) напоминать исполнителю о контролируемом документе, о чем в графе «Контрольные отметки» контрольной карточки проставляется соответствующая дата. О нарушении срока исполнения доку-

мента Служба делопроизводства извещает соответствующего руководителя. После исполнения документа исполнитель проставляет на нем отметку об исполнении [209; 224].

На документах, зарегистрированных в картотеке учета документов инвентарного (выделенного) хранения, отметка «В дело» и индекс дела не проставляются (см. разд. 3.6).

Исполненный документ вместе с документом-ответом (при наличии) сдается в Службу делопроизводства. Ее сотрудник должен проверить наличие и правильность отметки об исполнении документа, соответствие вида и заголовка документа заголовку дела, в которое он направляется, просчитать количество листов документа и проверить соответствие их учетным данным, расписаться за получение документа в соответствующих графах регистрационных журналов (карточек). Контролируемый документ по решению соответствующего руководителя снимается с контроля, контрольная карточка (дубликат учетной карточки) или уничтожается, или помещается в справочную картотеку. Основная регистрационная карточка (при карточной регистрации) перекладывается в картотеку исполненных документов, в которой карточки располагаются в последовательности их номеров.

Если конфиденциальный документ не требует исполнения, а адресован лишь для ознакомления, то он может не выдаваться на рабочее место исполнителя, а ознакомление с ним осуществляется в Службе делопроизводства (комнате для исполнителей). При этом, если ознакомление производится в присутствии сотрудника, ответственного за учет и регистрацию документа, подпись в регистрационно-учетной форме за получение документа может не проставляться. Подписи об ознакомлении с документами с проставлением даты должны быть на самих документах, а подписи об ознакомлении с конфиденциальными распорядительными документами – на специальном листе ознакомления.

После исполнения поступившего документа или ознакомления с ним соответствующих должностных лиц приложения, не имеющие отметки конфиденциальности и не подлежащие совместному хранению с основным конфиденциальным документом, передаются в Службу делопроизводства. При этом заполняются графы 8–10 журнала учета и регистрации поступивших документов, делается отметка о передаче на основном документе или сопроводительном письме (см. разд. 3.1).

При работе с конфиденциальными документами руководители и исполнители обязаны:

• знакомиться только с теми конфиденциальными документами, к которым они получили разрешение на доступ в силу должностных обязанностей;

• предъявлять работнику Службы делопроизводства числящиеся за ними документы для проверки их наличия и комплектности;

• вести учет находящейся у них конфиденциальных документов;

• ежедневно по окончании рабочего дня проверять наличие документов и сдавать их на хранение в Службу делопроизводства;

• немедленно сообщать непосредственному руководителю и в Службу делопроизводства об утере или недодаче документов, обнаружении лишних или неучтенных документов, отдельных листов;

• сдавать по описи в Службу делопроизводства все числящиеся за ними документы при увольнении, уходе в отпуск, отъезде в командировку.

Руководители при рассмотрении конфиденциальных документов обязаны:

• принять правильное решение по составу исполнителей, допускаемых к документу;

• исключить возможность ознакомления с документом посторонних лиц;

• предотвратить возможность хищения или копирования документов посетителями и другими посторонними лицами;

• исключить возможность утечки информации по техническим каналам.

Посторонним лицом является любое лицо, не имеющее права доступа к данному конкретному конфиденциальному документу, в том числе другие руководители и сотрудники.

Сотрудник Службы делопроизводства, выдавая документы исполнителям для работы, обязан:

• предотвратить выдачу документов лицу, не имеющему права доступа к нему;

• зафиксировать факт передачи документа исполнителю;

• обеспечить физическую сохранность документа, приложений, листов и других частей документа;

• ознакомить исполнителя только с той частью документа, которая ему адресована;

• предотвратить возможность ознакомления с документом постороннего лица при выдаче документа исполнителю и его возврате;

• обеспечить учет документов, находящихся у исполнителей.

Ответственность за сохранность конфиденциальной информации и предотвращение утечки информации в структурных подразделениях организации несут их руководители и сотрудники. При работе с конфиденциальными документами руководители и исполнители должны быть обеспечены постоянным рабочим местом, личным сейфом (металлическим шкафом) и кейсом для хранения документов,

номерной личной металлической печатью. Ключи от сейфа и кейса, а также металлическая печать постоянно хранятся у руководителя или исполнителя. Дубликаты ключей должны находиться в Службе безопасности организации [224].

Все передачи конфиденциальных документов руководителям и исполнителям должны регистрироваться в передаточном журнале или карточках (в том числе электронных) учета документов. Прием и выдача документов должны визироваться подписью или отметкой в электронной карточке, что необходимо для установления факта возложения персональной ответственности за документ на конкретных работников.

При централизованной технологии делопроизводства хранение дел с конфиденциальными документами на рабочих местах руководителей и исполнителей запрещается. Отдельные дела с разрешения Службы делопроизводства могут находиться у исполнителя в течение срока, необходимого для выполнения задания, при условии полного обеспечения их сохранности и соблюдения правил хранения. Исполнение конфиденциальных документов сопровождается созданием других конфиденциальных документов. Особенности создания и изготовления конфиденциальных документов с помощью средств ЭВМ, печатания, копирования, тиражирования рассмотрены в разд. 2.6.

3.5. Учет и регистрация отправляемых (исходящих) конфиденциальных документов, их экспедиционная обработка и рассылка

3.5.1. Учет и регистрация отправляемых конфиденциальных документов

При отправлении документов в учетной и регистрационной форме 7, а также в других формах производятся соответствующие отметки, а именно:

- в журнале или карточке учета проектов внутренних (созданных/изданных) конфиденциальных документов в графах 12–14 (см. разд. 2.5);
- в журнале или карточке учета и распределения внутренних (созданных/изданных) конфиденциальных документов (см. ниже, форма 8);
- в журнале инвентарного (выделенного) учета в графах 8–10 (см. разд. 3.6).

Форма 7

№ п/п	Издано или поступило				Распределение			Возврат	Уничтожение
	Наименование документа	Откуда поступил, где отпечатан	Входящий номер сопроводительного письма и дата	Количество и номера экземпляров	Куда и кому отправлен или выдан	Номер исходящего документа или расписка в получении и дата	Количество и номера экземпляров	Дата, номера экземпляров	Дата, номер акта
1	2	3	4	5	6	7	8	9	10

Форма 8

Регистрационный номер и отметка конфиденциальности отправляемого документа	Дата отправления	Вид и заголовок документа	Адресат получателя отправляемого документа	Количество листов документа	Количество листов приложений	Индекс (номер) дела, номера листов дела	Номер по инвентарному (выделенному) учету	Примечание
1	2	3	4	5	6	7	8	9

При этом если документ отправлен без сопроводительного письма, то в графе «Наименование, номер и дата сопроводительного документа» пишется: «реестр», «расписка», «квитанция», а если с сопроводительным письмом – «сопроводительное письмо», с проставлением номеров и дат этих документов.

Если по каким-либо причинам отправлен документ (или часть его), зарегистрированный в журнале (карточке) учета проектов созданных документов, то в журнале проставляется отметка об отправлении (см. разд. 3.2.2). В ней указываются: количество отправленных листов, куда они отправлены, наименование, номер и дата сопроводительного документа, например: «3 листа отправлены в АОО «Межрегионсервис» по реестру № 7 от 21.01.2010 г.».

Тираж внутреннего (созданного/изданного) конфиденциального документа, полученного для рассылки, учитывается под одним номером в журнале или карточке учета и распределения созданных/изданных конфиденциальных документов.

Дополнительно размноженные экземпляры конфиденциального документа учитываются за регистрационным номером этого документа, о чем делается отметка на размножаемом документе и в журнале (карточке). Нумерация дополнительно размноженных экземпляров производится от последнего номера ранее учтенных экземпляров.

В размноженных документах в отметке о конфиденциальности проставляются номера экземпляров, а в учетной форме (журнал, карточка) отмечается количество экземпляров.

3.5.2. Экспедиционные технологии обработки и рассылки отправляемой конфиденциальной документированной информации

Конфиденциальные документы подлежат отправке в день их регистрации или на следующий рабочий день. В процессе экспедиционной обработки отправляемых конфиденциальных документов необходимо принять следующие меры по защите конфиденциальной информации и ее носителей:

- исключить возможность тайного вскрытия этих документов и несанкционированного ознакомления с ними в процессе их пересылки (передачи) адресату, подмены документов и листов;
- ограничить возможность утери, кражи или подмены пакета с конфиденциальными документами;
- подтвердить факт отправки конфиденциальной документированной информации и правильность оформления этого факта в учетных формах;
- исключить ошибочную отправку документов другому адресату, необоснованную рассылку ряду адресатов.

Разрешением на отправку конфиденциальной документированной информации является подписание руководством организации сопроводительного письма к ней или разрешительная отметка в учетном журнале отправляемых пакетов, если документы отправляются без сопроводительного письма по форме 9.

Технологии изготовления, копирования (размножения) и тиражирования рассмотрены в разд. 2.6. Рассылка размноженных и тиражированных конфиденциальных документов и изданий осуществляется на основании подписанного руководителем структурного подразделения списка адресов с указанием учетных номеров отправляемых экземпляров. Упаковка и отправка документов осуществляются сотрудником экспедиции, входящей в состав Службы делопроизводства. Отправка лично исполнителями не допускается.

Возможны два варианта упаковки конфиденциальных документов.

Первый вариант. Конфиденциальная документированная информация упаковывается в два пакета (двойное пакетирование). На внутреннем пакете проставляются: отметка конфиденциальности (в правом верхнем углу пакета), соответствующая наивысшей степени конфиденциальности документов, подлежащих вложению в пакет; фамилия лица, которому документ адресуется; номера вложенных документов, при необходимости ставится пометка «Лично». Внутренний пакет опечатывается бумажными наклейками, на которые ставится печать «Для пакетов» или Службы делопроизводства. Внешний пакет оформляется в соответствии с Почтовыми правилами, указанные сведения о конфиденциальности информации на него не выносятся. Пакеты с конфиденциальными документами пересылаются ценными отправлениями [42; 91].

Передача пакетов в почтовое отделение фиксируется в почтовом реестре, копия которого с почтовым штемпелем помещается в соответствующее дело. При передаче пакетов адресатам курьерами (нарочными) организации двойное упаковывание в конверты, как правило, не применяется.

Второй вариант. На одном светонепроницаемом пакете пишутся адрес и наименование организации-получателя (открытые или условные), под которыми перечисляются учетные номера конфиденциальных документов, вкладываемых в пакет. Если конфиденциальная документированная информация отправляется с сопроводительным письмом, то на пакете проставляется только номер сопроводительного письма без указания номеров приложений. При направлении документов в двух и более экземплярах на пакете рядом с номером документа в скобках указываются номера экземпляров. Ниже проставляются адрес и наименование организации-отправителя.

Форма 9

Дата отправления пакетов	Куда отправлены	Количество пакетов	Подпись лица, отправившего пакеты	Порядковые номера пакетов	Номера и грифы конфиденциальности вложенных в пакеты документов	Номера, присвоенные отправленным документам	Примечание
1	2	3	4	5	6	7	8

Пример. 1. *Получатель:* 117393, г. Москва, К-61. Организация п/я У-0901, № 543/ДСП, 456/ДСП
Отправитель: 420101, г. Казань, 101. Организация п/я М-7098

2. *Получатель:* 21403, г. Смоленск, 3. Завод «Алмаз», № 148 (пять экз.)
Отправитель: 173 007, г. Новгород, 6. КБ автоматики

На упаковке конфиденциальных документов и изданий не рекомендуется указывать фамилии и должности руководителей и сотрудников, а также наименования структурных подразделений.

Перед помещением документов в подготовленные пакеты проверяется соответствие данных на документах и пакетах, просчитывается количество листов и соответствие их учетным данным. При наличии сопроводительного письма проверяется, кроме того, соответствие названия, учетного номера, отметки конфиденциальности, номера экземпляра, количества листов приложения (с просчетом) записям в сопроводительном письме.

Для постоянных корреспондентов при большом объеме переписки целесообразно иметь пакеты с заранее воспроизведенными на них типографским способом адресами и наименованиями организаций-получателей и отправителя. Если в организации существует автоматизированная информационная система экспедиционной обработки, то возможен вариант автоматизированной распечатки адресов постоянных адресатов на пакетах, конвертах.

Все необходимые отметки делаются на одном светонепроницаемом пакете, который опечатывается. Передача документов курьером фиксируется в разносной книге или Реестре. Фиксация может производиться в электронном виде в автоматизированной информационной системе экспедиционной обработки.

Доставка документов через представителей других организаций производится на основании доверенности. Если организация передает пакеты через почтовые отправления, то перевозка и доставка могут выполняться силами и средствами специальной связи федерального органа исполнительной власти – фельдъегерской связью [42, ст. 22]. Пересылка пакетов фельдъегерской и специальной связью осуществляется на договорной основе.

При пересылке корреспонденции фельдъегерской или специальной связью составляется и распечатывается некоторое количество экземпляров реестра. Возможно составление его в электронном виде в автоматизированной информационной системе экспедиционной обработки. Последний экземпляр реестра остается в организации. Передача пакетов осуществляется в соответствии с Правилами служб фельдъегерской и специальной связи.

Если в конфиденциальной документированной информации имеются сведения, относящиеся к компетенции других организаций, передача их возможна только с согласия этих организаций.

Доставка конфиденциальных пакетов в другие организации, минуя органы связи, может осуществляться с разрешения руководителя организации-отправителя курьером экспедиционного подразделения Службы делопроизводства либо другим работником организации, допущенным к конфиденциальной информации, на служебном транспорте. Пакеты передаются по реестру или взамен разовой расписки, в которых, кроме подписи о получении пакетов, проставлена печать организации-получателя. Реестры и полученные расписки не должны иметь отметку конфиденциальности.

Пересылка конфиденциальной документированной информации по каналам сетей электросвязи и электронной почты в виде электронных сообщений в сети Интернет во многих случаях допускается, например для обеспечения информационного взаимодействия государственных структур, а также при оказании государственных услуг гражданам и организациям, связанных с обменом сведениями, содержащимися в базах данных информационных систем государственных структур, с использованием программно-аппаратных средств и телекоммуникационной инфраструктуры общероссийского государственного информационного центра. Использование ресурсов центра при информационном взаимодействии осуществляется в соответствии с требованиями к технологиям, форматам, протоколам информационного взаимодействия, унифицированным программно-техническим средствам и их применению, утверждаемыми Министерством информационных технологий и связи Российской Федерации [77; 89].

Под взаимодействием федеральных информационных систем электронного документооборота понимается обмен электронными сообщениями (ведение служебной переписки в электронной форме) между участниками межведомственного (межсетевого) электронного документооборота.

Одним из основных принципов межведомственного (межсетевого) электронного документооборота является обеспечение конфиденциальности передачи и получения информации. При осуществлении межведомственного (межсетевого) электронного документооборота допускается обмен электронными сообщениями, содержащими общедоступную информацию и информацию, отнесенную к сведениям, составляющим служебную тайну [74].

Аналогичные меры могут приниматься и в негосударственных организациях.

Более подробно система защищенного электронного документооборота и электронное взаимодействие системы ВЭД и МЭД рассмотрены в гл. 8.

Пересылка конфиденциальной информации по каналам сетей электросвязи и электронной почты в виде электронных сообщений в сети Интернет в сфере международного информационного обмена во многих случаях не допускается. Например, в соответствии с Указом Президента Российской Федерации «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» подключение информационных систем, информационно-телекоммуникационных сетей и средств вычислительной техники, применяемых для хранения, обработки или передачи информации, содержащей сведения, составляющие государственную тайну, либо информации, обладателями которой являются государственные органы и которая содержит сведения, составляющие служебную тайну, к информационно-телекоммуникационным сетям, позволяющим осуществлять передачу информации через государственную границу Российской Федерации, в том числе к международной компьютерной сети Интернет (далее – информационно-телекоммуникационные сети международного информационного обмена), не допускается.

Это положение должно быть оговорено в Инструкции по конфиденциальному делопроизводству и документообороту организации. В исключительных случаях разрешается внутри страны пересылать конфиденциальную информацию по указанным каналам связи при условии шифровки текста.

При использовании электрических (факсимильной или иной оперативной связи – телеграммы, телетайпные сообщения) и электронных каналов связи (электронная почта, сеть Интернет) организация должна руководствоваться законодательством в области связи и нормативными документами ФСБ России, ФСТЭК России, ФСО России, ряда других министерств и ведомств, а также действующими стандартами в области защиты информации (см. Список источников и литературы).

Федеральным законом «Об информации...» определено: «В целях заключения гражданско-правовых договоров или оформления иных правоотношений, в которых участвуют лица, обменивающиеся электронными сообщениями, обмен электронными сообщениями, каждое из которых подписано электронной цифровой подписью или иным аналогом собственноручной подписи отправителя тако-

го сообщения, в порядке, установленном федеральными законами, иными нормативными правовыми актами *или соглашением сторон*, рассматривается как обмен документами» [23, ст. 11, п. 4].

Не следует забывать, что согласно указанному закону (ст. 10, п. 3) при использовании для распространения информации средств, позволяющих определять получателей этой информации, в том числе почтовых отправлений и электронных сообщений, лицо, распространяющее информацию, обязано обеспечить ее получателю возможность отказа от нее.

3.6. Учет конфиденциальной документированной информации инвентарного (выделенного) хранения

На инвентарный (выделенный или списочный) учет берутся следующие конфиденциальные документы:

- не подлежащие подшивке в дела, например: сброшюрованные, документы большого формата, чертежно-графические, научно-технические, в том числе являющиеся приложениями к основным, фотографии, рисунки, электронные документы на соответствующих носителях (дискеты, флэш-памяти);
- изъятые по какой-либо причине из дела и переведенные на выделенное хранение (образовавшие самостоятельное дело), например документы, доступ к которым имеет более узкий круг лиц;
- технические носители информации (чистые или с записанной информацией), например дискеты, видео- и аудиокассеты, кассеты с фотопленкой и др.;
- бумажные носители информации для составления черновиков, оригиналов и подлинников документов, например рабочие тетради, отдельные листы бумаги, тетради с отрывными листами и др.;
- журналы (картотеки) учета документов, картотеки учета выдачи дел и документов, законченные дела [209].

Инвентарный учет осуществляется в журнале или карточках, в том числе в электронных автоматизированной информационной системы (если такая система функционирует в организации).

Журнал (картотека) инвентарного учета ведется непрерывно по форме 10, номера каждого года продолжают номера предыдущих лет. Вызвано это тем, что выделенному хранению подлежат, как правило, документы постоянного и долговременного хранения, и их ежегодная перерегистрация привела бы к увеличению трудоемкости обработки конфиденциальной документированной информации и созданию сложностей для пользователей.

Форма 10

Учетный номер и отметка конфиденциальности документа	Дата регистрации	Вид и заголовок	Откуда поступил документ или каким подразделением разработан	С каких учетных номеров переведена
1	2	3	4	5

Продолжение

Номера экземпляров	Количество листов в экземпляре	Отправление		
		Куда отправлена	Номера экземпляров	Наименование, номер и дата сопроводительного документа
6	7	8	9	10

Окончание

Отметка о возврате	Уничтожение		Передача на архивное хранение	
	Номера экземпляров	Номер и дата акта об уничтожении	Номер экземпляра	Архивный шифр
11	12	13	14	15

На инвентарный учет может браться вся конфиденциальная документированная информация, если ее объем невелик. Инвентарный номер указывается на документе в верхнем левом углу первого листа, например: «Инв. № __ и дата». Одновременно может формироваться электронный справочный массив по документам.

Поставленные на инвентарный учет технические носители информации маркируются. Маркировка предусматривает нанесение на них следующих данных: инвентарного номера, индекса или названия структурного подразделения, фамилии исполнителя. Надписи делаются красящим веществом, имеющим хорошую механическую стойкость. Этим же веществом окрашиваются винты или иные детали, скрепляющие корпус кассеты, дискеты или футляр с целью сигнализации об их несанкционированном вскрытии.

Если в организации производится копирование (тиражирование) конфиденциальных документов инвентарного учета, то между графами 7 и 8 помещаются графы о номере и дате разрешения на размножение, количестве и номерах размноженных экземпляров.

При значительном объеме конфиденциальных документов инвентарного хранения чертежно-графические и текстовые документы могут учитываться раздельно, но по однотипной форме. В этом случае вместо добавляемого к номеру документа индекса И (инвентарный учет) или В (выделенный учет) на чертежно-графических документах проставляется индекс Ч, на текстовых – Т. В момент регистрации заполняются графы 1–7.

При поступлении конфиденциальной документированной информации, созданной другой организацией и подлежащей инвентарному учету, ей сразу (без оформления в журнале учета и регистрации поступивших конфиденциальных документов) присваивается очередной порядковый номер по журналу (карточке) инвентарного учета. Этот номер проставляется на документе, в графе 8 журнала учета поступивших пакетов и в графе 1 журнала (карточки) инвентарного учета с одновременным заполнением граф 2–7 этого журнала. При этом в графе 5 указывается: «п/ж № __ за __» (где «п/ж» – журнал учета пакетов), с проставлением номера и даты поступления пакета, в котором находился конфиденциальный документ.

При учете чертежно-графических документов в графе 3 проставляется вид носителя (калька, ватман), а для текстовых также вид носителя (электронный, бумажный) и индекс (обозначение) документа.

При взятии на учет конфиденциальной документированной информации, переводимой с регистрации поступивших конфиденциальных документов, в графе 4 указывается, откуда поступил документ, в графе 5 – его номер по журналу учета и регистрации поступивших документов, в графе 13 проставляются номер, присвоенный конфиденциальной документированной информации по журналу инвентарного учета, и количество листов.

При взятии на учет конфиденциальных документов, переводимых с учета внутренних (созданных/изданных) документов, в графе 4 указывается подразделение организации, разработавшее конфиденциальный документ, в графе 5 –номер по журналу учета внутренних (созданных/изданных) конфиденциальных документов, в графе 17 проставляются номер, присвоенный документу по журналу учета инвентарного хранения, и количество переведенных на инвентарное хранение экземпляров (см. разд. 3.3).

При взятии на учет носителя, переводимого с учета бумажных носителей (см. разд. 3.2.1), в графе 4 указывается подразделение организации, в графе 5 – номер носителя по журналу учета носителей, в графе 9 – проставляется номер, присвоенный носителю по журналу учета инвентарного хранения.

При взятии на учет инвентарного хранения носителя без регистрации его в журнале учета бумажных носителей (рабочая тетрадь, калька и др.) в графе 5 делается прочерк.

Взятая на инвентарный учет текстовая документированная информация брошюруется (прошивается) и помещается в обложку (если ее не было). При этом после последнего листа документа помещается лист с заверительной надписью, в которой прописью указывается количество листов в документе. Надпись заверяется подписью (с расшифровкой) составившего ее лица и проставлением даты. Если в документе имеются вклеенные на листы фотоотпечатки, то они оговариваются в заверительной надписи.

Индексы и номера, присвоенные по журналу (карточке) инвентарного учета, проставляются на текстовых документах в верхнем левом углу обложки и титульного листа (при его наличии). В правом верхнем углу проставляется гриф конфиденциальности и под ним номер экземпляра. На чертежно-графических документах индекс и номер проставляются на каждом листе в местах, отведенных соответствующими стандартами. На присланных документах имеющиеся там номера зачеркиваются тушью тонкими линиями [209].

На каждый конфиденциальный документ заводится карточка учета выдачи по форме 11.

Форма 11

КАРТОЧКА
выдачи конфиденциального документа инвентарного учета

_____
(учетный номер и наименование документа)

Количество листов	Кому выдан	Подпись за получение и дата	Подпись за возврат и дата
1	2	3	4

3.7. Учет конфиденциальной информации при ее автоматизированной обработке

3.7.1. Особенности автоматизированного учета и регистрации конфиденциальной информации. Реестр конфиденциальной информации автоматизированной информационной системы

Учет конфиденциальной информации при ее автоматизированной обработке производится с помощью Реестра конфиденциальной информации автоматизированной информационной системы (далее – Реестр).

Реестр разрабатывается в целях обеспечения учета конфиденциальной информации при ее автоматизированной обработке в АИС организации. Как документ он предназначен для использования организацией, выполняющей функции оператора эксплуатации, технической поддержки и защиты конфиденциальной информации, циркулирующей в АИС .

Положение о Реестре разрабатывается в соответствии с нормативно-правовыми документами, нормативно-технической документацией в области информационной безопасности и защиты информации в целях обеспечения учета не только конфиденциальной информации, но и всех информационных ресурсов АИС организации для решения следующих задач:

- организации контроля за выполнением требований по защите информации от утечки, уничтожения, блокирования или модификации;
- обеспечения анализа защищенного информационного обмена в единой информационной среде организации.

Реестр должен содержать: учетные записи, соответствующие объектам учета, и дела объектов учета.

Конфиденциальная информация, циркулирующая в АИС, в целях ее защиты подлежит обязательному учету на всех этапах ее жизненного цикла: предпроектной стадии, стадии проектирования и создания, ввода в действие и стадии эксплуатации.

Сбор, хранение и обработка информации Реестра осуществляются оператором с использованием разрабатываемой или разработанной АИС «Реестр информационных ресурсов» [326].

3.7.2. Объекты учета Реестра

Учет данных конфиденциального характера, содержащихся в АИС и информационных ресурсах, организуется и ведется на уровне:

- организации, имеющей доступ к информации объекта защиты, – подразделением информационной безопасности (если оно существует), обеспечивающей защиту информации;
- единой информационной среды организации – оператором Реестра, который входит в состав Службы информационных технологий организации, при непосредственном участии Службы безопасности (информационной безопасности) и Службы делопроизводства организации.

Учету подлежат машинные носители информации, средства вычислительной техники, средства защиты информации, средства передачи данных и каналы связи (объекты учета), в которых хранится, обрабатывается и циркулирует конфиденциальная информация. Данные организации учитываются по каждому структурному подразделению.

Машинные носители с конфиденциальной информацией учитываются в соответствии с целевым назначением, мобильностью и типом носителя: хранения, записи и считывания данных (жесткий магнитный диск, оптический диск, карта флэш-памяти и др.).

Должны учитываться как машинные носители, съемные и несъемные, так и отчуждаемые машинные носители, используемые для записи, считывания данных конфиденциального характера на средствах АИС.

Локальная вычислительная сеть (ЛВС) – это вычислительная сеть, поддерживающая в пределах ограниченной территории один или несколько высокоскоростных каналов передачи цифровой информации, предоставляемых подключаемым устройствам для кратковременного монопольного использования [191].

Каналы связи (передачи данных) являются также носителями информации конфиденциального характера и учитываются на уровне ЛВС и магистралей (трактов) сетей передачи данных, обеспечивающих связь как между внутренними (между зданиями, уровнями межсетевой иерархии АИС и др.), так и с внешними относительно организации – обладателя АИС и конфиденциальной информации ЛВС.

Обособленные устройства, обеспечивающие обмен конфиденциальной информацией по магистральным каналам передачи данных, рассматриваются как частный случай ЛВС при оценке объекта учета.

Все виды объектов учета идентифицируются по наименованию АИС и информационных ресурсов в соответствии с проектной и эксплуатационной документацией. До принятия АИС в эксплуатацию конфиденциальные данные технического характера типа паролей, применяемых для идентификации и аутентификации пользователей в АИС, в отчетных формах по объектам учета организации в отчетных формах не фиксируются.

Учет машинных носителей, содержащих конфиденциальную информацию, а также документов (на бумажном носителе) конфиденциального характера, исполняемых с помощью средств вычислительной техники, производится в установленном в организации порядке, определенном для обращения документов ограниченного доступа и распространения, за исключением документированной информации, составляющей государственную тайну.

Наличие в АИС конфиденциальной информации определяется ответственным исполнителем организации – Службой безопасности при участии Службы делопроизводства на основании Перечня конфиденциальной документированной информации организации (см. разд. 2.3, а также приложение 2).

В организации выделяются следующие потоки конфиденциальной информации, циркулирующие в АИС:

- потоки, циркулирующие внутри организации;
- поступающие (входящие) потоки, собственником которых организация не является, – они получены ею от внешних источников – сторонних организаций и предприятий;
- отправляемые (исходящие) потоки, переданные в установленном порядке иным (сторонним) организациям.

На основании информации по объектам учета структурных подразделений организации и потоков конфиденциальной информации формируются данные обобщенного объекта учета организации.

Дополнительные формы объектов учета – систем связи и магистральных каналов связи, используемых для доставки входящих и исходящих потоков информации АИС, содержащих сведения конфиденциального характера, – определяются оператором Реестра в порядке, установленном организацией по взаимодействию с операторами связи, оказывающими телекоммуникационные услуги организации – владельцу АИС и конфиденциальной информации.

3.7.3. Технологии ведения Реестра

Как говорилось ранее, ведение Реестра направлено на обеспечение защиты конфиденциальной информации организации с помощью технологий учета и контроля обращения данных конфиденциального характера, содержащихся в АИС и ее информационных ресурсах.

Все структурные подразделения организации – пользователи АИС и ее информационных ресурсов обязаны учесть и обеспечить предоставление данных объекта учета структурного подразделения оператору Реестра, ведущему обобщенный объект учета организации.

Актуальной информационной базой является база, которая существует в указанный момент или период времени, квалифицируемый как «сейчас», и отражает дополнительные высказывания, отличные от необходимых [167].

Технологии ведения Реестра в части учета и сопровождения объектов учета включают в себя следующие этапы:

- первичный учет;
- внесение изменений в учетные данные при внедрении проектируемой АИС в промышленную эксплуатацию, а также изменение прав собственности на АИС и информационные ресурсы;
- внесение изменений в учетные данные в процессе опытной или промышленной эксплуатации АИС;
- аннулирование объекта учета в связи с прекращением эксплуатации, а также последующей ликвидацией АИС и информационных массивов и др.

Структурные подразделения организации, имеющие только открытую информацию, должны предоставлять информацию в части средств защиты информации.

Внесение первичных данных об объектах учета в Реестр, изменений этих данных или аннулирование осуществляются оператором Реестра на основе заявления структурного подразделения по приведенной ниже форме.

Заявление
о внесении в Реестр конфиденциальной информации

1. _____
(полное наименование структурного подразделения организации-заявителя)
в лице_____
(должность, Ф.И.О. руководителя структурного подразделения)
просит (нужное подчеркнуть):
1) внести в Реестр новый объект учета;
2) внести изменения в Реестр в связи с перерегистрацией объекта учета;
3) исключить объект учета из Реестра

в соответствии с прилагаемыми данными.

2. С порядком регистрации АИС и информационных массивов
_____ _____,
(наименование организации)
содержащих данные конфиденциального характера, ознакомлены.

3. Для обеспечения взаимодействия в процессе рассмотрения документов и внесения в Реестр нами уполномочен
_____
(Ф.И.О., должность уполномоченного лица, тел., факс, E-mail)

4. Наши реквизиты:

Почтовый адрес:_____

Телефон_____факс_____

Адрес Интернет-сайта_____Адрес ЭП_____

5. Перечень прилагаемых документов:_____

6. Достоверность сведений, содержащихся в прилагаемых документах, подтверждаю:
_____
(подпись руководителя структурного подразделения, дата) (Ф.И.О. руководителя)

К заявлению прилагаются следующие документы:

- данные об объекте учета по утвержденной форме;
- копия акта работ или иного документа, определяющего факт регистрации, перерегистрации или аннулирования объекта учета;
- копия аттестата соответствия по результатам аттестационного контроля АИС и информационного массива.

Аттестацией соответствия является подтверждение экспертизой и предоставлением объективных доказательств того, что конкретные требования к определенным объектам полностью реализованы. Термин «аттестован» используется для обозначения соответствующих состояний объекта. Возможно проведение ряда аттестаций, если они преследуют различные цели. Более подробно об организации проведения аттестации АИС по требованиям безопасности информации говорится в разд. 8.7.

При представлении заявления об аннулировании учета к заявлению прилагается копия распорядительного документа о прекращении разработки (эксплуатации) системы. Заявитель (структурное подразделение организации) обязан представить документы по процедуре учета объекта не позднее 30 дней после наступления одного из следующих событий:

- подписания договора на проектирование (создание) АИС;
- утверждения акта приемки АИС в промышленную эксплуатацию;
- принятия решения о прекращении создания или эксплуатации, утверждения иных распорядительных документов организации, изданных по фактам наступления событий по учету объекта.

При изменениях в объекте учета в ходе эксплуатации АИС структурное подразделение в течение 3 рабочих дней после наступления событий, обусловленных качественными изменениями видов и потоков конфиденциальной информации, качественным и количественным изменениям состояния АИС и информационных ресурсов (например, окончания работ по модернизации системы, завершения изменений состава рабочих мест подразделения, начала владения конфиденциальной информацией сторонней организации и др.), представляет в Службу безопасности (информационной безопасности) обновленные данные по утвержденной организацией форме структурного подразделения с указанием причин внесения изменений.

На основании обновленных данных по объектам учета, обобщенных Службой безопасности, оператору Реестра представляется заявка на внесение изменений по приведенной ниже форме.

Заявка на внесение изменений в Реестр представляется заявителем в течение 10 рабочих дней после регистрации подразделением Службы безопасности (информационной безопасности) изменений по объектам учета структурных подразделений. К заявке прилагаются:

- копия распорядительного документа, определяющего факт изменения объекта учета;
- копии измененных документов.

Заявка
на внесение изменений в Реестр

1. _____
(полное наименование структурного подразделения – заявителя)
в лице_____
(должность, Ф.И.О. руководителя)
просит внести изменения в Реестр в соответствии с прилагаемыми документами.

2. Перечень прилагаемых документов:_____

3. Достоверность сведений, содержащихся в прилагаемых документах, подтверждаю:

_____
(подпись руководителя, дата) Ф.И.О. руководителя

При отсутствии в течение календарного года изменений в обобщенном объекте учета заявитель направляет оператору Реестра, следующего за отчетным, информационное сообщение, в котором говорится о том, что в обобщенный объект учета изменения не вносились.

В процессе регистрации он проверяет правильность оформления и достоверность поданных документов и имеет право потребовать дополнительные материалы, подтверждающие достоверность представленных документов, а заявитель обязан предоставить указанные документы. По истечении установленного срока рассмотрения заявитель уведомляется о включении или невозможности включения объектов учета в Реестр. В случае отказа о включении объекта в Реестр заявителю направляется соответствующее уведомление с указанием основания для отказа. Отказ допускается в случаях:

- несоответствия представленных документов требованиям, установленным Положением о ведении Реестра, разрабатываемым организацией;
- недостоверности предоставляемой информации.

Оператор Реестра выполняет процедуры исключения объекта учета из Реестра путем аннулирования соответствующей учетной записи и организации архивного хранения реестрового дела по инициативе либо заявителя, либо руководства организации в случае прекращения разработки или эксплуатации АИС и информационных массивов.

Реестровое дело исключенного объекта учета находится на оперативном хранении у оператора Реестра в течение 5 лет.

ГЛАВА 4

РАЗРЕШИТЕЛЬНАЯ СИСТЕМА ДОСТУПА К КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

4.1. Основные требования к разрешительной системе доступа

4.1.1. Общие сведения

Ключевым звеном в защите конфиденциальной информации, в том числе информации, циркулирующей в АИС, или, иначе, системах конфиденциального электронного документооборота, является организация санкционированного (разрешенного) доступа к ней.

Разрешительная система допуска и доступа к конфиденциальной информации основана на выполнении установленных руководством организации нормативных положений, обеспечивающих обоснованный и правомерный доступ пользователей к необходимому им для выполнения служебных обязанностей объему конфиденциальной информации. При этом под *допуском к конфиденциальной информации* понимается процедура оформления права граждан на доступ к такой информации, а для организаций, предприятий, учреждений – права на проведение работ с использованием такой информации. *Доступ* к информации – это возможность ее получения и использования [23, ст. 2]. Под *доступом к конфиденциальной информации* понимается санкционированное полномочным должностным лицом ознакомление с данной информацией, ее получение и использование конкретным физическим или юридическим лицом.

При этом право давать разрешение на ознакомление и право работать может быть предоставлено только лицам, имеющим доступ к конфиденциальной информации.

При установлении разрешительной системы доступа к конфиденциальной информации должны быть обеспечены такие требования, как:

• надежность – исключение возможности несанкционированного доступа (НСД) посторонних лиц к КДИ и конфиденциальной информации, циркулирующей в АИС, в обычных и экстремальных условиях (под экстремальными условиями понимаются чрезвычайные ситуации, пожары, наводнения и др.);

• полнота охвата всех категорий исполнителей и всех категорий конфиденциальной информации;

• конкретность и однозначность решения о доступе (да/нет);

• производственная и служебная необходимость – единственный критерий доступа к конфиденциальной информации;

• определенность состава должностных лиц, дающих санкцию на доступ к конфиденциальной информации, исключение возможности бесконтрольной и несанкционированной выдачи таких санкций;

• регламентация и организация работы всех категорий персонала с конфиденциальной информацией;

• соответствие функциональных обязанностей работника передаваемой ему конфиденциальной документированной информации;

• наличие нормативно-методических документов и положений по защите и охране конфиденциальной информации, режиму конфиденциальности информации и доступа к ней (см. разд. 4.1.2), в том числе утвержденного Перечня конфиденциальной документированной информации (см. разд. 2.3), Реестра конфиденциальной информации и АИС (см. разд. 3.7);

• наличие необходимых условий в зданиях, помещениях, кабинетах для работы с конфиденциальной документированной информацией;

• оформление разрешения на ознакомление с конфиденциальной информацией;

• ознакомление пользователя, при необходимости, только с частью конфиденциального документа, при этом в разрешении на ознакомление должны быть указаны разделы, пункты или страницы, с которыми можно знакомить пользователя, если конфиденциальная документированная информация находится на бумажном носителе.

Разрешительная система должна предусматривать порядок доступа к конфиденциальной информации граждан, других должностных лиц и организаций, например при выполнении совместных работ и услуг (более подробно см. разд. 4.2–4.7).

Следует иметь в виду, что сотрудники уполномоченных органов государственной власти и органов местного самоуправления (далее – уполномоченные органы), например налоговая служба, служба

судебных приставов, органы МВД и др., имеют право на доступ к различным видам конфиденциальной информации в пределах компетенции, определенной для этих органов законодательством Российской Федерации. Поэтому организации, обладающие конфиденциальной информацией, обязаны не только знакомить должностных лиц уполномоченных органов с конфиденциальной документированной информацией, но и предоставлять им в распоряжение конфиденциальные документы в случаях, установленных законодательством Российской Федерации.

Уполномоченные органы обязаны обеспечить защиту полученной информации от разглашения и неправомерного использования должностными лицами и иными служащими этих органов, которые ознакомились с конфиденциальной информацией в связи с выполнением служебных обязанностей. Это положение относится к служебной, налоговой и коммерческой, банковской тайнам (см. гл. 1). За разглашение или неправомерное использование содержащейся в документах конфиденциальной информации данные органы несут перед обладателем этой информации правовую ответственность (см. приложение 6).

4.1.2. Регламент доступа к конфиденциальной информации

Разрешительная система доступа не только обеспечивает доступ к конфиденциальным документам, но и определяет порядок доступа к другим носителям конфиденциальной информации, например к циркулирующей в АИС. Эти функции системы должны находить свое отражение в Регламенте доступа к конфиденциальной информации (далее – Регламент) или Положении о режиме конфиденциальности информации.

Регламент разрабатывается Экспертной комиссией по защите конфиденциальной информации (см. разд. 4.1.3) и содержит следующие разделы:

1. ***Общие положения***. В этом разделе указываются:

- цель разработки Регламента;
- основные задачи и принципы системы допуска и доступа;
- нормативные документы, на которых базируется Регламент организации, а также лица, на которых возлагается ответственность за невыполнение его требований;
- руководство организации, руководители Службы безопасности, Службы делопроизводства, структурных подразделений, осуществляющих контроль за соблюдением норм Регламента в пределах их компетенции.

При этом указывается, что ответственность за невыполнение требований Регламента несут все должностные лица, имеющие право давать разрешение на доступ, а также все пользователи конфиденциальной информацией.

2. ***Круг лиц, имеющих право давать разрешение на допуск и доступ к конфиденциальной информации.*** В данном разделе должны быть перечислены все должности лиц, которые могут давать разрешение на доступ к конфиденциальной информации, с указанием категории пользователей, состава информации и ее носителей. Право давать разрешение на доступ к соответствующей конфиденциальной информации имеют:

- руководитель организации – всем категориям пользователей;
- заместители руководителя по отдельным направлениям – всем пользователям, но в пределах своей сферы деятельности;
- руководители структурных подразделений – всем сотрудникам подразделений.

Для возможности доступа к конфиденциальной информации какого-либо подразделения сотрудников и работников других подразделений необходимо разрешение соответствующего заместителя руководителя организации. Первые заместители руководителей, а также должностные лица, временно исполняющие ту или иную должность, могут, как правило, разрешать доступ в объеме всех прав, предусмотренных для замещаемого ими лица.

3. ***Порядок оформления разрешений на доступ к конфиденциальной информации и предоставление ее пользователям.*** В данном разделе определяется порядок оформления разрешений на доступ к различным носителям конфиденциальной информации и выдачи носителей пользователям (см. разд. 4.7). Разрешение на ознакомление должно оформляться: по поступившим и созданным/изданным документам – в форме резолюции на конфиденциальном документе; по документам, зарегистрированным по учету инвентарного (выделенного) хранения (см. разд. 3.6), – в форме резолюции на документе или подписанного соответствующими руководителями списка пользователей на внутренней стороне обложки документа, титульном листе либо в карточке учета выдачи конфиденциального документа. При этом следует оговорить, что исполнители и лица, которые визировали, согласовывали, подписывали и утверждали конфиденциальные документы, допускаются к соответствующей конфиденциальной информации, в том числе циркулирующей в АИС, без оформления дополнительных разрешений, если они продолжают выполнять те же функциональные обязанности. Без специального разрешения могут допускаться также лица, указанные в тексте распорядительных документов организации (приказов, распоряжений).

4. ***Порядок учета работников и должностных лиц организации, а также работников должностных лиц других организаций, получивших доступ к конфиденциальной информации*** (см. разд.4.7).

5. ***Порядок учета выдачи конфиденциальной документированной информации***.

Регламент подписывается членами Экспертной комиссии по защите конфиденциальной информации, визируется всеми лицами, имеющими право давать разрешение на доступ, и вводится в действие приказом руководителя организации. В приказе определяются также и мероприятия по введению Регламента в действие (порядок изучения Регламента пользователями, технология осуществления контроля за его выполнением и др.). После утверждения с Регламентом должны быть ознакомлены под расписку все сотрудники и работники организации, работающие с конфиденциальной информацией.

Технологии допуска и доступа к конфиденциальной документированной информации являются основой при постановке задач и разработке технических заданий для создания соответствующей АИС допуска и доступа к конфиденциальной информации, которая является одним из главных модулей интегрированной системы электронного конфиденциального документооборота.

4.1.3. Экспертная комиссия по защите конфиденциальной информации*

Экспертная комиссия по защите конфиденциальной информации – коллегиальный орган, который занимает ключевое положение в системе структурных подразделений организации, отвечающих за допуск и доступ к КДИ, ее защиту и охрану.

В Экспертную комиссию по защите конфиденциальной информации входят следующие подразделения: Служба безопасности, Служба делопроизводства, Служба кадров и подразделение информационных технологий и АИС (информационно-технологический центр, главный вычислительный центр и др.).

Основными функциями Экспертной комиссии являются:

• координация деятельности указанных структурных подразделений, обеспечивающих в интересах разработки и выполнения программ и планов, нормативных и методических документов, в том числе Регламента по защите конфиденциальной информации,

* Данный раздел составлен по материалам Межведомственной комиссии по защите государственной тайны.

Реестра конфиденциальной информации и АИС (см. разд. 3.7, 4.1.2) реализацию нормативно-правовых документов и системы стандартов Российской Федерации в области защиты информации;

• организация разрешительной системы доступа.

Экспертная комиссия создается в соответствии с приказом руководителя организации. Функции комиссии и ее полномочия реализуются в соответствии с Положением, утверждаемым руководителем организации. В состав комиссии должны входить руководители организации, курирующие вопросы защиты конфиденциальной информации, руководители перечисленных выше структурных подразделений организации или их заместители. Состав данной комиссии по должностям, а также персональный состав утверждаются руководителем организации.

Решения Экспертной комиссии, принятые в соответствии с ее полномочиями, обязательны для исполнения всеми структурными подразделениями организации, всем персоналом организации, включая руководство, а также другими организациями и предприятиями при выполнении совместных работ, связанных с доступом к конфиденциальной информации и ее защитой.

Основными функциями Экспертной комиссия являются:

• организация работы по формированию Перечня (номенклатуры) должностных лиц, имеющих полномочия в отношении отнесения информации к конфиденциальной. Перечень утверждается приказом организации;

• организация работы по формированию и созданию Перечня конфиденциальной документированной информации организации (см. разд. 2.3);

• организация работы по формированию и созданию Реестра конфиденциальной информации и автоматизированной информационной системы (см. разд. 3.7);

• подготовка предложений по организации разработки и выполнению программ, планов, нормативных и методических документов, обеспечивающих реализацию доступа к конфиденциальной информации, ее защиту и охрану, и представление их в установленном порядке руководству организации;

• рассмотрение и представление руководству организации предложений по нормативному регулированию вопросов режима конфиденциальности информации, доступа к ней и совершенствованию системы защиты и охраны конфиденциальной информации в организации;

• определение порядка снятия грифа ограничения доступа (отметки конфиденциальности) в случае ликвидации организации – фондообразователя и отсутствия ее правопреемника;

• рассмотрение запросов государственных и негосударственных структур (предприятий, учреждений, организаций), юридических лиц и граждан о снятии грифа ограничения доступа;

• подготовка экспертных заключений на КДИ в целях решения вопроса о возможности ее передачи и предоставления другим организациям и уполномоченным органам;

• принятие решения о передаче КДИ другой организации в случаях изменения функций, форм собственности, ликвидации или прекращения работ с использованием этой информации;

• подготовка и предоставление руководству организации предложений по порядку определения размеров ущерба, который может быть нанесен организации вследствие несанкционированного распространения и доступа к конфиденциальной информации, а также ущерба, наносимого организации в связи с приданием конфиденциальности информации, находящейся в ее собственности;

• подготовка и предоставление руководству организации предложений по отнесению информации к конфиденциальной, к различным степеням конфиденциальности (см. разд. 2.2);

• рассмотрение по поручению руководства организации проектов договоров (государственных контрактов), в том числе международных, о совместном использовании конфиденциальной информации, доступе к ней и о ее защите; подготовка соответствующих предложений и экспертных заключений; участие в международном сотрудничестве по этим вопросам;

• выдача заключений на решения руководителей структурных подразделений, связанные с изменением действующих в подразделениях перечней конфиденциальной документированной информации (эти заключения могут привести к изменению Перечня конфиденциальной документированной информации, Реестра конфиденциальной информации и АИС организации);

• выдача заключений на защиту разрабатываемых и разработанных всевозможных АИС, включая интегрированные системы защищенного электронного документооборота организации;

• координация работ по организации сертификации технических средств защиты конфиденциальной информации, лицензированию деятельности организации, связанной с использованием конфиденциальной информации, созданию технических средств защиты информации, а также осуществление мероприятий и (или) оказание услуг по защите конфиденциальной информации, если организация оказывает такие услуги другим организациям;

• решение вопросов о продлении срока конфиденциальности документов и информации.

Экспертная комиссия имеет следующую структуру: председатель комиссии, его заместители, члены комиссии, ответственный секретарь комиссии, служба делопроизводства (организационно-техническое обеспечение деятельности комиссии), рабочие и экспертные группы по направлениям деятельности (по мере надобности).

4.2. Особенности доступа к конфиденциальной документированной информации, составляющей служебную, коммерческую, профессиональную тайны, секрет производства (ноу-хау) и служебный секрет производства

Федеральный закон «О коммерческой тайне» содержит определение: «Доступ к информации, составляющей коммерческую тайну, – это ознакомление определенных лиц с информацией, составляющей коммерческую тайну, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации» [29, ст. 3, п. 5]. Можно сказать, что обладатель конфиденциальной информации, составляющей коммерческую или служебную тайну, – это лицо, которое владеет конфиденциальной информацией на законном основании, ограничивает доступ к этой информации и устанавливает в отношении нее режим коммерческой или служебной тайны.

Конфиденциальная информация, составляющая коммерческую, служебную, профессиональную тайны, секрет производства (ноу-хау) и служебный секрет производства, обладателем которой является другое лицо, считается полученной незаконно, если доступ к ней осуществлялся с умышленным преодолением принятых обладателем данной информации мер по охране ее конфиденциальности, в том числе по ограничению доступа к ней.

Существуют три вида договоров, регулирующих ограничение доступа к секрету производства и служебному секрету производства: 1) договор об отчуждении исключительного права на секрет производства; 2) лицензионный договор о предоставлении права использования секрета производства; 3) секрет производства, полученный при выполнении работ по договору подряда. Подробно эти договоры рассматривались в разд. 1.1.7.

Передача конфиденциальной информации – это передача обладателем информации, зафиксированной на материальном носителе, контрагенту на основании договора в объеме и на условиях, предусмотренных договором, включая условие о принятии контрагентом установленных договором мер по охране ее конфиденци-

альности. Контрагент – сторона гражданско-правового договора, которой обладатель конфиденциальной информации передал эту информацию.

В договорах должны быть определены условия защиты и охраны конфиденциальности информации и доступа к ней, в том числе в случае реорганизации или ликвидации одной из сторон договора в соответствии с гражданским законодательством, а также обязанность контрагента по возмещению убытков при разглашении им этой информации вопреки договорам, в соответствии со следующим типовым текстом пункта договора.

Пункт договора (государственного контракта) о неразглашении информации

Контрагент (лицензиат) обязан:

1) не разглашать конфиденциальную информацию Организации, которая будет доверена или станет известной по условиям договора;

2) не передавать третьим лицам и не раскрывать публично конфиденциальную информацию Организации без ее согласия;

3) выполнять по договору требования инструкций и положений по обеспечению сохранности конфиденциальной информации Организации и доступу к ней;

5) сохранять конфиденциальную информацию тех организаций, с которыми у Организации имеются служебные и деловые отношения;

6) не использовать знание конфиденциальной информации Организации для занятий любой деятельностью, которая может нанести ей ущерб;

7) в случае расторжения договора все носители конфиденциальной информации Организации (рукописи, черновики, чертежи, магнитные ленты, диски, дискеты, распечатки на принтерах, кино-, фотонегативы и позитивы, модели, материалы, изделия и др.), которые находились в распоряжении в связи с выполнением договорных обязанностей, передать Организации;

8) незамедлительно сообщить Организации о допущенном контрагентом либо ставшем ему известным факте разглашения или угрозы разглашения, незаконном получении или незаконном использовании конфиденциальной информации третьими лицами, об утрате или недостаче носителей конфиденциальной информации и о других фактах, которые могут привести к разглашению конфиденциальной информации Организации, а также о причинах и условиях возможной утечки информации.

Нарушение указанных положений Договора может повлечь уголовную, административную, гражданско-правовую или иную ответственность, предусмотренную ст. 13.11, 13.14 КоАП РФ, ст. 183 УК РФ, иными нормативными правовыми актами Российской Федерации, в виде лишения свободы, возмещения ущерба Организации (убытков, упущенной выгоды и морального ущерба) и других наказаний.

Организация подтверждает, что данные обязательства не ограничивают прав контрагента на интеллектуальную собственность, полученную в результате работ по договору.

В случае, если иное не установлено договорами, контрагент в соответствии с законодательством Российской Федерации самостоятельно определяет способы защиты информации, переданной ему по указанным договорам, и доступ к ней в соответствии с нормативными правовыми актами.

Контрагент обязан незамедлительно сообщить обладателю конфиденциальной информации о допущенном контрагентом либо ставшем ему известным факте разглашения или угрозы разглашения, незаконном получении или незаконном использовании конфиденциальной информации третьими лицами.

Обладатель конфиденциальной информации, переданной им контрагенту, до окончания срока действия договора не может разглашать эту информацию, а также в одностороннем порядке прекращать охрану ее конфиденциальности и доступа к ней, если иное не установлено договорами.

Гражданин, которому в связи с выполнением своих трудовых обязанностей или конкретного задания работодателя стал известен секрет производства, обязан сохранять конфиденциальность полученных сведений до прекращения действия исключительного права на секрет производства.

Исключительное право на секрет производства, созданный работником в связи с выполнением своих трудовых обязанностей или конкретного задания работодателя, – это служебный секрет производства, который принадлежит работодателю (ст. 1470 ГК РФ).

В целях охраны конфиденциальности информации организации работодатель (обладатель конфиденциальной информации) должен:

• ознакомить под расписку работника, доступ которого к конфиденциальной информации необходим для выполнения им своих трудовых обязанностей, с Перечнем конфиденциальной документированной информации организации;

• ознакомить под расписку работника с установленным режимом конфиденциальности информации и с мерами ответственности за его нарушение в соответствии с Регламентом доступа к информации по следующей типовой форме*.

---

* Данная типовая форма может быть приложением к Регламенту доступа к конфиденциальной информации.

ОБЯЗАТЕЛЬСТВО
о неразглашении конфиденциальной информации

Я, _____,
(фамилия, имя, отчество, должность)
в качестве работника
_____
(наименование структурного подразделения)
(именуемого в дальнейшем «Организация») в период трудовых (служебных) отношений с Организацией (ее правопреемником) и в течение _____ лет после их окончания, в соответствии с п. __ трудового договора, заключенного между мной и Организацией, а также соответствующими положениями по обеспечению защиты и охраны конфиденциальной информации, действующими в Организации, обязуюсь:

1) не разглашать конфиденциальную информацию Организации, которая мне будут доверена или станет известна по работе (службе);

2) не передавать третьим лицам и не раскрывать публично конфиденциальную информацию Организации без согласия Организации;

3) выполнять относящиеся ко мне требования приказов, инструкций и положений по обеспечению сохранности конфиденциальной информации Организации;

4) в случае попытки посторонних лиц получить от меня конфиденциальную информацию Организации немедленно сообщить
_____;
(должностное лицо или подразделение Организации)

5) сохранять конфиденциальную информацию тех организаций, с которыми у Организации имеются деловые отношения;

6) не использовать знание конфиденциальной информации Организации для занятий любой деятельностью, которая может нанести ущерб Организации;

7) в случае моего увольнения все носители конфиденциальной информации Организации (рукописи, черновики, чертежи, магнитные ленты, диски, дискеты, распечатки на принтерах, кино-, фотонегативы и позитивы, модели, материалы, изделия и пр.), которые находились в моем распоряжении в связи с выполнением мною служебных обязанностей во время работы в Организации, передать
_____
(должностное лицо или подразделение Организации)

8) об утрате или недостаче носителей конфиденциальной информации, удостоверений, пропусков, ключей от режимных помещений, хранилищ, сейфов (металлических шкафов), личных печатей и о других фактах, которые могут привести к разглашению конфиденциальной информации Организации, а также о причинах и условиях возможной утечки сведений немедленно сообщать
_____
(должностное лицо или подразделение Организации)

Я предупрежден, что в случае невыполнения любого из пп. 1, 2, 3, 4, 5, 6, 8 настоящего обязательства могу быть уволен из Организации в соответствии с п. «в» ч. 6 ст. 81 ТК РФ.

До моего сведения также доведены с разъяснениями соответствующие положения по обеспечению сохранности конфиденциальной информации Организации, и я получил один экземпляр этих положений.

Мне известно, что нарушение этих положений может повлечь уголовную, административную, гражданско-правовую или иную ответственность, предусмотренную ст. 13.11, 13.14 КоАП РФ, ст. 183 УК РФ, иными нормативными правовыми актами Российской Федерации, в виде лишения свободы, денежного штрафа, обязанности по возмещению ущерба Организации (убытков, упущенной выгоды и морального ущерба) и других наказаний.

С Перечнем конфиденциальной документированной информации Организации и Регламентом по доступу к конфиденциальной информации ознакомлен.

_____	_____	_____
(подпись)	(расшифровка подписи)	(дата подписания)

Руководство Организации подтверждает, что данные Вами обязательства не ограничивают Ваших прав на интеллектуальную собственность. Об окончании срока действия обязательства руководство Организации уведомит Вас заблаговременно в письменной форме.

«_____» _____ _____ г.

_____	_____	_____
(должность)	(подпись)	(расшифровка подписи)

Обязательства составлены в двух экземплярах. Один экземпляр находится у работника, второй хранится в Организации в качестве приложения к трудовому договору или личному делу работника.

Один экземпляр обязательств получил.

_____	_____	_____
(подпись)	(расшифровка подписи)	(дата подписания)

Основными требованиями доступа к конфиденциальной информации являются:

- наличие приказа о приеме на работу, переводе, временном замещении, изменении должностных обязанностей и др. или назначении на должность, которая предусматривает работу с конфиденциальной информацией;
- наличие подписанного сторонами трудового договора (служебного контракта для государственных служащих), имеющего пункт о неразглашении конфиденциальной информации, составляющей какую-либо тайну Организации, например секрет производства, кроме государственной тайны, или подписанного обязательства

о неразглашении информации и обеспечении защиты и охраны конфиденциальности информации, обладателем которой являются Организация и ее контрагенты.

4.3. Особенности доступа к конфиденциальной документированной информации при ее предоставлении уполномоченным органам государственной власти

Предоставление конфиденциальной информации – это передача информации, зафиксированной на материальном носителе, ее обладателем органам государственной власти в целях выполнения ими функций. Обладатель конфиденциальной информации по мотивированному требованию уполномоченных органов государственной власти должен предоставлять им данную информацию на безвозмездной основе.

Руководство организации, Экспертная комиссия по защите конфиденциальной информации, Службы безопасности, делопроизводства, кадров и другие подразделения должны знать, что без мотивированного требования, которое должно быть подписано уполномоченным должностным лицом и содержать указание цели, а также без правового основания затребования конфиденциальной информации и определения срока ее предоставления конфиденциальная информация в соответствии с законодательством может не предоставляться.

В случае отказа обладателя конфиденциальной информации предоставить ее уполномоченному органу государственной власти, последний вправе затребовать ее только в судебном порядке.

Особенность доступа к предоставляемой конфиденциальной информации заключается в том, что документы, которые содержат информацию, составляющую коммерческую тайну, должны иметь гриф ограничения доступа «Коммерческая тайна» с указанием ее обладателя (для юридических лиц – полное наименование и место нахождения, для индивидуальных предпринимателей – фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

В случае предоставления организацией (юридическим лицом или индивидуальным предпринимателем) информации уполномоченные органы в соответствии с российским законодательством обязаны создать условия, обеспечивающие ее защиту и охрану, а также регламентированный доступ к ней. Информация, относящаяся к коммерческой тайне, секретам производства, профессиональной тайне и др., предоставленная в уполномоченные органы, становится служебной тайной этих органов.

Должностные лица уполномоченных органов (государственные или муниципальные служащие), которым в силу выполнения должностных (служебных) обязанностей стала известна конфиденциальная информация, без согласия обладателя этой информации не вправе разглашать или передавать ее другим лицам, органам государственной власти, другим государственным органам, органам местного самоуправления, а также не вправе использовать эту информацию в корыстных или иных личных целях.

4.4. Особенности доступа к конфиденциальной документированной информации, составляющей персональные данные

4.4.1. Письменное согласие субъекта персональных данных на доступ к ним и их дальнейшую обработку

Физическое лицо – субъект персональных данных – принимает решение о доступе к ним и их предоставлении, а также дает согласие на обработку этих данных своей волей и в своих интересах. Согласие на обработку персональных данных может быть отозвано физическим лицом (более подробно технологии обработки персональных данных были рассмотрены в разд. 1.2).

В российском законодательстве предусматриваются случаи обязательного предоставления субъектом персональных данных (без всякого согласия) конфиденциальной информации в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Обработка конфиденциальной информации осуществляется только с согласия субъекта персональных данных в письменной форме, где указываются:

- фамилия, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- наименование (фамилия, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных;
- цель обработки конфиденциальной информации – персональных данных;

• перечень персональных данных, на обработку которых дает согласие субъект этих данных;

• перечень действий с персональными данными, на совершение которых дается согласие;

• общее описание используемых оператором способов обработки персональных данных;

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

Доступ к специальным категориям персональных данных. Доступ к конфиденциальной информации и дальнейшая обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускаются. Не требуется согласия физического лица, если доступ к конфиденциальной информации и дальнейшая обработка персональных данных осуществляются и необходимы в определенных случаях, а именно:

• если субъект персональных данных, в том числе биометрических (конфиденциальная информация, которая характеризует физиологические особенности человека и на основе которой можно установить его личность), дал согласие в письменной форме на обработку этих данных;

• если персональные данные являются общедоступными;

• если персональные данные относятся к состоянию здоровья субъекта и их обработка необходима для защиты его жизни, здоровья или реализации иных жизненно важных для него либо других лиц интересов, а получение согласия субъекта невозможно;

• если необходимо установить медицинский диагноз, оказать медицинские и медико-социальные услуги либо использовать эту информацию в медико-профилактических целях, при условии, что обработка персональных данных осуществляется лицом, которое профессионально занимается медицинской деятельностью и обязано в соответствии с законодательством Российской Федерации сохранять врачебную тайну [19, ст. 61];

• если в учредительных документах общественного объединения или религиозной организации указано, что обработка персональных данных членов (участников) выполняется соответствующими общественным объединением или религиозной организацией и эта информация не будет распространяться без согласия в письменной форме физического лица;

• если доступ и дальнейшая обработка персональных данных, в том числе биометрических, осуществляются в соответствии с правосудием и законодательством Российской Федерации о безопасности, об оперативно-розыскной деятельности [47], а также в соответствии с уголовно-исполнительным законодательством Российской Федерации [13];

• если доступ и дальнейшее использование конфиденциальной информации о наличии судимости субъекта персональных данных осуществляются государственными или муниципальными органами в пределах полномочий, предоставленных им в соответствии с законодательством Российской Федерации [22].

Без согласия субъекта биометрических персональных данных доступ к ним и дальнейшая их обработка могут осуществляться в связи с отправлением правосудия, а также в случаях, предусмотренных законодательством Российской Федерации о безопасности [24; 34; 52], об оперативно-розыскной деятельности, о государственной службе [30], о порядке выезда из Российской Федерации и въезда на ее территорию [45].

4.4.2. Уведомление об обработке персональных данных

При намерении заняться обработкой персональных данных или ее выполнении оператор должен направить в уполномоченный орган по защите прав субъектов персональных данных установленное нормативными документами уведомление.

Федеральным законом «О персональных данных» указаны случаи, когда допускается обработка персональных данных без уведомления уполномоченного органа. Оператор вправе осуществлять без уведомления уполномоченного органа обработку персональных данных, если:

• субъектов персональных данных связывают с оператором трудовые отношения в соответствии с ТК Российской Федерации [8, гл. 14], законодательством о государственной службе и о муниципальной службе [30];

• полученные оператором персональные данные в связи с заключением договора, одной стороной которого является субъект персональных данных, не распространяются, а также не предоставляются третьим лицам без согласия субъекта и используются оператором исключительно для исполнения указанного договора;

• конфиденциальная информация не будет распространяться без согласия в письменной форме субъектов персональных данных, относящихся к членам (участникам) общественного объединения или религиозной организации и будет обрабатываться указанными объединением или организацией для достижения ими законных целей, предусмотренных их учредительными документами;

• персональные данные являются общедоступными;

• персональные данные включают в себя только фамилию, имя и отчество физического лица;

• персональные данные необходимы в целях однократного пропуска физического лица на территорию, на которой находится оператор, или в иных аналогичных целях;

• персональные данные включены в АИС, имеющие в соответствии с федеральными законами статус федеральных, а также в государственные АИС, созданные в целях защиты безопасности государства и общественного порядка [75];

• персональные данные, обрабатываемые без средств автоматизации, или в соответствии с нормативными правовыми актами, устанавливающими требования к обеспечению безопасности при их обработке, отвечают соблюдению прав физических лиц [22, ст. 22, п.1, 2; 78; 82].

О своем намерении осуществить обработку персональных данных оператор обязан уведомлять уполномоченный орган по защите прав физических лиц (таким органом является федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи). Уведомление должно быть направлено в письменной или электронной форме и подписано уполномоченным лицом либо иметь электронную цифровую подпись.

Уведомление оформляется на бланке оператора, осуществляющего обработку персональных данных, и направляется в территориальный орган Россвязькомнадзора. Оно может быть направлено либо в письменной форме и подписано уполномоченным лицом, либо в электронной форме с электронной цифровой подписью (ЭЦП).

Форма уведомления об обработке (о намерении осуществлять обработку) персональных данных приведена ниже [121].

Руководителю Управления Федеральной службы
по надзору в сфере связи и массовых коммуникаций
по_____

УВЕДОМЛЕНИЕ
об обработке (о намерении осуществлять обработку) персональных данных

_____
(наименование (фамилия, имя, отчество), адрес оператора)
руководствуясь_____
(правовое основание обработки персональных данных)
в целях_____
(цель обработки персональных данных)
осуществляет обработку_____
(категории персональных данных)
принадлежащих_____
(категории субъектов, персональные данные которых обрабатываются)

Обработка вышеуказанных персональных данных будет осуществляться путем _____
(перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных)
_____
(описание мер, которые оператор обязуется осуществлять при обработке персональных данных, по обеспечению безопасности персональных данных при их обработке)

Дата начала обработки персональных данных_____

Срок или условие прекращения обработки персональных данных_____
_____

_____ _____ _____
(должность) (подпись) (расшифровка подписи)

«____» _____ _____ г.

В поле «наименование (фамилия, имя, отчество), адрес оператора» указываются следующие сведения:

1. Для юридических лиц (операторов):

- полное наименование с указанием организационно-правовой формы и сокращенное наименование юридического лица (оператора), осуществляющего обработку персональных данных;
- наименование филиала(ов) (представительства юридического лица (оператора), производящего обработку персональных данных;
- место нахождения;
- индивидуальный номер налогоплательщика (ИНН);

2. Для физических лиц:

• фамилия, имя, отчество физического лица (оператора);

• место жительства;

• данные документа, удостоверяющего личность, – дата его выдачи, наименование органа, выдавшего документ, удостоверяющий личность;

3. Для государственных, муниципальных органов (операторов):

• полное и сокращенное наименование государственного, муниципального органа;

• наименование территориального(ых) органа(ов), осуществляющего(их) обработку персональных данных;

• место нахождения;

• индивидуальный номер налогоплательщика (ИНН).

При указании наименования (фамилии, имени, отчества), адреса оператора, а также направления деятельности рекомендуется использовать также ссылки на код(ы) классификаторов (ОКВЭД, ОКПО, ОКОГУ, ОКОП, ОКФС).

В поле «цель обработки персональных данных» указываются цели обработки персональных данных (а также их соответствие полномочиям оператора). Под целью обработки персональных данных понимаются как цели, указанные в учредительных документах оператора, так и цели фактически осуществляемой оператором деятельности по их обработке.

В поле «категории персональных данных» указываются все категории персональных данных, подлежащих обработке.

В поле «категории субъектов, персональные данные которых обрабатываются», указываются категории субъектов (физических лиц) и виды отношений с субъектами (физическими лицами), персональные данные которых обрабатываются, например: работники (субъекты), состоящие в трудовых отношениях с юридическим лицом (оператором); физические лица (абонент, пассажир, заемщик, вкладчик, страхователь, заказчик и другие субъекты), состоящие в договорных и иных гражданско-правовых отношениях с юридическим лицом (оператором) и др.

В поле «правовое основание обработки персональных данных» указываются: федеральный закон, постановление Правительства Российской Федерации, иной нормативный правовой акт, закрепляющие основание и порядок обработки персональных данных (указываются не только соответствующие статьи Федерального закона «О персональных данных», но и статьи иного нормативного правового акта, регулирующие осуществляемый вид деятельности и ка-

сающиеся их обработки, например: ст. 85–90 Трудового кодекса Российской Федерации, ст. 85.1 Воздушного кодекса Российской Федерации, ст. 12 Федерального закона «Об актах гражданского состояния» и др.); номер, дата выдачи и наименование лицензии на осуществляемый вид деятельности с указанием лицензионных условий, закрепляющих запрет на передачу персональных данных третьим лицам без согласия в письменной форме субъекта персональных данных.

В поле «перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных» указываются действия, совершаемые с ними оператором, а также описание используемых им способов их обработки:

- неавтоматизированная обработка персональных данных;
- исключительно автоматизированная обработка персональных данных с передачей полученной информации по сети или без таковой;
- смешанная обработка персональных данных.

При автоматизированной обработке, а также смешанной обработке необходимо указать, будет ли осуществляться передача полученной в ходе их обработки информация по внутренней сети юридического лица (информация доступна лишь для строго определенных сотрудников юридического лица) или по сети общего пользования – Интернет либо такая передача не будет производиться.

В поле «описание мер, которые оператор обязуется осуществлять при обработке персональных данных по обеспечению их безопасности» указываются организационные и технические меры, в том числе использование шифровальных (криптографических) средств, используемых для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения и иных неправомерных действий при их обработке.

В поле «дата начала обработки персональных данных» указывается конкретная дата начала совершения действий с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование и их уничтожение (фактическая дата начала обработки персональных данных).

В поле «срок или условие прекращения обработки персональных данных» указывается конкретная дата или основание (условие), наступление которого повлечет прекращение обработки.

4.5. Особенности доступа к архивным конфиденциальным документам

Согласно ст. 24 и 25 Федерального закона «Об архивном деле в Российской Федерации», «доступ к архивным документам может быть ограничен в соответствии с международным договором Российской Федерации, законодательством Российской Федерации, а также в соответствии с распоряжением собственника или владельца архивных документов, находящихся в частной собственности. Условия доступа к архивным документам, находящимся в частной собственности, за исключением архивных документов, доступ к которым регламентируется законодательством Российской Федерации, устанавливаются собственником или владельцем архивных документов» [27].

Ограничивается доступ к архивным документам независимо от их форм собственности, содержащим сведения, составляющие государственную и иную охраняемую законодательством Российской Федерации тайну, а также к подлинникам особо ценных документов, в том числе уникальных документов, и документам Архивного фонда Российской Федерации, признанным в порядке, установленном специально уполномоченным Правительством Российской Федерации федеральным органом исполнительной власти и находящимся в неудовлетворительном физическом состоянии.

Отмена ограничения на доступ к архивным документам, содержащим сведения, составляющие государственную и иную охраняемую законодательством Российской Федерации тайну, осуществляется в соответствии с законодательством Российской Федерации о государственной тайне и других видах тайн – конфиденциальной информации (см. гл. 1).

Право собственности на архивные документы независимо от их форм собственности охраняется законом. Изъятие архивных документов, не предусмотренное федеральными законами, запрещается. Архивные документы, находящиеся в незаконном владении, подлежат передаче собственникам или законным владельцам в соответствии с международным договором Российской Федерации и законодательством Российской Федерации.

К конфиденциальным архивным документам ограниченного доступа относятся документы государственной и негосударственной частей Архивного фонда Российской Федерации, содержащие информацию, отнесенную российским законодательством к конфиденциальной информации, составляющей какую-либо тайну, за исключением государственной тайны. Государственная часть

Архивного фонда Российской Федерации – архивные фонды и архивные документы, являющиеся государственной или муниципальной собственностью. Негосударственная часть Архивного фонда Российской Федерации, – архивные фонды и архивные документы, являющиеся собственностью негосударственных юридических лиц, собственностью физических лиц и включенные в состав Архивного фонда Российской Федерации на основании соглашения (договора) с собственником после экспертизы их ценности.

Пользователь архивными документами имеет право свободно искать и получать для изучения архивные документы. Доступ к ним обеспечивается путем предоставления пользователю справочно-поисковых средств и информации об этих средствах, а также подлинников и (или) копий необходимых ему документов. Условия доступа к находящимся в частной собственности, за исключением тех документов, доступ к которым регламентируется законодательством Российской Федерации, устанавливаются собственником или владельцем архивных документов.

Следует отметить, что действие Федерального закона «О персональных данных» не распространяется на отношения, возникающие при организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда Российской Федерации, а также других архивных документов, в соответствии с законодательством об архивном деле.

Государственные органы, органы местного самоуправления, организации и граждане, занимающиеся предпринимательской деятельностью без образования юридического лица, обязаны обеспечивать сохранность архивных документов, в том числе по личному составу, в течение сроков их хранения, установленных федеральными законами или иными нормативными правовыми актами Российской Федерации, а также перечнями типовых архивных документов с указанием сроков их хранения или отраслевыми перечнями.

В этом разделе определена работа архива (учреждения или структурного подразделения организации, осуществляющих хранение, комплектование, учет и использование архивных документов) в части доступа пользователей к архивной конфиденциальной документированной информации.

Государственный или муниципальный архив, в том числе архив как структурное подразделение организации (далее – Архив), не вправе ограничивать или устанавливать пользователям условия использования документированной информации, полученной ими в результате самостоятельного поиска, и обязан обеспечивать в установленном порядке доступ к конфиденциальным документам, базам и банкам данных с уче-

том ограничений, установленных законодательными и нормативными правовыми актами Российской Федерации или оговоренных в договоре Архива с пользователем по информационному обслуживанию.

Доступ пользователей к архивным документам определен Правилами организации хранения, комплектования, учета и использования документов Архивного фонда Российской Федерации и других архивных документов в государственных и муниципальных архивах, музеях и библиотеках, организациях Российской академии наук (далее – Правилами) [128].

В соответствии с этими Правилами Архив предоставляет пользователю открытые документы Архивного фонда Российской Федерации и другие документы, а также справочно-поисковые средства к ним и издания библиотечного (справочно-информационного) фонда.

Архив обеспечивает доступ пользователя к секретным делам, делам, содержащим конфиденциальную информацию, базам данных с учетом ограничений, определенных законодательством Российской Федерации, и условий, которые установили собственники или владельцы архивных документов при их передаче в Архив.

Доступ пользователя к подлинникам особо ценных документов, в том числе уникальных, и к документам Архивного фонда Российской Федерации, находящимся в неудовлетворительном физическом состоянии, осуществляется в исключительных случаях (в том числе для проведения работ по изучению палеографических особенностей текстов архивных документов) с письменного разрешения руководителя Архива. Пользователю предоставляются копии указанных документов (фонд пользования) или документальные публикации, содержащие эти документы.

Руководитель Архива организует проведение работы по контролю за сроками секретности и конфиденциальности архивных документов и информирует руководителей государственных органов, наделенных полномочиями по отнесению сведений к государственной тайне и конфиденциальной информации, а также руководителей организаций о наличии в Архиве секретных и конфиденциальных документов со сроками секретности содержащихся в них сведений свыше 30 лет, их составе и объемах.

Анализ и учет состояния системы научно-справочного аппарата Архива производятся либо на бумажном носителе (журнал по учету состояния научно-справочного аппарата, картотека), либо в автоматизированном режиме. Архив дает пользователю соответствующие разъяснения или выдает копии части дела, документа, не содержащих указанные сведения конфиденциального характера, а также предупреждает его об ответственности за сохранение конфиденциальных сведений, содержащихся в документах.

Доступ пользователей к документам с пометками «Для служебного пользования», «Коммерческая тайна», «Конфиденциально», «Строго конфиденциально», а также без пометок осуществляется в порядке, установленном для документов ограниченного доступа (см. разд. 4.1–4.3). Этот порядок сохраняется при передаче дел в государственный или муниципальный Архив, а также Архив другой организации, если фондообразователь, Экспертная комиссия по защите конфиденциальной информации или ликвидационная комиссия не оговорили особых требований доступа относительно данной категории документов.

Хранящимися на особых условиях доступа являются документы, собственники которых, передавая их в Архив на постоянное хранение, т.е. в собственность государства, или на временное, в том числе депозитарное, оговорили особые условия доступа к ним и их использования в соглашении (договоре).

Архив ограничивает доступ пользователей к документам, содержащим информацию о фактах, событиях и обстоятельствах частной жизни конкретного лица, если не истек срок в 75 лет с момента их создания. К таким документам и делам относятся: личные, персональные, следственные, судебные дела, документы служб кадров, персонифицированные материалы переписей, социологических и иных обследований, медицинская документация, личная переписка. Ограничения на доступ к документам, содержащим информацию о частной жизни граждан, устанавливаются при наборе персональных данных, позволяющих в совокупности идентифицировать личность. Ограничение на доступ к архивным документам, содержащим сведения о личной и семейной тайне гражданина, его частной жизни, а также сведения, создающие угрозу для его безопасности, устанавливается на срок 75 лет со дня создания указанных документов. С письменного разрешения гражданина, а после его смерти – с письменного разрешения наследников данного гражданина ограничение на доступ к указанным выше архивным документам может быть отменено ранее, чем через 75 лет со дня создания этих документов [27, ст. 25].

Ограничения на доступ к сведениям о частной жизни ранее 75-летнего срока снимаются в случае:

- наличия письменного, нотариально заверенного распоряжения физического лица – субъекта персональных данных или его наследника – на передачу этих сведений третьему лицу для ознакомления с ними;
- обезличивания персональных данных путем изъятия при копировании той их части, которая позволяет отождествить их с конкретным человеком.

Субъект персональных данных для получения сведений о его частной жизни может установить режим общедоступной информации, проинформировав об этом руководство Архива. Документы, содержащие информацию о персональных данных, Архив может выдавать пользователям для проведения статистических, социологических, демографических и других научных и практических исследований, составления биобиблиографических справочников, биографий, публикации документальных изданий при условии соблюдения пользователем прав личности на неприкосновенность частной жизни.

По запросам организаций разрешается выдавать справки, содержащие информацию о служебной и общественной деятельности граждан, для использования их в указанных выше целях.

Архив по заявкам пользователей на копирование документов осуществляет услугу по обезличиванию персональных данных, т.е. действия, в результате которых невозможно определить принадлежность персональных данных конкретному физическому лицу, придавая им при копировании форму анонимных сведений.

Запрещается без согласия усыновителей, а в случае их смерти без согласия органов опеки и попечительства выдавать гражданам документы, содержащие сведения об усыновлении (тайна усыновления, семейная тайна – см. разд. 1.2).

Архив также имеет право отказать до истечения 75-летнего срока с момента создания документов в выдаче выписок из книг регистрации актов гражданского состояния, решений судов, органов исполнительной власти и образования, из которых было бы видно, что усыновители не являются кровными родителями усыновленного. В исключительных случаях Архив знакомит заинтересованных лиц с записями актовых книг с разрешения руководителя органа записи актов гражданского состояния или органа исполнительной власти субъекта Российской Федерации.

Архив может выслать по запросам органов записи актов гражданского состояния, опеки, попечительства, правоохранительных органов, нотариата, а также судов и органов юстиции копии записей актов гражданского состояния. Он имеет также право предоставлять для пользования документы, содержащие коммерческую и служебную тайны, за исключением государственной тайны (особый режим доступа), хранящиеся в фондах организаций, независимо от их организационно-правовой формы, по мотивированным запросам уполномоченных органов государственной власти – правоохранительных, антимонопольных органов, органов арбитража, судов, прокуратуры, налоговых служб (см. разд. 4.3). Конфиденциальные

документы, содержащие коммерческую, служебную, профессиональную тайны, секреты производства и служебные секреты производства, могут быть выданы также иным пользователям на основании письменного разрешения фондообразователя или его правопреемника.

Доступ к научно-популярным, документальным фильмам и другим кинодокументам осуществляется по согласованию с правообладателями и с соблюдением авторских и смежных прав, в том числе на основании договоров (соглашений).

Выдача пользователям произведений, перешедших по истечении установленных законодательством Российской Федерации сроков в общественное достояние, не ограничивается.

4.6. Особенности доступа должностных лиц при их командировании к конфиденциальной документированной информации

При командировании работников в другие организации-контрагенты для проведения совместных работ им выдаются справки, удостоверяющие наличие у них доступа к конфиденциальной информации другой организации (далее – справка).

Справка выдается Службой безопасности организации, в которой работает командированный, под расписку командированного в журнале (карточке) учета выдачи справок о доступе на срок разовой командировки или на срок выполнения задания, но не более чем на год. Справка подписывается руководителем Службы безопасности или Службы кадров и заверяется печатью организации. Делать в справке отметки, содержащие конфиденциальную информацию, запрещается.

На обороте справки о допуске указываются степень конфиденциальности информации, с которой ознакомилось командированное лицо, и дата. Запись заверяется подписью руководителя Службы безопасности организации или Службы кадров, куда было командировано должностное лицо, и печатью организации [223].

Справка возвращается ее владельцу для сдачи в Службу безопасности или Службу кадров по месту его постоянной работы, после чего уничтожается, о чем делается отметка в журнале (карточке), которая заверяется подписями двух сотрудников Службы безопасности. При этом акт на уничтожение не оформляется.

Кроме справки, командировочному выдается предписание на выполнение задания. *Предписание* – это документ на выполнение задания, связанного с информацией конфиденциального характера, который подписывается руководителем организации или структурного подразделения организации и заверяется печатью организации.

В предписании кратко излагается основание командирования (номер и дата приказа, договора, совместный план научно-исследовательских и опытно-конструкторских работ и т.д.), а также определяется, с какой информацией необходимо ознакомить командируемое лицо для выполнения им задания.

Предписание, в котором содержится информация всех степеней конфиденциальности («Конфиденциально», «Совершенно конфиденциально»), пересылается почтой в порядке, установленном для конфиденциальных документов (см. разд. 3.5). Предписание выдается для посещения только одной организации. Командированное лицо может иметь доступ только к той информации, которая ему необходима в рамках выполняемого задания, указанного в предписании. Доступ для ознакомления с данной информацией осуществляется с письменного разрешения руководителя принимающей организации или структурного подразделения.

Предписание на выполнение задания с разрешением руководителя принимающей организации ознакомить командированное лицо с конфиденциальной информацией вместе со справками о допуске регистрируется в журнале (картотеке) учета командированных.

Предписание с визой соответствующего руководителя подразделения и отметкой о доступе командированного лица передается принимающим его должностным лицам. Те, в свою очередь, производят на обороте предписания отметки о степени конфиденциальности информации, с которой фактически ознакомилось командированное лицо. Отметки подтверждаются подписью командированного лица, после чего один экземпляр предписания передается для хранения в Службу безопасности организации, а также другой организации, в которую прибыл командированный.

Предписание хранится в специальном деле в Службе безопасности или Службе кадров организации, а также в принимающей организации в течение не менее 5 лет.

Доступ к конфиденциальной информации командируемых работников и должностных лиц в принимающей организации осуществляется после предъявления ими документов, удостоверяющих личность, справок о доступе, предписаний на выполнение заданий [72].

4.7. Учет персонала, получившего доступ к конфиденциальной документированной информации, и (или) лиц, которым она была передана или предоставлена

Особенность информационного обслуживания пользователей – потребителей конфиденциальной информации заключается в том, что вопросы определения состава необходимой им информации решаются должностным лицом, дающим разрешение на доступ к информации в зависимости от Перечня конфиденциальной документированной информации организации, а не самими пользователями.

Структура технологии разграничения доступа должна быть многоуровневой, иерархической. Иерархическая последовательность доступа к информации реализуется по следующим принципам:

- чем выше уровень доступа, тем уже круг допущенных лиц;
- чем выше ценность информации, тем меньшее число персонала может ее знать.

Выдача допуска или санкций (разрешений) на доступ к конфиденциальной информации осуществляется с учетом двух аспектов:

1) выдачи разрешений в зависимости от категории конфиденциальной информации, в соответствии с Перечнем конфиденциальной документированной информации и Реестром конфиденциальной информации и автоматизированной информационной системы организации;

2) выдачи разрешений в зависимости от занимаемой должности лица, выдающего разрешение.

Задачей технологии разграничения доступа является регламентация минимальных потребностей персонала в конфиденциальной информации. Это дает возможность разделить знание персонала о конфиденциальной информации на элементы знания информации в целом.

В соответствии с иерархической последовательностью доступа определяется структура границ защиты информации, которая предусматривает постепенное ужесточение защитных мер по иерархической вертикали, возрастание степени конфиденциальности информации. Этим обеспечивается недоступность информации для случайных людей или злоумышленников и определяется необходимая степень защищенности информации. Поэтому технологии ограничения доступа предполагают создание в организации номенклатуры должностей работников, подлежащих оформлению на допуск к конфиденциальной документированной информации по форме 1.

Форма 1

_____

Утверждаю

_____

(руководитель организации или зам. руководителя по вопросам защиты КДИ)

«___»_____20___ г.

Номенклатура должностей работников, подлежащих оформлению на допуск к КДИ

(по заполнении конфиденциально)

№ п/п	Подразделение	Количество работающих	Должность	Обоснование необходимости допуска	Количество лиц, подлежащих оформлению на доступ к КДИ			Количество лиц, оформленных на доступ к КДИ	Примечание
					вид конфиденциальной информации	степень «Конфиденциально»	степень «Строго конфиденциально»		
1	2	3	4	5	6	7	8	9	10

«___» _____ 20__ г.

Руководитель Службы безопасности _____

(подпись)

Примечания.

1. Должности в номенклатуре указываются по каждому структурному подразделению с подведением итогов.
2. Порядковые номера указываются в возрастающей последовательности независимо от структурных подразделений.
3. В графе 5 кратко отражаются характер документов или выполняемых работ и степень их конфиденциальности со ссылкой на конкретный пункт Перечня конфиденциальной документированной информации.
4. В графе 9 указывается только общее количество лиц, подлежащих оформлению на допуск к конфиденциальной документированной информации, без обоснования необходимости допуска.
5. В графах 6–9 подводится итог по организации.

Номенклатура составляется Службой безопасности совместно со Службой кадров, согласовывается с Экспертной комиссией по защите конфиденциальной информации и подписывается руководителем организации.

Номенклатура хранится в Службе безопасности, второй экземпляр – в Службе кадров организации, третий – в Службе делопроизводства. В номенклатуру включаются должности, по которым допуск персонала к этой информации действительно необходим для выполнения ими должностных обязанностей, а также могут включаться должности работников, допуск которых к информации соответствующей степени конфиденциальности необходим для выполнения ими заданий в других организациях при их командировании (см. разд. 4.6).

Изменения и дополнения в номенклатуру вносятся по мере необходимости, согласовываются и утверждаются в установленном порядке. Номенклатура должностей пересматривается не реже одного раза в 5 лет [72].

Технология доступа к конфиденциальной информации также включает учет должностных лиц других организаций, получивших доступ, и (или) лиц, которым такая информация была предоставлена или передана. Учет производится по форме 2.

Журнал (картотека) может вестись в автоматизированном режиме. При обнаружении факта утраты конфиденциальной документированной информации или факта разглашения информации должно вводиться ограничение на доступ или прекращение доступа к любой информации до окончания служебного расследования, которое оформляется актом по следующей типовой форме 3.

Форма 2

ЖУРНАЛ (КАРТОТЕКА)
учета работников, включая работников других организаций, получающих в пользование конфиденциальную документированную информацию

Дата выдачи документа	Номер записи	Наименование документа	Номер и дата документа	Наименование структурного подразделения или иной организации	Должность, фамилия, имя, отчество
1	2	3	4	5	6

Окончание

Цель получения	Основание получения	Расписка в получении	Дата возврата	Подтверждение возврата (подпись лица, ответственного за выдачу документов)	Примечание
7	8	9	10	11	12

Форма 3

АКТ
проведения внутреннего расследования по факту разглашения информации и (или) утраты, хищения, порчи документов

(дата)_____

Комиссия в составе:
председатель комиссии _____
(должность, фамилия, имя, отчество)
члены комиссии:
1. _____
(должность, фамилия, имя, отчество)
2. _____
(должность, фамилия, имя, отчество)
3. _____
(должность, фамилия, имя, отчество)
по факту _____
(хищение, разглашение, порча документов, другое)
на основании _____
(докладная записка, акт проверки, другое)
провели расследование и выяснили следующее: _____

Прилагаются документы:
1. Объяснительная записка
_____
(структурное подразделение, должность, фамилия, имя, отчество работника)
2. _____
3. _____

На основании полученной информации и прилагаемых документов комиссия сделала вывод: _____

Акт составлен в 3-х экземплярах:
1-й экз. подшит в дело № __.
2-й экз. передан работнику.
Председатель комиссии: _____
(подпись) (расшифровка подписи)

Члены комиссии: _____
(подпись) (расшифровка подписи)
_____
(подпись) (расшифровка подписи)
_____
(подпись) (расшифровка подписи)

3-й экз. подшит в личное дело.

ГЛАВА 5

СОСТАВЛЕНИЕ НОМЕНКЛАТУРЫ ДЕЛ, ФОРМИРОВАНИЕ И ОФОРМЛЕНИЕ КОНФИДЕНЦИАЛЬНЫХ ДЕЛ

5. 1. Документальный фонд организации

5.1.1. Общие положения

Документальный фонд федерального органа исполнительной власти формируется в порядке, установленном Правительством Российской Федерации в Правилах делопроизводства и документооборота [76]. Как ранее говорилось, требования, установленные в Правилах делопроизводства, могут распространяться и на негосударственные структуры. В связи с этим в этом разделе будут рассмотрены общие требования по составлению номенклатуры дел, формированию дел в соответствии с Правилами делопроизводства и документооборота федеральных органов исполнительной власти, адаптированными на государственные и негосударственные структуры.

В соответствии с ГОСТ Р 51141–98 [163] «номенклатура дел – систематизированный перечень наименований дел, заводимых в организации, с указанием сроков их хранения, оформленный в установленном порядке»; «дело – совокупность документов или документ, относящихся к одному вопросу или участку деятельности, помещенных в отдельную обложку».

Основной формой учета конфиденциальных дел является номенклатура дел текущего года, в соответствии с которой организуются формирование, хранение и проверка наличия дел.

Организация (государственные и негосударственные структуры) выполняет следующие функции:

• формирует свой документальный фонд из образующихся в процессе ее деятельности документов;

• разрабатывает и утверждает по согласованию с уполномоченными органами в области архивного дела перечень документов, образующихся в процессе ее деятельности, а также подведомственных ей организаций, с указанием сроков хранения.

Документальный фонд организации создается Службой делопроизводства организации, которая составляет номенклатуру дел, формирует и оформляет дела, обеспечивает их сохранность и ведет учет, передает дела в Архив организации. Порядок группировки конфиденциальных дел предусматривается номенклатурами дел открытого делопроизводства.

Номенклатура дел организации составляется на основе номенклатур дел структурных подразделений. После ее согласования с Экспертной проверочной комиссией (ЭПК) утверждается руководителем организации не позднее конца текущего года и вводится в действие с 1 января следующего года. Один раз в 5 лет она согласовывается с Экспертно-проверочной комиссией федерального государственного архива, куда на постоянное хранение передаются образующиеся в процессе деятельности организации документы Архивного фонда Российской Федерации. В случае изменения функций и структуры организации номенклатура также подлежит согласованию с Экспертно-проверочной комиссией федерального государственного архива [76, разд. IV].

Наименованиями разделов номенклатуры дел организации являются наименования структурных подразделений.

Дела формируются в соответствии с номенклатурой дел, а также с соблюдением принципов систематизации документов и их распределения (группировки) на дела постоянного и долговременного (свыше 10 лет) хранения, в том числе дела по личному составу, и дела временного (до 10 лет включительно) хранения.

Дела до передачи в Архив организации или на уничтожение хранятся в структурных подразделениях по месту их формирования. Дела выдаются во временное пользование сотрудникам структурных подразделений на срок, определяемый руководителем организации. После истечения этого срока они подлежат возврату.

Выдача дел другим организациям производится на основании их письменных запросов с разрешения руководителя организации или его заместителя, курирующего вопросы делопроизводства.

Изъятие документов из дел постоянного хранения допускается в исключительных случаях с разрешения руководителя организации. При этом в деле оставляется копия документа, заверенная в установленном порядке, и акт о причинах выдачи подлинника.

Дела постоянного и долговременного (свыше 10 лет) хранения передаются в Архив федерального органа исполнительной власти не ранее чем через год и не позднее 3 лет со дня начала их использования или хранения в структурных подразделениях. Передача дел в Архив организации производится на основании описей дел постоянного и долговременного (свыше 10 лет) хранения, в том числе дел по личному составу, составляемых в структурных подразделениях. Дела временного (до 10 лет включительно) хранения в Архив организации не передаются и подлежат уничтожению в установленном порядке (см. гл. 6).

Основой составления описей дел постоянного и долговременного (свыше 10 лет) хранения является номенклатура дел. Номенклатура дел может вестись в электронном виде как классификатор интегрированной автоматизированной информационной системы делопроизводства, что позволяет автоматически определять сроки хранения документов.

5.1.2. Особенности учета конфиденциальных дел и составления номенклатуры конфиденциальных дел

Номенклатура дел структурного подразделения организации, предназначенная для систематизации конфиденциальной документированной информации, может быть составной частью общей номенклатуры дел организации или существовать в качестве самостоятельного документа. По форме она не отличается от номенклатуры дел для несекретных, т.е. открытых, документов. Однако дополнительно в ней указываются: фамилия исполнителя (исполнителей), которому предоставлено право пользоваться делом; фамилия лица, ответственного за формирование и сохранность дела; инвентарный архивный номер дела; номер и дата акта об уничтожении; отметка о снятии отметки конфиденциальности доступа и передаче дела на открытое хранение и другая информация [209].

Для обеспечения оперативного поиска необходимых документов, создания условий для их сохранности и удобства использования исполненные конфиденциальные документы, поступившие, созданные (изданные) и заверенные копии отправляемых конфиденциальных документов должны быть сгруппированы в дела. В исключительных случаях конфиденциальную документированную

информацию в зависимости от производственной необходимости допускается группировать в дела отдельно или вместе с другими несекретными документами по одному и тому же вопросу. Дела формируются централизованно в Службе делопроизводства, которая обеспечивает их текущее и оперативное архивное хранение. Возможно децентрализованное оперативное хранение дел в структурных подразделениях организации.

Распределение документов по делам производится в течение года по мере их исполнения в соответствии с номенклатурой конфиденциальных дел.

Номенклатура конфиденциальных дел – это оформленный в установленном порядке систематизированный перечень наименований дел, заводимых в организации, с указанием их индексов (номеров), сроков хранения и лиц, которым предоставлено право пользования этими делами [209].

Таким образом, номенклатура конфиденциальных дел, определяя наименования (заголовки) дел и выступая тем самым в роли плана распределения исполненных документов по делам, одновременно устанавливает индексы и сроки хранения дел и является составной частью разрешительной системы доступа к конфиденциальной информации (см. гл. 4). Кроме того, номенклатура позволяет проверить наличие конфиденциальных дел и может быть использована в качестве схем построения справочной картотеки по конфиденциальным документам и составления описей дел постоянного и долговременного хранения (свыше 10 лет), передаваемых в Архив организации.

Номенклатура конфиденциальных дел – самостоятельный документ, ее не рекомендуется объединять с номенклатурой открытых дел, так как графы в формах этих номенклатур имеют существенные различия.

Номенклатура конфиденциальных дел разрабатывается в организации в целом (сводная номенклатура дел). Она составляется на каждый год (в конце текущего года на следующий год) Службой делопроизводства на основе письменных предложений структурных подразделений. К разработке номенклатуры должны привлекаться квалифицированные специалисты, имеющие доступ к соответствующим конфиденциальным документам и хорошо знающие направления деятельности организации, характер связей с другими учреждениями, организациями, предприятиями, состав конфиденциальных документов в соответствии с Перечнем конфиденциальной документированной информация организации (см. разд. 2.3),

Реестром конфиденциальной информации и автоматизированной информационной системы (см. разд. 3.7) и классификатором конфиденциальной информации (см. разд. 8.5.2), а также планами работы организации и ее структурных подразделений на предстоящий год.

Номенклатура дел подписывается руководителем Службы делопроизводства, визируется руководителями структурных подразделений, в которых оперативно хранятся конфиденциальные документы, согласовывается с Архивом организации, рассматривается на заседании постоянно действующей Экспертной проверочной комиссии и утверждается руководителем организации [295].

Такой порядок должен быть при первоначальной разработке номенклатуры конфиденциальных дел и в случае ее значительной переработки (существенное изменение заголовков дел, включение большого количества новых дел, расширение списка лиц, допущенных к делам). Если таких изменений нет, то на каждый последующий год (до 5 лет) номенклатура перепечатывается (с возможными незначительными изменениями), подписывается руководителем Службы делопроизводства, утверждается руководителем организации и вводится в действие без перечисленных выше согласований.

В случаях, когда образуется большое количество одних и тех же видов документов и дел (распоряжения, постановления, приказы, инструкции, отчеты, сводки и т. д.) с отметкой конфиденциальности и без этой отметки, но являющихся конфиденциальной документированной информацией, например кадровая документация – персональные данные, целесообразно предусматривать их обособленное формирование в дела. При этом в графе номенклатуры дел «Индекс дела» к номеру дела добавляется отметка конфиденциальности. При снятии с документов отметки конфиденциальности они перемещаются в аналогичное дело без этой отметки, которое хранится в Службе делопроизводства. Например:

Индексы дел	*Заголовки дел*
01-1	Приказы по основной деятельности
01-1/ДСП	То же
08-98	Переписка об аренде помещений
08-98/КФД	То же

При включении конфиденциальных документов в дело с несекретными (открытыми) документами, не имеющими отметки конфиденциальности, данное дело получает соответствующую отметку конфиденциальности, и это уточнение вносится в номенклатуру дел.

Если в деятельности структурного подразделения организации образуется небольшое количество конфиденциальной документированной информации, номенклатурой дел может быть предусмотрено заведение одного дела, которое именуется, например: «Материалы для служебного пользования» или «Конфиденциальные материалы». Срок хранения одного такого дела не устанавливается, а в соответствующей графе номенклатуры дел проставляется отметка ЭК (Экспертная комиссия).

Номенклатура должна иметь соответствующую отметку конфиденциальности, издаваться в двух экземплярах и регистрироваться в журнале регистрации созданных/изданных внутренних конфиденциальных документов. Первый экземпляр номенклатуры хранится в Службе делопроизводства и по окончании года подшивается в специальное дело, второй передается в качестве рабочего в Архив организации. Лица, допущенные к делам, должны быть ознакомлены с соответствующими разделами номенклатуры под подпись на первом экземпляре номенклатуры, что является основанием для привлечения их к ответственности в случаях неправильного адресования документов в конфиденциальные дела.

После утверждения номенклатуры дел возможные в течение года изменения вносятся в нее руководителем Службы делопроизводства (с проставлением подписи) на основании служебных записок руководителей структурных подразделений.

В номенклатуру включаются также: журналы (картотеки) всех видов учета и регистрации конфиденциальных документов, дела с реестрами, квитанциями и расписками на отправленные документы независимо от того, имеют ли они или не имеют отметку конфиденциальности. Кроме того, в номенклатуру включаются конфиденциальные дела, поступившие из других организаций: закрытые дела прошлых лет – в номенклатуру дел соответствующего года, незакрытые – в номенклатуру дел текущего года.

Дела, ведущиеся в течение нескольких лет (переходящие дела), вносятся в номенклатуру дел каждого года с момента их заведения до закрытия.

В номенклатуру не включаются документы, зарегистрированные по журналу инвентарного (выделенного) учета конфиденциальных документов (см. разд. 3.6).

Планируемая группировка документов в дела закрепляется в номенклатуре в заголовках дел. Заголовки должны в обобщенном виде правильно и четко отражать состав и содержание документов, подлежащих группировке в дело. Не допускаются заголовки типа

«Общая (разная) переписка», «Руководящие материалы» и им подобные, которые не раскрывают содержания дел и нередко являются причиной неправомерного ознакомления с конфиденциальными документами дела.

Заголовок может включать в себя указание вида дела («дело», «документы», «переписка») или видов документов, название автора, корреспондента, содержание документа (вопрос), время и место события. Термин «дело» употребляется в заголовках личных (персональных), судебных, следственных и арбитражных дел. Термин «документы» употребляется в заголовках в исключительных случаях, когда трудно предусмотреть конкретные виды документов, которые будут группироваться в дело, или когда таких видов много (более пяти-шести). Термин «документы» применяется также в заголовках дел, в которых объединяются документы, являющиеся приложением к другому документу, например: «Документы к плану».

Термин «переписка» применяется в заголовках дел, включающих письма-запросы и письма-ответы. Если в дело, помимо писем, планируется внести другие документы, то они должны указываться в заголовке, например: «Договоры и переписка» [295].

Вид дела или виды документов обязательно указываются в заголовке любого дела и помещаются в начале его.

Содержание документов указывается в заголовках всех дел, за исключением дел с распорядительными документами, которые подразделяются лишь по видам деятельности (например, приказы по основной деятельности, личному составу), и протоколами, которые подразделяются по принадлежности (например, протоколы совещаний у председателя правления).

Полнота и сочетание в заголовках других компонентов могут быть различными. Указывать их следует тогда, когда они несут в себе необходимую информацию и без их наличия теряются индивидуальные особенности заголовка или возникает его двоякое понимание. При этом:

- в заголовках дел с финансово-отчетной документацией указывается периодичность этой документации, например: «Годовые финансовые планы...», «Отчет о выполнении финансирования за 20... г.»;
- если в деле объединяется переписка с несколькими однородными организациями, то в заголовке указывается их обобщенное название, например: «Переписка с коммерческими банками...»;
- в конце заголовков дел с копиями распорядительных документов пишется слово «Копия».

При составлении заголовков дел необходимо предусматривать группировку:

• документов в дело по одному вопросу (за исключением распорядительных документов и протоколов);

• документов постоянного, долговременного (свыше 10 лет) и временного (до 10 лет) сроков хранения;

• с учетом распределения обязанностей между сотрудниками организации, что позволяет в значительной мере предотвращать ознакомление пользователей с документами, не имеющими к ним отношения по роду выполняемой работы;

• распорядительных документов по видам документов (приказы, указания, постановления, распоряжения, решения);

• приказов по основной деятельности, личному составу (при наличии конфиденциальных приказов) и оперативным вопросам;

• приказов по основной деятельности с подлинниками и копиями;

• документов коллегиальных органов в два дела: 1) протоколы и решения; 2) документы к заседаниям (повестка дня, доклады, справки, заключения, проекты решений и др.);

• приложений к документам вместе с документами, к которым они относятся (исключение допускается для больших по объему приложений, для которых могут предусматриваться отдельные дела);

• планов, отчетов, смет, лимитов, титульных списков и других финансово-отчетных или бухгалтерских документов отдельно от их проектов;

• документов по планированию текущего года отдельно от документов по планированию следующего года [295].

Систематизация конфиденциальных дел в номенклатуре должна производиться с учетом их важности и взаимосвязи, что ускоряет поиск документов. Дела с планами и отчетами располагаются в последовательности сроков их хранения: вслед за делами с годовыми планами (отчетами) должны вноситься дела с квартальными, а затем с месячными планами (отчетами). Дела с перепиской по одному вопросу, различающиеся между собой корреспондентским признаком, располагаются по алфавиту корреспондентов, а дела с документами, различающиеся географическим признаком, – по алфавиту населенных пунктов.

При значительном количестве дел целесообразно группировать их в номенклатуре по разделам, соответствующим наименованиям структурных подразделений или основным направлениям

(вопросам) деятельности организации. Каждому разделу присваивается номер, например: 02 – Отдел кадров или 01 – Служба делопроизводства (при структурной схеме), 14 – Финансирование (при производственно-отраслевой схеме).

Дело с номенклатурой конфиденциальных дел, конфиденциальные и открытые журналы (картотеки) регистрации и учета конфиденциальных документов, а также открытые дела с материалами на конфиденциальные документы (реестры, квитанции, расписки на отправленные документы, акты проверок наличия документов и др.) помещаются в конце номенклатуры, не имеющей деления по разделам.

При структурной схеме построения номенклатуры дел, имеющей деления на разделы, указанные документы размещаются в разделе, соответствующем названию Службы делопроизводства, а при производственно-отраслевой схеме построения – в разделе «Конфиденциальное делопроизводство».

Каждому делу присваивается самостоятельный цифровой индекс, который состоит из номера структурного подразделения (при структурной схеме построения номенклатуры) или номера направления (при производственно-отраслевой схеме) и через тире порядкового номера дела в пределах каждого раздела, например: 01–01, 01–02, 02–01 и т. д.

В номенклатуре, не имеющей деления на разделы, вместо индекса дела проставляется его порядковый номер по номенклатуре.

Номенклатура конфиденциальных дел, являющаяся одновременно учетной формой конфиденциальных дел, имеет форму 1.

Заполнение граф номенклатуры дел производится следующим образом.

При делении номенклатуры на разделы перед группой дел раздела проставляются номер и название раздела. Разделы следует начинать с нового листа или оставлять между ними свободное место для возможного внесения в течение года новых дел.

В графе 1 указываются индекс или номер дела и отметка конфиденциальности. Переходящие дела сохраняют одни и те же индексы (номера) на весь период ведения дела. Графа заполняется при составлении номенклатуры дел.

В графу 2 вносится заголовок дела. Переходящие дела сохраняют одни и те же заголовки до их закрытия. Графа заполняется при составлении номенклатуры дел. При закрытии дела заголовок может корректироваться, все изменения переносятся в номенклатуру дел.

Форма 1

Индекс (номер) дела, отметка конфиденциальности	Заголовок дела	ФИО лиц, которым предоставлено право пользования делом	№ тома	Дата		Количество листов в томе	Срок хранения и номера статей по Перечню	Архивный шифр; номер и дата акта об уничтожении; номер и дата сопроводительного документа
				заведения тома	закрытия тома			
1	2	3	4	5	6	7	8	9

В графе 3 перечисляются инициалы и фамилии всех лиц, которым предоставляется право пользования соответствующим делом. Состав лиц, допускаемых к каждому конкретному делу, должен определяться в соответствии с принципами и требованиями разрешительной системы доступа к конфиденциальной информации и регламента доступа к конфиденциальной информации (см. разд. 4.1.1) и исключать необоснованный доступ пользователей к делам. Графа заполняется при составлении номенклатуры дел. В течение года в список могут вноситься изменения.

В графах 4 и 5 арабскими цифрами проставляются номер каждого тома и дата его заведения. Графы заполняются в день подшивки первого документа тома дела (заполнения первой позиции журнала (карточки) учета и регистрации. Если дело переходящее, то в графе 5 при составлении номенклатуры указывается: «Переходящее с 20__ г.» с проставлением года заведения дела.

В графе 6 арабскими цифрами проставляется дата закрытия каждого тома. Графа заполняется в день закрытия тома. Если дело переходит на следующий год, то в графе указывается: «Переходит на 20__ г.»;

В графе 7 указывается количество листов в томе (без учета листов описи документов дела). Графа заполняется при заведении журнала учета и при закрытии тома дела, картотеки;

Графы 4–7 заполняются по каждому тому отдельной строкой. Не допускается открывать очередной том до закрытия предыдущего.

В графе 8 проставляются срок хранения и номера статей (их может быть несколько) по определенному перечню документов со сроками хранения (подробнее см. разд. 6.1). Графа заполняется при составлении номенклатуры дел. При закрытии дела и проведении экспертизы ценности имеющихся документов срок хранения и номера статей могут корректироваться. Изменения должны быть перенесены в номенклатуру дел.

В графе 9 указываются архивный шифр дела (номера фонда, описи, единицы хранения), если дело передано в архив; номер и дата акта об уничтожении дела или, если дело направлено в другую организацию, наименование организации, номер и дата сопроводительного документа (письма, реестра, расписки, квитанции). При отправлении дела во временное пользование отметка об этом проставляется карандашом. Графа заполняется после проведения соответствующих операций.

При заведении дел, не предусмотренных номенклатурой, они вносятся в соответствующий раздел номенклатуры в день заведения. Дела, поступившие из других учреждений, организаций,

предприятий, вносятся в соответствующие разделы номенклатуры с проставлением дат их фактического заведения, а для законченных дел – дат закрытия.

Если предусмотренное номенклатурой дело не было заведено, то по окончании года в графе 9 проставляется отметка: «Дело не заводилось».

5.2. Формирование конфиденциальных дел

Формирование дел включает группировку документов по делам в соответствии с номенклатурой дел и систематизацию документов внутри дел. Дела формируются в течение года по мере поступления в них документов.

Конфиденциальные дела формируются централизованно в Службе делопроизводства. Возможны случаи формирования дел в структурных подразделениях, если конфиденциальное делопроизводство в организации децентрализовано.

В дела помещаются исполненные документы (подлинники или заверенные копии), оформленные в установленном порядке. Вторые экземпляры могут помещаться в дело лишь в случаях, когда на них имеются какие-либо резолюции, пометки, дополняющие содержание основного экземпляра. При необходимости допускается помещать в дела временного (до 10 лет) хранения проекты документов. В исключительных случаях с разрешения руководителя Службы делопроизводства допускается помещать в конфиденциальные дела отдельные открытые документы, имеющие прямое отношение к содержанию конфиденциальных документов дела.

В деле группируются документы одного календарного года.

Ведение переходящих дел допускается в отдельных случаях, главным образом это дела по планированию, финансированию, проектированию, разработке научных тем.

В зависимости от вида и содержания документы систематизируются внутри дел в вопросно-логической или хронологической последовательности, а также их сочетании.

Созданные/изданные распорядительные документы (приказы, протоколы, акты) систематизируются в делах хронологически в порядке возрастания номеров. В делах с перепиской поступив-

шие (входящие) документы помещаются вместе с копиями отправленных (исходящих) документов, которыми они исполнены. Копии созданных инициативных документов, направляемых в другие учреждения, организации, предприятия, в целях обеспечения их сохранности подшиваются, как правило, в дело сразу, до получения на них ответов.

Распорядительные документы вышестоящих учреждений, организаций, появившихся в текущем году, но поступившие в начале следующего года, помещаются в дело текущего года.

Листы ознакомления с распорядительными документами и листы рассылки помещаются после этих документов, нумеруются и вносятся в описи документов дел (см. разд. 5.3) как самостоятельные.

Каждое дело должно содержать не более 250 листов. При большем количестве листов заводятся в последовательности тома дела, которые должны иметь один и тот же индекс и заголовок.

Формирование дел производится путем подшивки документов в обложки. Дела постоянного и долговременного хранения должны иметь твердые обложки. Отдельные дела могут формироваться в папках-скорошивателях или в папках-регистраторах, если это вызвано интересами обеспечения режима конфиденциальности. Пользователям такие дела не выдаются (при необходимости могут быть выданы отдельные документы дел). В каждом деле ведется опись документов, которая по окончании года или перед сдачей дела в Архив на хранение подшивается в обложку вместе с документами дела.

Если в дела подшиваются поступившие конфиденциальные документы, зарегистрированные по предшествующему или следующему году, то в журналах их учета рядом с индексом (номером) дела (графа 12 формы 2, разд. 3.2.2) в скобках проставляется год дела, в которое они помещены. В журнале (карточке) регистрации созданных/изданных конфиденциальных документов (см. разд. 3.3) индекс (номер) дела, год заведения дела проставляют в графе 7 – местонахождение документа.

Изъятие по каким-либо причинам документов из дела разрешается руководителем Службы делопроизводства, а при направлении их в другие учреждения, организации, предприятия – руководителем организации. Вместо изъятых документов в дело помещается справка-заместитель следующей формы.

СПРАВКА-ЗАМЕСТИТЕЛЬ

Документ № _____ от_____ на _____л. из дела изъят и ____

_____

(указывается новое местонахождение документа: при подшивке в другое дело – индекс дела, номера тома и листов; при отправлении – куда направлен, постоянно или временно, наименование, номер и дата сопроводительного документа; при уничтожении – номер и дата акта об уничтожении)

Основание: _____

(подпись, инициалы, фамилия лица, производившего изъятие, дата)

О документах, изъятых из дела безвозвратно, делается соответствующая отметка в описи документов дела (см. форму 2, разд. 5.3). При необходимости вместо изъятых документов в дело могут быть подшиты их копии. В этом случае справка-заместитель не требуется. Отметки о снятии копий и местонахождении подлинников производятся в соответствующих регистрационных и учетных формах.

В небольших организациях конфиденциальные документы при поступлении могут сразу же подшиваться в дело. В дальнейшем исполнитель работает с делом, а не с отдельным документом. В этом случае в опись документов, находящихся у исполнителя, включается дело в целом.

Конфиденциальные дела постоянного и временного хранения с отметкой конфиденциальности или без отметки доступа периодически просматриваются в целях возможного снятия этой отметки. Просмотр осуществляется при передаче дел из структурных подразделений в Архив организации.

Решение вопроса о снятии отметки конфиденциальности с дел возлагается на создаваемую в установленном порядке постоянно действующую Экспертную комиссию или Экспертную комиссию по защите конфиденциальной информации (см. разд. 4.1.2). В состав Экспертной комиссии входят сотрудники Службы делопроизводства и Архива организации, а также сотрудники Службы безопасности, ответственные за делопроизводство структурных подразделений организации.

Решение Экспертной комиссии оформляется в виде акта произвольной формы, который утверждается руководством организации. В акте перечисляются дела, с которых снята отметка ограничения доступа. Один экземпляр акта вместе с делами передается в Архив организации.

5.3. Оформление конфиденциальных дел

Оформление конфиденциального дела включает описание дела на обложке, проставление на внутренней стороне обложки инициалов и фамилий лиц, допущенных к делу, заведение карточки учета выдачи дела, заполнение описи документов дела, нумерацию листов, составление заверительной надписи, прошивку и опечатывание дела.

Обложка дела имеет форму 1.

Форма 1

_____
(отметка конфиденциальности)

_____
(название организации)

_____
(название структурного подразделения)

Д Е Л О №___ Т О М №___

_____
_____
_____
(заголовок дела)

«____» _____ 20___ г.
«____» _____ 20___ г.
(крайние даты документов)

На _____ листах
Хранить _____ ст. ___
Перечня документов со сроками хранения

Эти же данные проставляются в соответствии с формой на обложках журналов или (при карточном способе регистрации и учета) на отдельном листе, наклеиваемом на картотеку. Кроме того, на обложках журналов проставляется количество имеющихся в них листов.

В течение года на обложке могут проставляться: номер тома (при заведении второго тома номер проставляется на обоих томах дела, а если дело однотомное, номер тома не указывается), и новое название организации или структурного подразделения при изменении их названий или в случае получения дела из другой организации, предприятия (при этом новое название пишется ниже прежнего, а прежнее наименование берется в скобки).

При закрытии дела на обложке проставляются крайние даты документов в деле, которые должны соответствовать датам создания/издания (подписания, утверждения) или поступления само-

го раннего и самого позднего документов, вне зависимости от расположения этих документов в деле. Расхождение между датами, указанными в номенклатуре дел и на обложках дел, обусловлено тем, что даты, проставляемые в номенклатуре, диктуются режимом конфиденциальности (в случае утраты дела для обеспечения его поиска необходимо знать, когда оно было заведено или когда закрыто), а даты, проставляемые на обложке, показывают, к какому периоду относятся документы, находящиеся в деле. Эти даты ускоряют поиск необходимых документов и переносятся в опись дел, подлежащих передаче на архивное хранение. На обложке также указывается количество листов (без листов описи документов дела).

При закрытии учетной картотеки проставляется количество карточек. Кроме того, при закрытии дела уточняются заголовок и срок хранения дела с внесением состоявшихся изменений на обложку дела и в номенклатуру дел.

Перед заведением каждого конфиденциального дела любого срока хранения в него подшивается приблизительно необходимое количество листов описи документов дела (форма 2).

Данные о документах вносятся в опись в момент подшивки документов. При подшивке в конфиденциальные дела открытых документов в графах 3 или 4 производится отметка «н/к» – неконфиденциальный. Если в дело подшивается документ, имеющий приложения, в том числе открытые, то запись в графах 3 или 4 производится одной позицией за номером основного документа без отметок о наличии приложений, с проставлением в графе 6 номеров общего количества листов, включая листы приложений. Если документ внутренний, то в графе 5 указывается только его краткое содержание. В описи документов дел временного хранения при небольшом объеме справочной работы по документам графа 5 может не заполняться.

При заведении дела на внутреннюю сторону обложки дела переносятся из номенклатуры инициалы и фамилии лиц, которым предоставлено право пользования делом. Список заверяется подписью сотрудника Службы делопроизводства. Это позволяет при определении правомерности выдачи дела пользователю не обращаться к номенклатуре дел. Одновременно заводится карточка учета выдачи дела (форма 3).

Графа 2 необходима потому, что в процессе формирования дела меняется количество его листов.

Форма 2

ОПИСЬ ДОКУМЕНТОВ
ДЕЛА № ____ ТОМ № _____
за 20___ г.

№ п/п	Дата документа	Номер и отметка конфиден-циальности поступившего документа	Номер и отметка конфиден-циальности созданного/ изданного документа	Откуда поступил или куда адресован документ	№ листа дел	Отметка о местонахождении изъятого из дела документа
1	2	3	4	5	6	7

Форма 3

КАРТОЧКА УЧЕТА ВЫДАЧИ ДЕЛА

_____
(индекс (номер) и гриф конфиденциальности дела, номер тома, заголовок дела)

Дата выдачи	Количество листов	Кому выдано	Подпись за получение	Подпись за возврат
1	2	3	4	5

Карточка помещается в бумажный карман, приклеенный к внутренней стороне обложки дела. По заполнении одной карточки заводится следующая, а заполненная вносится в опись документов дела после последней записи. Карточки не нумеруются и листами дела не считаются. Карточки, заводимые после закрытия дела, также вносятся в опись документов дела. Необходимость сохранения всех карточек вызвана тем, что в случае разглашения конфиденциальной информации, содержащейся в документах дела, по карточкам можно установить, кто пользовался делом, и тем самым определить круг лиц, которые могли разгласить информацию.

Листы дела нумеруются (за исключением листа с заверительной надписью). Листы описи документов дела нумеруются отдельно при начале заполнения каждого листа, оставшиеся чистые листы не нумеруются. Листы дела нумеруются при подшивке документа арабскими цифрами черным графическим карандашом или нумератором в правом верхнем углу листа без затрагивания текста документа. Если дело имеет несколько томов, нумерация листов производится по каждому тому отдельно.

Лист любого формата, подшитый за один край, нумеруется как один лист, сложенный и подшитый за середину – как два листа. Другие документы (вырезки, вставки текста, переводы и т. д.), подклеенные к листу одним краем, нумеруются отдельно вслед за листом основного документа. Лист с наглухо наклеенными документами и фотографиями нумеруется как один, в этом случае наклеенные документы оговариваются в заверительной надписи.

Фотографии и другие иллюстрированные документы, подшитые в дело как самостоятельные листы, нумеруются при наличии свободного поля на лицевой стороне в правом верхнем углу, при отсутствии – на оборотной стороне в левом верхнем углу.

Конверты с надписями или вложениями, подшитые в дело, также нумеруются, при этом каждое вложение нумеруется очередным номером вслед за конвертом. На лицевой стороне конверта пишется опись вложенных документов с указанием их регистрационных номеров, краткого названия и номеров листов дела.

При изъятии документов из дел старая нумерация листов сохраняется. При нумерации листов необходимо строго следить за ее правильностью. Однако если все же лист не был занумерован или один номер повторен на нескольких листах, то разрешается проставлять литерные номера, например 12, 12а, 12б и т.д., которые оговариваются в заверительной надписи.

При закрытии дела на отдельном чистом листе составляется заверительная надпись по следующей форме.

ЗАВЕРИТЕЛЬНАЯ НАДПИСЬ ДЕЛА № _____Т. № _____

В деле подшито и опечатано печатью № _____ _____ листов
(прописью) (цифрами)

+ _____ листов описи документов дела.
(цифрами)

Листы № № _____литерные.
(цифрами)

На листах № № _____ наклеено_____документов (фотоотпечатков)
(цифрами) (прописью)

за уч. № № _____ .
(цифрами)

_____
(подпись, инициалы, фамилия лица, оформившего заверительную подпись, дата)

При незаполнении каких-либо позиций заверительной надписи в них делается прочерк. Незаполненные листы описи документов дела не учитываются.

Листы каждого тома дела при закрытии тома проверяются, прошиваются плотной ниткой в четыре прокола и опечатываются или пломбируются таким образом, чтобы захватывались оба конца нити прошивки. Дела могут переплетаться, в этом случае их опечатывание не производится.

Следующим этапом конфиденциального документооборота является этап подготовки конфиденциальных документов и дел к архивному хранению или уничтожению.

ГЛАВА 6

ПОДГОТОВКА КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ ДЛЯ АРХИВНОГО ХРАНЕНИЯ И УНИЧТОЖЕНИЯ

6.1. Экспертиза ценности конфиденциальных документов

Согласно Федеральному закону «Об архивном деле в Российской федерации» [27], Архивный фонд Российской Федерации разделен на две составные части: государственную и негосударственную. К государственной части отнесены документы государственных и муниципальных органов власти и подведомственных им организаций и предприятий, а также документы предприятий смешанных форм собственности, в уставном капитале которых имеется преобладающая доля государственной собственности. Негосударственную часть составляют документы, находящиеся в собственности общественных и религиозных объединений и организаций или в частной собственности негосударственных объединений, организаций и физических лиц и представляющие собой историческую, научную, социальную, экономическую, политическую или культурную ценность.

Государственные и муниципальные органы власти и подведомственные им организации обязаны в установленном государственными нормативными актами порядке и в установленные сроки передавать документы постоянного хранения в государственные архивы.

Негосударственные организации, включая коммерческие, обладают правом собственности на созданные в процессе их деятельности документы, отнесенные к негосударственной части Архивного фонда, и могут передавать документы постоянного хранения в государственные архивы на основе соглашения (договора), оговаривая при необходимости особые условия хранения передаваемых документов и пользования ими.

Состав государственных и муниципальных органов власти и подведомственных им организаций, предприятий, передающих документы постоянного хранения в государственные архивы,

а также категории передаваемых ими документов (все документы постоянного хранения или часть из них) определяются Федеральным архивным агентством России (Росархивом) и органами управления архивным делом субъектов Российской Федерации. В отношении негосударственных организаций такое определение производится органами и учреждениями Росархива совместно с собственниками документов и оформляется договором*.

Таким образом, применительно к конфиденциальным документам источниками комплектования Архивного фонда Российской Федерации могут быть негосударственные организации, а также государственные и муниципальные органы власти и их организации, в деятельности которых образуются документы с информацией, составляющей служебную, коммерческую, профессиональную тайны, секреты производства (ноу-хау), служебные секреты производства, персональные данные работников в соответствии с Трудовым кодексом Российской Федерации [8], персональные данные государственных служащих [30; 61] (см. разд. 1.2–1.7).

Конфиденциальные документы государственных и негосударственных структур, источников комплектования Архивного фонда, могут передаваться в государственные архивы с согласия их обладателей, но на практике такая передача осуществляется в исключительных случаях, обычно при ликвидации организаций, предприятий с отсутствием правопреемника. Если таких ситуаций не возникает, то документы передаются в государственные архивы, как правило, только после снятия с них отметки конфиденциальности, т. е. после того, как они перестают быть носителями конфиденциальной информации.

Конфиденциальные документы, подлежащие передаче в государственные архивы, до их фактической передачи должны храниться соответствующим образом в Архиве организации, а при отсутствии Архива – в Службе делопроизводства. В некоторых случаях Архив может входить в состав Службы делопроизводства как структурное подразделение.

В таком же порядке необходимо хранить документы постоянного и при наличии долговременного (свыше 10 лет) хранения, не подлежащие передаче в государственные архивы. При этом должны быть обеспечены условия для физической сохранности документов и предотвращения утечки содержащейся в них информации.

---

* Отбор на государственное хранение документов, образующихся в деятельности организаций и предприятий нового типа: аналит. обзор – М.: ВНИИДАД, 1994. – 21 с. – Деп. в ОЦНТИ по документоведению и архивному делу 24.05.1994 № 118.

В целях уточнения или определения сроков хранения документов и отбора их на основе этих сроков для архивного хранения и уничтожения проводится экспертиза ценности документов. Проведение такой экспертизы целесообразно возлагать на постоянно действующую Экспертную комиссию организации.

Экспертиза ценности конфиденциальных документов проводится ежегодно или при небольшом объеме документов один раз в несколько лет, однако подвергать экспертизе целесообразно документы, изданные 3–5 лет назад, когда одновременно с подготовкой документов для архивного хранения возможны отбор их для уничтожения (значительное количество документов имеет срок хранения 3–5 лет) и снятие отметки конфиденциальности с существенной части документов [315].

Экспертизой ценности должны быть охвачены все конфиденциальные дела и документы инвентарного (выделенного) хранения за соответствующий период времени, поскольку последние являются составной частью документального фонда организации (см. разд. 3.6). К проведению экспертизы ценности конкретного дела (документа выделенного хранения) привлекаются члены постоянно действующей Экспертной комиссии, имеющие доступ к этому делу (документу).

Экспертиза ценности документов дела проводится путем изучения содержания каждого подшитого в дело вида документа и установления его соответствия сроку хранения и номерам статей Перечня документов со сроками хранения, указанными на обложке дела (см. разд. 5.3) . Одновременно проверяется правильность формирования дела: соответствие видов и содержания документов заголовку дела, отсутствие в делах постоянного срока хранения документов временного срока хранения, а также определяется возможность снятия отметки конфиденциальности с отдельных документов или с дела в целом.

Нормативным актом, регламентирующим хранение и отбор на хранение, а также уничтожение типовых документов, служит Перечень типовых управленческих документов с указанием сроков хранения [291].

Таким образом, перечни служат целям охраны, организации и качественного пополнения состава Архивного фонда Российской Федерации.

В Перечень входят современные типовые документы, образующиеся при документировании общих для всех учреждений, организаций и предприятий функций управления, с указанием сроков

хранения документов. Перечень является нормативным пособием при определении сроков хранения и отборе документов на хранение и уничтожение и должен быть использован при подготовке других пособий и перечней (отраслевых, ведомственных) по экспертизе ценности документов и комплектованию архивов [294].

При проведении экспертизы ценности научно-технических документов, содержащих информацию о секретах производства (ноу-хау), служебную и коммерческую тайны, необходимо использовать Перечень типовых архивных документов, образующихся в научно-технической деятельности организаций, с указанием сроков хранения [290], а также методические рекомендации по экспертизе ценности [97].

В соответствии с Федеральным законом «Об архивном деле в Российской Федерации», с учетом положений нормативно-правовых актов, регламентирующих создание, состав и образование документов на различных носителях информации о научной, научно-технической, производственно-технической, проектной и строительной деятельности, Всероссийским научно-исследовательским институтом документоведения и архивного дела (ВНИИДАД) разработан Единый классификатор документной информации Архивного фонда Российской Федерации и Методические рекомендации по его внедрению [333].

Если в организации имеются документы, не предусмотренные названными перечнями и методическими рекомендациями, то срок их хранения следует определять на основе критериев оценки документов, к важнейшим из которых относятся:

- содержание документа (значимость отображенного события, полнота его освещения, новизна, уникальность информации или ее повторяемость, целевое назначение документа);
- происхождение документа (место и время издания);
- внешние особенности документа (подлинник или копия, характер резолюций, наличие пометок, физическое состояние).

Срок хранения дела в целом устанавливается по наивысшему сроку хранения документов, находящихся в деле.

Экспертиза ценности документа выделенного хранения проводится путем изучения содержания документа и определения срока его хранения на основе Перечней документов с указанием этих сроков или критериев установления ценности документов.

Результаты экспертизы ценности документов целесообразно фиксировать в рабочей карточке (тетради) эксперта с отражением в ней номера дела (документа выделенного хранения), его заголов-

ка, операций (с обоснованиями), которые необходимо произвести: какие документы и в какое дело перешить, какие уничтожить, с каких можно снять отметку конфиденциальности, какими должны быть уточненные заголовок, срок хранения и номера статей по перечням.

По завершении экспертизы всех дел и документов инвентарного (выделенного) хранения (см. разд. 3.6) результаты работы всех экспертов рассматриваются на заседании постоянно действующей Экспертной комиссии и фиксируются в протоколе с отражением следующей информации:

- какие дела и документы выделенного хранения (с уточненными заголовками, отметками конфиденциальности, сроками хранения и номерами статей по Перечню) подлежат передаче на архивное хранение (раздельно – постоянное и долговременное (свыше 10 лет));
- какие документы, из каких дел и в какие дела необходимо перешить;
- какие дела, документы из дел и документы выделенного хранения подлежат уничтожению;
- с каких дел, документов выделенного хранения или отдельных документов, подшитых в дела, должна быть снята отметка о конфиденциальности (в последнем случае должно быть указано, подлежит ли документ, с которого снимается отметка конфиденциальности, изъятию из дела или должен оставаться в нем).

Протокол заседания подписывается председателем и всеми членами постоянно действующей Экспертной комиссии и утверждается руководителем организации.

6.2. Подготовка конфиденциальных документов и дел для архивного хранения

Согласно протоколу заседания Экспертной комиссии сотрудниками Службы делопроизводства производится частичное переформирование и дооформление соответствующих дел и документов, в том числе:

- изъятие из дел документов, подлежащих перешивке в другие дела, и подшивка их в эти дела с проставлением в описях документов дел, из которых изъяты документы, их нового местонахождения и помещением в дела справок-заместителей, а также с перенуме-

рацией листов, перешитых документов в делах, в которые они помещены, внесением их в описи документов дел и исправлением количества листов в заверительной надписи дел, на обложках дел и в номенклатуре дел;

• изъятие из дел документов, подлежащих уничтожению;

• зачеркивание отметки конфиденциальности с проставлением даты и номера протокола заседания Экспертной комиссии, подписи на документах, подшитых в дела, обложках дел и документов, подлежащих снятию ограничения доступа (в описях документов дела, номенклатуре дел и журнале учета документов выделенного хранения отметка конфиденциальности зачеркивается без ссылки на протокол заседания Экспертной комиссии);

• изъятие из дел (по решению Экспертной комиссии) документов, с которых снята отметка конфиденциальности с отметкой в описях документов дел и помещением в дела справок-заместителей (см. разд. 5.2);

• передача снятых с ограничения доступа дел и документов выделенного хранения по акту в Службу делопроизводства с отметкой в графе 9 номенклатуры дел (см. разд. 5.1.2, форма 1);

• корректировка заголовков, сроков хранения и номеров статей по перечням отраслевых, ведомственных документов со сроками хранения, на обложках дел и в номенклатуре дел;

• проставление сроков хранения и номеров статей Перечня на обложках дел.

Если срок хранения дел и документов установлен не Перечнем, а постоянно действующей Экспертной комиссией, то вместо статей Перечня проставляется отметка ЭК.

После изъятия из дел документов листы дела не перенумеровываются. На обложках дел и в номенклатуре дел рядом с количеством проставленных листов в скобках указывается количество листов, оставшихся в деле. В заверительной надписи дела под прежней надписью пишется:

«_____ листов изъято согласно записям в описи дела»
(прописью)

с проставлением подписи, фамилии и инициалов лица, произведшего запись, и даты.

На дела и документы инвентарного (выделенного) хранения, которые отобраны для постоянного хранения, составляется опись по следующей форме 1.

Форма 1

УТВЕРЖДАЮ

Наименование должности
руководителя организации

_____
(подпись, расшифровка подписи)

Дата _____

ФОНД № _____
ОПИСЬ № _____
конфиденциальных дел _____
и документов инвентарного (выделенного)
хранения за _____год

№ п/п	Индекс (номер) дела или номер документа и отметка конфиденциальности	Заголовок дела или документа	Количество листов	Примечание
1	2	3	4	5

В данную опись внесено _____дел и документов
(цифрами и прописью)
№ _____ по № _____ , в том числе:
литерные номера: _____
пропущенные номера: _____

Наименование должности
сотрудника, составившего опись _____
(подпись, расшифровка подписи)

Дата _____
Одобрено _____
Протокол ЭК _____
от _____ № _____

Включенные в настоящую опись дела и документы принял:
Наименование должности
сотрудника Архива организации_____
(подпись, расшифровка подписи)

Дата_____

На дела и документы долговременного хранения (свыше 10 лет) составляется аналогичная опись с добавлением перед графой «Примечание» графы «Срок хранения и номера статей по Перечню».

На научно-техническую, проектную, конструкторскую и иную специальную документацию составляются отдельные описи документов. При составлении описей необходимо иметь в виду следующее:

- каждой из описей присваивается отметка конфиденциальности;
- если дела и документы подлежат передаче в государственный архив, то номер фонда устанавливает государственный архив; если не подлежат, то фонду присваивается номер 1;
- опись во всех случаях имеет номер 1 с добавлением прописных букв: П (постоянного), В (временного) сроков хранения, Т (техническая документация). Кроме того, к номеру и букве добавляется аббревиатура отметки конфиденциальности;
- если при составлении первой описи в нее включаются дела и документы с начала деятельности организации, то эти дела и документы могут вноситься за несколько лет с разделением по годам, но с валовой порядковой нумерацией, начиная с номера 1.

В последующем составляются годовые разделы описей или описи, включающие документы за несколько лет при небольшом их объеме. При этом продолжается порядковая нумерация дел и документов, внесенных в предыдущие описи, например первая опись дел и документов за 2001–2005 гг. имеет порядковые номера 1–125 за 2001 г., 126–150 за 2002 г. и т.д. Порядковая нумерация дел является учетным архивным номером (единицей хранения) дела (документа).

В опись за соответствующий год вносятся сначала дела, потом документы инвентарного хранения (дела располагаются в последовательности, предусмотренной номенклатурой дел) и документы выделенного хранения (в последовательности учетных номеров).

В графе 2 описи отметка конфиденциальности проставляется аббревиатурой, например «Строго конфиденциально» – СКФД, «Конфиденциально» – КФД, «Для служебного пользования» – ДСП [209].

Если дело состоит из нескольких томов, то каждый том вносится в опись под самостоятельным порядковым номером, при этом заголовок первого тома пишется полностью. Вместо заголовков остальных томов в этой графе пишется: «То же, т. ___» с проставлением номера тома (на каждом новом листе описи, если он начинается с записи второго или последующих томов, заголовок воспроизводится полностью).

Переходящие дела включаются в раздел описи по году их заведения, в последующие разделы описи вносятся индексы и заголовки этих дел, но без присвоения порядкового номера, а в графе «Примечание» делается отметка: «см. ед. хр. № ___» с проставлением порядкового номера, присвоенного делу при его включении в опись.

В графе 4 указывается фактическое количество листов дела, оставшееся в нем после изъятия документов (если такие изъятия осуществлялись).

На дела и документы инвентарного (выделенного) хранения, подлежащие передаче в государственный архив, описи составляются в четырех экземплярах. Эти описи дополнительно утверждаются протоколом экспертно-проверочной комиссии государственного архива. На дела и документы, не подлежащие передаче в государственный архив, описи составляются в двух экземплярах, если дела и документы передаются в Архив организации, или в одном экземпляре, если не передаются.

При передаче дел и документов в государственный архив или Архив организации в Службе делопроизводства остается один экземпляр описи с подписью сотрудника Архива за получение включенных в опись дел и документов, остальные экземпляры передаются в Архив.

На обложке дел и документов инвентарного (выделенного) хранения проставляются номера фонда, описи и единицы хранения.

В номенклатуре дел в графе 9 (см. разд. 5.1.2, форма 1) проставляется архивный шифр включенных в опись дел: номер фонда, описи, единицы хранения (порядкового номера по описи), в журнале (карточке) учета документов инвентарного (выделенного) хранения в графе 14 – номер экземпляра, а в графе 15 – архивный шифр документа (см. разд. 3.6).

6.3. Подготовка конфиденциальных документов и дел к уничтожению

В течение делопроизводственного года в организации создается большое количество документов, в том числе конфиденциальных. Часть их подлежит передаче на государственное хранение как документов, имеющих научную, историческую, экономическую и иную ценность (об особенностях доступа к архивным конфиденциальным документам см. в разд. 4.5). Остальные документы хранятся

в Архиве организации и по истечении установленного срока могут быть уничтожены. Суть этой процедуры заключается в выявлении в процессе экспертизы научной и практической ценности документов с истекшими сроками хранения, утративших практическое, научное или общественное значение, и отборе их к уничтожению. Отбор документов и дел к уничтожению оформляется актом. Форма акта представлена в «Основных правилах работы архивов организаций» [287].

После утверждения описей дел и конфиденциальных документов постоянного срока хранения составляется акт по тем делам и конфиденциальным документам за соответствующий период, которые подлежат уничтожению. В акт включаются дела, отдельные документы из дел и документы инвентарного (выделенного) хранения, отобранные Экспертной комиссией. Акт имеет форму 2.

Приведенная ниже форма 3 может быть применена в тех организациях, которые не сдают документы на государственное хранение, или если уничтожаемые документы имеют специфическую особенность (испорченные трудовые книжки, бланки дипломов). В нашем случае специфическую особенность имеют конфиденциальные документы.

В акт на уничтожение документов, не подлежащих хранению, в любой последовательности вносятся заголовки отдельных дел или групповые заголовки с указанием количества дел, включенных в группу.

Сроки хранения дел исчисляются с первого дня года, следующего за делопроизводственным годом. Например, в 2009 г. можно выделить подлежащие уничтожению дела с истекшими сроками хранения:

- трехгодичным – законченные в 2005 г.;
- пятилетним – законченные делопроизводством в 2003 г.;
- десятилетним – законченные делопроизводством в 1998 г.

Пример составления акта в соответствии с требованиями ГОСТ Р 6.30–2003 [151].

В конце акта может быть сделана и такая пометка: «Документы уничтожены путем механического измельчения» или «Документы уничтожены путем сожжения».

Если в акте указаны дела нескольких структурных подразделений, то название каждого указывается перед группой заголовков дел. Если в акт включены конфиденциальные документы, акт содержит дополнительную запись (например, форма 4).

Форма 2

УТВЕРЖДАЮ

Наименование должности
руководителя организации

_____
(подпись, расшифровка подписи)
Дата _____

АКТ №
о выделении к уничтожению дел и документов, не подлежащих хранению

На основании _____
(название и выходные данные перечня документов с указанием сроков их хранения)

отобраны к уничтожению как не имеющие научно-исторической ценности и утратившие практическое значение документы фонда № _____
(название фонда)

№ п/п	Заголовок дела или групповой заголовок дел	Даты дела или крайние даты дела	Номера описей (номенклатур) за годы	Индекс дела (тома, части) по номенклатуре или номер дела по описи	Количество дел (томов, частей)	Сроки хранения дела и номера статей по Перечню	Примечание
1	2	3	4	5	6	7	8

Итого _____ дел за _____ годы.

(цифрами, прописью)

Всего подлежит уничтожению _____ документов и дел.

Описи дел постоянного хранения за _____ годы утверждены, а по личному составу согласованы с ЭПК _____

(наименование архивного учреждения)

(Протокол от _____№ _____)

Наименование должности лица,
проводившего экспертизу ценности документов _____

(Подпись, расшифровка подписи)

Дата_____

СОГЛАСОВАНО
Протокол ЦЭК (ЭК) от _____№ _____

Документы в количестве _____ дел, весом _____ кг.
сданы в _____ на переработку
по приемо-сдаточной накладной от _____ № _____.
Наименование должности работника Архива (Службы делопроизводства),
внесшего изменения в учетные документы _____

Дата _____

Записи в таблицу производятся следующим образом.

1	Графики предоставления отпусков	1998–2002 гг.	Номенклатуры 1998–2002 гг.	03-13	1	1 год, ст. 356
2	Приказы о командировках	1997 г.	Номенклатура 1997 г.	03-05	1	5 лет, ст. 66
3	Переписка о физической защите банкоматов	1998 г.	Номенклатура 1998 г.	01-03 КФД	1	3 года, ст. 48
4	Переписка о заключении договора	2003 г.	Номенклатура 2003 г.	07-05 КТ	1	3 года, ст. 19
5	Инструкция о порядке кредитования	2005 г.	Номенклатура 2005 г.	1-03 СКФД	1	До замены новой

Форма 3

УТВЕРЖДАЮ

АКТ_____ № ____Наименование организации_____

Место составления _____Наименование должности руководителя_____

О выделении к уничтожению документов и дел организации_____

(подпись, расшифровка подписи)

Дата _____

Основание: наименование распорядительного документа _____ № _____

Составлен экспертной комиссией

Председатель _____

(должность, инициалы, фамилия)

Члены комиссии: 1. _____

(должность, инициалы, фамилия)

2._____

(должность, инициалы, фамилия)

Присутствовали: _____

(должность, инициалы, фамилия)

Комиссия, руководствуясь Перечнем (название перечня), отобрала к уничтожению как не имеющие научно-исторической ценности и утратившие практическое значение следующие документы и дела, сформировавшиеся в деятельности организации (наименование организации).

№ п/п	Годы документов и дел	Заголовки документов и дел (групповые или индивидуальные), индекс дел по номенклатуре, описи	Количество документов и дел (томов)	Номера статей по Перечню	Примечание
1	2	3	4	5	6

Итого дел _____
(цифрами и прописью)

Председатель _____
(подпись, расшифровка подписи)

Члены комиссии: 1. _____
(подпись, расшифровка подписи)

2._____
(подпись, расшифровка подписи)

Документы измельчены и сданы для уничтожения конторе по заготовке вторичного сырья по приемо-сдаточной накладной № _____ от _____.

Председатель ЭК _____
(подпись, расшифровка подписи)

Дата _____

Форма 4

№ п/п	Заголовок дела или групповой заголовок дел	Дата дела или крайние даты дела	Номера описей (номенклатур за год (ы))	Индекс дела (тома, части) по номенклатуре или номер описи	Количество томов, частей	Сроки хранения дела (тома, части) и номера статей по Перечню	Примечание
1	2	3	4	5	6	7	8

01-Служба делопроизводства

Включенные в акт дела и документы сверены с записями в протоколе ЭК, акте и учетных формах

_____

(подпись, инициалы, фамилия, дата)

Дела и документы полностью уничтожены путем _____

_____

(подпись, инициалы, фамилия, дата)

Отметки об уничтожении дел и документов в номенклатуре дел, журнале (карточках) учета документов инвентарного (выделенного) хранения и в описях документов дел произведены.

_____

(подпись, инициалы, фамилия, дата)

Лишние экземпляры (копии) документов инвентарного (выделенного) хранения, журналы (картотеки) учета конфиденциальных носителей, созданных/изданных документов, поступивших пакетов и документов могут включаться в данный акт или уничтожаться без рассмотрения Экспертной комиссией по мере истечения сроков хранения по акту аналогичной формы (с исключением данных, относящихся к делам) без ссылки на протокол этой комиссии и без подписи ее председателя.

Данные каждого дела, документа, журнала (картотеки) регистрации и учета вносятся в акт отдельной позицией и должны соответствовать зафиксированным в протоколе Экспертной комиссии и регистрационно-учетных формах. Если дело состоит из нескольких томов, то каждый из них включается в акт отдельной позицией, а в графе 3 вместо заголовков второго и последующих томов пишется: «То же, т.___», с добавлением номера тома. При внесении в акт дел, из которых перед уничтожением были изъяты отдельные документы, в графе 6 указывается количество листов, фактически оставшихся в деле.

Перед уничтожением включенных в акт дел, документов и журналов (картотек) учета проверяется соответствие данных акта записям, сделанным:

- в протоколе постоянно действующей Экспертной комиссии;
- в номенклатуре дел;
- в журнале учета документов инвентарного (выделенного) хранения;
- на обложках и заверительных листах дел и документов инвентарного (выделенного) хранения;
- в описях документов дела (по документам, изъятым из дела).

Листы и учетные карточки просчитываются, сложенные документы разворачиваются. Соответствие данных заверяется в акте подписями проверявших.

Дела, документы и журналы (картотеки) учета уничтожаются путем сжигания или с помощью бумагорезательной машины. При уничтожении документов вне территории организации доставка их к месту уничтожения производится на служебном транспорте, при этом должны быть приняты меры, исключающие доступ к документам посторонних лиц.

После уничтожения делаются отметки об уничтожении дел и регистрационно-учетных журналов (картотек) в графе 9 номенклатуры дел, документов инвентарного (выделенного) хранения и в графах 12 и 13 журнала учета документов инвентарного хранения. Отметки об уничтожении отдельных документов из дел проставляются в опи-

сях документов дел. Вместо уничтоженных документов в дела помещаются справки-заместители. В акте проставление таких отметок подтверждается подписью сотрудника, делавшего отметки.

Составление акта о выделении дел и документов, подлежащих уничтожению, и проставление в учетных формах отметок об их уничтожении осуществляются сотрудником Службы делопроизводства. В проверке правильности включения в акт дел и документов и их физического уничтожения, кроме этого сотрудника, должен участвовать второй сотрудник Службы делопроизводства или другого подразделения организации, имеющий доступ к уничтожаемым делам и документам.

В акт о выделении дел, подлежащих уничтожению, вносятся документы только с истекшими сроками хранения. Одновременно за тот же период составляются годовые разделы сводных описей дел по личному составу (приказы, списки личного состава, карточки учета и личные дела уволенных рабочих и служащих, лицевые счета или расчетные ведомости по зарплате, невостребованные трудовые книжки и другие личные документы, акты о несчастных случаях) и дел долговременного хранения (свыше 10 лет), а также целесообразно включение в опись и дел со сроком хранения 10 лет.

Акты рассматриваются и одобряются Экспертной комиссией организации (структурного подразделения), подписываются должностным лицом, проводившим экспертизу, и утверждаются руководством. Экспертные комиссии – это совещательные органы, создаваемые приказом руководителя организации в составе не менее трех-пяти человек под председательством одного из руководящих работников. В состав комиссии могут входить: заместитель руководителя, главный бухгалтер, начальник отдела кадров, главный специалист и секретарь. Члены комиссии помогают персоналу Службы делопроизводства в подготовке дел к последующему хранению и уничтожению.

По утвержденным актам вносятся изменения в учетные документы архива (опись дела, номенклатура дел), а выделенные к уничтожению документы в упакованном виде передаются на утилизацию бумагоперерабатывающим фабрикам. Оформляется это приемосдаточными накладными, данные которых (дата сдачи, номер накладной, вес сданной макулатуры) указываются в акте о выделении к уничтожению документов.

У отдельных категорий документов есть своя специфика уничтожения. Так, бухгалтерские документы не могут быть уничтожены до проведения ревизии по ним. Факт уничтожения черновика конфиденциального документа и других материалов данной группы подтверждается пометкой на копии документа, оставшейся в деле Службы делопроизводства: «Черновик уничтожен. Дата. Подпись» (см. разд. 2.4 и 2.5).

ГЛАВА 7

РЕЖИМ КОНФИДЕНЦИАЛЬНОСТИ ДОКУМЕНТИРОВАННОЙ ИНФОРМАЦИИ

7.1. Режим обмена конфиденциальной документированной информацией

В каждой организации должен быть установлен строгий порядок обмена конфиденциальной документированной информацией, который является составной частью внутриобъектового режима и направлен на обеспечение сохранности конфиденциальных документов и предотвращение утечки содержащейся в них информации.

Передача конфиденциальных документов возможна только сотрудникам, имеющим санкционированный доступ к этим документам, под роспись в регистрационно-учетных формах или с отметкой сотрудником Службы делопроизводства в электронных формах, если в организации существует интегрированная АИС делопроизводства.

Если сотрудники работают с конфиденциальными документами в своих служебных кабинетах, то документы (кроме дел) разрешается выдавать им как на один рабочий день, так и на все время, необходимое для работы с ними. В последних случаях, помимо сейфа и номерной печати, сотруднику выдаются под подпись в лицевом счете специальный портфель (кейс), имеющий устройство для опечатывания, и типовая форма: «Опись конфиденциальных документов, находящихся у исполнителя». В опись сотрудник должен вносить каждый документ в момент его получения и вычеркивать его после исполнения и передачи в Службу делопроизводства. Опись составляется по форме 1.

Форма 1

№ п/п	Номер и отметка конфиденциальности				Количество листов
	созданного (изданного) документа	поступившего документа	инвентарного (выделенного) хранения	носителя	
1	2	3	4	5	6

Опись предназначена для проведения самоконтроля за наличием конфиденциальных документов. С этой целью сотрудник должен перед сдачей документов в конце каждого рабочего дня в Службу делопроизводства проверить наличие находящихся у него конфиденциальных документов и бумажных носителей, необходимых при документировании конфиденциальной информации (см. разд. 2.4.), и их соответствие описи. В случае отсутствия каких-либо документов или части их об этом немедленно ставится в известность Служба делопроизводства и организуется их поиск. После проверки конфиденциальные документы вместе с описью помещаются в портфель, который опечатывается личной печатью сотрудника и передается в Службу делопроизводства. Не допускается хранить в спецпортфеле открытые документы, если они не являются приложением к конфиденциальным документам.

Сдача портфеля и его последующее получение производятся в обмен на специально заготовленную расписку (жетон), удостоверение или пропуск сотрудника. При наличии большого числа сотрудников, работающих с конфиденциальными документами, на специальную расписку может наклеиваться фотокарточка сотрудника. При приеме-передаче спецпортфеля должны быть проверены соответствие номера и четкость оттиска печати.

Должностные лица, которым разрешено в нерабочее время хранить конфиденциальные документы в личных сейфах, при условии подключения их к охранной сигнализации, по окончании рабочего дня помещают документы в сейф, опечатывают его и сдают под охрану по специальному журналу, ведущемуся Службой охраны.

По завершении работы с конфиденциальными документами сотрудники обязаны своевременно возвращать их в Службу делопроизводства.

К рабочему месту сотрудника организации предъявляют определенные требования.

Рабочее место сотрудника должно быть размещено таким образом, чтобы исключить возможность обозрения находящихся на столе документов лицами, не имеющими к ним отношения. Рабочий стол не должен просматриваться через окно из соседних домов. Помещения, в которых конфиденциальная документированная информация обрабатывается на компьютерах, должны иметь защиту от технических средств разведки и шпионажа. Особенности создания и изготовления конфиденциальных документов при помощи средств вычислительной техники, печатания, копирования, тиражирования более подробно рассмотрены в разд. 2.6.

На рабочем столе всегда должны находиться только тот конфиденциальный документ и материалы к нему, с которыми в данный момент работает сотрудник. Другие документы следует хранить в запертом сейфе. Руководители и исполнители не должны вести какие-либо картотеки для организации работы с конфиденциальными документами и контроля за их исполнением. Очередность исполнения определяется раскладкой документов по рабочим папкам: «Ознакомление», «Согласование», «Срочно», «Задания на такое-то число» и т.д. Не рекомендуется хранить документы в ящиках рабочего стола, в шкафах и других широкодоступных местах, даже если они имеют замки и запоры.

Если на рабочем месте руководителя или исполнителя отсутствуют необходимые условия для работы с конфиденциальными документами, то ознакомление с документами и их исполнение осуществляются в специальном помещении Службы делопроизводства.

Вся конфиденциальная документированная информация, бумажные, машинные носители информации (дискеты, флэш-память), дела и другие материалы, полученные руководителем или исполнителем на срок более одного дня, вносятся Службой делопроизводства в опись конфиденциальных документов, находящихся у исполнителя (форма 1). Электронный экземпляр описи находится в Службе делопроизводства, а его распечатка на бумажном носителе передается исполнителю. Документы, полученные на время рабочего дня, в опись не вносятся. За полученный документ исполнитель расписывается в карточке учета. При возврате документа сотрудник Службы делопроизводства расписывается и в карточке, и в описи или делает соответствующую отметку в электронной форме.

Выданные для работы дела с отметкой о конфиденциальности подлежат возврату в Службу делопроизводства или ответственному за делопроизводство структурного подразделения, в зависимости от места хранения документа, в тот же день. Запрещается выносить документы и дела из служебных помещений для работы с ними на дому, в гостиницах и др. В необходимых случаях руководство Службы делопроизводства и руководство структурного подразделения могут разрешить исполнителям вынос из здания указанных материалов для их согласования, подписи и т.д. в организациях, находящихся в пределах населенного пункта организации.

Сотрудникам, работающим с конфиденциальной документированной информацией, запрещается (это должно быть отражено в разделе Инструкции по делопроизводству либо Инструкции по конфиденциальному делопроизводству):

• использовать конфиденциальные сведения в публикациях, открытых документах, докладах и переписке, рекламных материалах, выставочных проспектах и информационных сообщениях;

• передавать кому-либо, в том числе работникам организации, устно или письменно конфиденциальную информацию, документы, если это не связано со служебной необходимостью и не разрешено непосредственным руководителем;

• вести переговоры, содержащие конфиденциальные данные, по незащищенным линиям связи, в неприспособленных помещениях, в присутствии посторонних лиц;

• снимать копии с документов и делать из них выписки без письменного разрешения непосредственного руководителя;

• знакомиться с конфиденциальными документами, делами и базами данных других сотрудников, работать за их компьютерами;

• переписывать сведения из документов в личные записные книжки, дневники, календари, карточки учета работы;

• вносить в помещения организации личные фото-, видеокамеры, компьютеры (ноутбуки), аудиотехнику, магнитофоны, плееры, переговорные устройства, технические носители информации (дискеты и др.), мобильные телефоны, копировальные аппараты и пользоваться ими;

• выносить конфиденциальные документы из здания без разрешения руководства организации, работать с конфиденциальной документированной информацией в непредназначенных для этого помещениях;

• оставлять конфиденциальные документы на рабочем столе без контроля, хранить эти документы вместе с открытыми документами и материалами, оставлять без контроля компьютер с загруженной конфиденциальной информацией;

• разглашать сведения о характере автоматизированной обработки конфиденциальной информации на компьютере в АИС и о личных идентифицирующих паролях;

• разглашать сведения о составе находящейся у сотрудника конфиденциальной документированной информации, системе ее защиты и месте хранения, а также об известных ему элементах обеспечения информационной безопасности организации.

Представители других организаций допускаются к ознакомлению и работе с конфиденциальной документированной информацией с разрешения руководства организации, руководства Службы делопроизводства, а также структурных подразделений, в ведении которых находятся эти материалы, при наличии письменного запроса тех организаций, в которых они работают, с указанием темы выполняемого задания.

По окончании рабочего дня руководители и исполнители должны проверить конфиденциальные документы (в том числе электронные документы на компьютере), убедиться в их комплектности и сдать их в Службу делопроизводства. Оставлять документы на рабочем месте запрещается. Каждый конфиденциальный документ сдается, как правило, в отдельности. При наличии у исполнителя нескольких конфиденциальных документов, необходимых ему для ежедневной работы, они могут помещаться вместе с описью в специальный портфель (кейс), который запирается, опечатывается личной печатью этого сотрудника и сдается в Службу делопроизводства.

Служба делопроизводства обязана периодически проверять порядок хранения конфиденциальных документов в служебных комнатах сотрудников и обращения с ними.

Нарушения порядка обмена конфиденциальными документами целесообразно учитывать в целях последующего анализа и принятия мер по их предотвращению. Учет нарушений может осуществляться в карточке (журнале) по форме 2.

Форма 2

Дата нарушения	Инициалы, фамилия лица, допустившего нарушение	Краткое изложение характера нарушения	Причины нарушения	Принятые меры
1	2	3	4	5

О серьезных нарушениях, которые привели или могли привести к утрате документов или утечке содержащейся в них информации, Служба делопроизводства и Служба безопасности (если такая существует в организации) должны докладывать руководителю организации и вносить предложения об отстранении от работы с конфиденциальной документированной информацией или о привлечении к ответственности виновных лиц.

При смене руководителя и сотрудников подразделения Службы делопроизводства, их временном отсутствии, а также временном отсутствии исполнителей передача конфиденциальных документов замещающим их лицам производится по актам или распискам с обязательной проверкой наличия документов (см. разд. 7.4).

7.2. Режим сохранности конфиденциальных документов и дел

Для обеспечения физической сохранности конфиденциальных документов и дел, предотвращения утечки содержащейся в них информации должен быть установлен специальный режим их хранения.

Помещения Службы делопроизводства, предназначенные для круглосуточного хранения конфиденциальных документов и дел, в целях обеспечения дополнительных гарантий от постороннего проникновения в них должны, как правило, находиться не на первом и последнем этажах. Кроме того, они должны соответствовать нормам, установленным для хранения документов и дел: быть удалены от помещений с пищевыми продуктами и химическими веществами, не иметь с ними общих вентиляционных каналов, отвечать требованиям пожарной безопасности, санитарным нормам, а также иметь гарантию от затопления.

Вход в такие помещения необходимо строго регламентировать. Кроме руководителя организации и сотрудников, имеющих прямое отношение к обработке и хранению конфиденциальных документов и дел, в помещения могут допускаться лица, обеспечивающие их обслуживание. Уборка помещений, ремонт находящихся в них оборудования и технических средств, выполнение других работ, связанных с привлечением лиц, не имеющих доступа к хранящимся в помещениях документам, должны проходить только в присутствии сотрудников Службы делопроизводства.

Окна помещений должны иметь надежные средства защиты, исключающие возможность проникновения в помещения посторонних лиц. Кроме того, на них должны быть защитная сетка или жалюзи, предотвращающие возможность выпадения документов, а также визуального просмотра документов и экранов видеомониторов с улицы. Если помещения расположены на первом или последнем этаже или рядом с ними находятся пожарные лестницы, балконы, водосточные трубы или другие какие-либо пристройки, с помощью которых можно проникнуть в помещения, то для предотвращения проникновения окна дополнительно защищаются распашной металлической решеткой с замком.

Входные двери помещений должны быть обиты металлом и оборудованы замками, гарантирующими их надежное закрытие. По окончании рабочего дня двери необходимо не только запирать, но и опечатывать печатью Службы делопроизводства. Печать проставляется на тонкий слой пластилина или специальной мастики таким образом, чтобы оттиск невозможно было снять и восстановить. Перед отпиранием двери проверяются сохранность оттиска печати и целостность запоров. При обнаружении попыток проникновения в помещения нужно немедленно поставить в известность Службу безопасности и доложить руководству организации. До принятия решения руководством организации помещения не открываются и обеспечиваются физической охраной.

Для предотвращения несанкционированного входа в помещения в течение рабочего дня на дверях могут устанавливаться электромеханические или электронные замки.

Конфиденциальные документы и дела в помещениях должны храниться в сейфах, металлических шкафах или на металлических стеллажах, которые по окончании рабочего дня запираются и опечатываются сотрудниками, ответственными за учет и хранение документов и дел. Хранение открытых документов вместе с конфиденциальными допускается только в случаях, когда они являются приложениями к конфиденциальным документам.

Входные двери, окна помещений, а также сейфы, шкафы и стеллажи следует оснастить охранной сигнализацией, связанной со Службой безопасности организации или Службой охраны.

Помещения, в которых для фиксации, обработки, хранения, воспроизведения и передачи конфиденциальной документированной информации используются компьютеры, объединенные в локальную сеть, электронные множительные аппараты, средства аудио-, видеозаписывающей и воспроизводящей техники и другие технические средства, создающие электромагнитное излучение, необходимо оборудовать дополнительными средствами защиты, предотвращающими перехват злоумышленниками электромагнитных сигналов, несущих конфиденциальную информацию. В этих же целях целесообразно приобретать сертифицированные технические средства обработки информации, отвечающие требованиям по защите конфиденциальной информации от ее утечки (более подробно см. разд. 8). Замки дверей помещений, распашных металлических решеток на окнах, сейфов, шкафов или стеллажей должны иметь рабочие и запасные экземпляры ключей. Запасные экземпляры ключей могут храниться в опечатанных их владельцами пеналах или конвертах либо у руководителя организации, либо в Службе охраны, либо (ключи от сейфов, шкафов, стеллажей, металлических решеток) в сейфе (шкафу) сотрудника Службы делопроизводства, ответственного за хранение документов.

Рабочие экземпляры ключей от сейфов, шкафов, стеллажей, решеток в нерабочее время могут храниться в опечатанном пенале (конверте) либо в службе охраны, либо в сейфе (шкафу) сотрудника Службы делопроизводства, ответственного за хранение документов. В последнем случае по окончании рабочего дня ключ от этого сейфа вместе с рабочим экземпляром ключа от входной двери помещения передается в пенале, опечатанном печатью сотрудника Службы делопроизводства, в Службу охраны с внесением соответствующих данных в графы 1–6 журнала передачи-приема под охрану помещений и пеналов с ключами (форма 3).

Форма 3

Наименование или номера помещений, передаваемых под охрану	Номера печатей, которыми опечатаны помещения и пеналы с ключами	Дата и время передачи под охрану	Подпись и фамилия лица, передающего помещение и пеналы под охрану
1	2	3	4

Окончание

Отметка о включении сигнализации	Подпись и фамилия лица, принявшего помещение и пеналы под охрану	Дата и время получения пеналов	Подпись и фамилия лица, получившего пеналы	Отметка о выключении сигнализации
5	6	7	8	9

При получении пенала из Службы охраны заполняются графы 7–9. Получение пенала с ключами из Службы охраны и вскрытие помещений должны осуществляться только сотрудниками Службы делопроизводства, ответственными за хранение конфиденциальных документов и дел.

В случае утраты рабочих или запасных экземпляров ключей об этом необходимо немедленно поставить в известность руководство организации. При утрате ключа от сейфа, шкафа или стеллажа до замены замка или смены секрета замка хранить документы в этом сейфе (шкафу, стеллаже) не следует.

Для выдачи конфиденциальных документов и дел исполнителям (пользователям) помещения должны оборудоваться специальными окошками, не выходящими в общий коридор, или внутри отгораживаться барьером.

Исполнители могут работать с конфиденциальными документами или в специально выделенных помещениях Службы делопроизводства, или в своих служебных комнатах, если эти комнаты отвечают требованиям обеспечения сохранности и конфиденциальности документов. При работе с документами в служебных помещениях каждый исполнитель должен быть обеспечен постоянным рабочим местом, сейфом (металлическим шкафом) или отдельной ячейкой сейфа для хранения конфиденциальных документов и номерной металлической печатью (см. разд. 7.1).

Ключи от сейфа и номерная печать выдаются исполнителю под подпись в лицевом счете. Рабочий экземпляр ключа и номерная печать хранятся постоянно у исполнителя. Запасные экземпляры ключей должны храниться в Службе делопроизводства или Службе охраны в опечатанном номерной печатью исполнителя конверте либо пенале.

Все сейфы, шкафы и стеллажи, установленные в помещениях Службы делопроизводства и в служебных комнатах исполнителей, в которых круглосуточно или в рабочее время хранятся конфиденциальные документы, а также ключи от них должны учитываться Службой охраны по журналу учета хранилищ и ключей от них (форма 4).

При внесении в журнал данных о ключах от распашных металлических решеток графы 2 и 3 не заполняются.

Ежегодно должна проводиться проверка фактического наличия ключей от хранилищ и номерных печатей исполнителей.

Форма 4

№ п/п	Наименование хранилища (сейф, металлический шкаф, металлический стеллаж)	Инвентарный номер хранилища	Местонахождение хранилища (подразделение, номер комнаты)
1	2	3	4

Окончание

Инициалы и фамилия ответственного за хранилище	Количество экземпляров ключей и их номера	Подпись ответственного за хранилище, за получение ключей, дата	Подпись сотрудника Службы охраны за прием ключей
5	6	7	8

Для эвакуации конфиденциальных документов и дел при возникновении стихийных бедствий, пожара, аварии, грозящих затоплением, или других формах чрезвычайных ситуаций, грозящих уничтожением документов и дел, в помещениях, предназначенных для хранения конфиденциальных документов, должно находиться необходимое количество тары (мешков, чемоданов, контейнеров и т. д.), в которой можно транспортировать документы.

При возникновении чрезвычайной ситуаций сотрудники Службы делопроизводства обязаны немедленно вызвать пожарную команду или соответствующую аварийную службу, службу МЧС, уведомить руководство организации, принять меры к ликвидации такой ситуации, а при невозможности ликвидации обеспечить охрану документов и дел собственными силами, а также силами Службы безопасности и Службы охраны организации и начать эвакуацию документов и дел в заранее определенное место.

При возникновении чрезвычайной ситуации в нерабочее время проведение аналогичных действий должен организовать дежурный по организации, поставив в известность руководство организации, а также Служб безопасности, охраны и делопроизводства. О проведенном вскрытии (при необходимости) помещений, а также о вскрытии, по согласованию с руководством организации или Служб безопасности, охраны, делопроизводства, сейфов, шкафов или стеллажей составляется акт, в котором указываются должности и фамилии лиц, производивших вскрытие, а также хранилища, которые были вскрыты, места, куда помещены документы и дела, номера печатей на таре.

7.3. Режим конфиденциальности при проведении совещаний и переговоров

Совещания и переговоры, в процессе проведения которых может упоминаться информация с ограниченным доступом, именуются конфиденциальными. Разрешение на проведение таких совещаний и переговоров (далее – совещание) с приглашением представителей других организаций, предприятий дает руководитель организации.

Решение руководителя о предстоящем совещании доводится до сведения руководителей Службы делопроизводства и Службы безопасности. Информация об этом решении фиксируется специально выделенным сотрудником Службы делопроизводства в карточке учета, в том числе электронной, в целях дальнейшего контроля за подготовкой и проведением такого совещания.

Плановые и неплановые конфиденциальные совещания, которые проводятся без приглашения посторонних лиц руководством организации, его заместителями, ответственными исполнителями (специалистами по направлениям работы), обязательно предварительно согласовываются с руководителями Службы безопасности и Службы делопроизводства. По факту проведения таких совещаний в Службе делопроизводства заводится учетная карточка, в том числе электронная, в которой фиксируются рассмотренные вопросы, принятые решения и состав присутствовавших работников организации.

Допуск работников на любые совещания, в том числе и конфиденциальные, осуществляется на основе действующей в организации разрешительной системы доступа (см. гл. 4). Приглашение на такие совещания лиц, не являющихся работниками организации, допускается только в случае крайней необходимости их личного участия в обсуждении конкретного вопроса. Присутствие их при обсуждении других вопросов не разрешается. Допуск участников конфиденциального совещания в помещение, в котором оно будет проводиться, обеспечивает ответственный организатор совещания в соответствии с утвержденным списком и предъявляемыми участниками персональными документами.

Перед началом обсуждения каждого вопроса состав присутствующих корректируется. Нахождение (ожидание) в помещении лиц, в том числе работников данной организации, не имеющих отношения к обсуждаемому вопросу, запрещается. Требуется, чтобы организовавший совещание работник перед его открытием напомнил участникам о необходимости соблюдения режима конфиденциальности информации и уточнил, какая конкретно информация является конфиденциальной на данном совещании.

Ответственность за обеспечение защиты конфиденциальной информации и соблюдение конфиденциальности в ходе подготовки и проведения совещания несет сотрудник подразделения, организующий данное совещание. Сотрудник Службы делопроизводства оказывает помощь сотруднику, организующему данное совещание, и совместно со Службой безопасности осуществляет контроль за перекрытием возможных организационных и технических каналов утечки информации.

Подготовку конфиденциального совещания проводит организующий его сотрудник с привлечением других сотрудников, допущенных к работе с конкретной конфиденциальной документированной информацией. Из числа этих сотрудников назначается ответственный организатор (например, ответственный секретарь коллегиального

органа организации или помощник руководителя организации), планирующий и координирующий выполнение подготовительных мероприятий и проведение совещания.

В процессе подготовки конфиденциального совещания составляются: программа его проведения, повестка дня, информационные материалы, проекты решений и список участников совещания по каждому вопросу повестки дня. Все документы, составляемые в процессе подготовки конфиденциального совещания, должны иметь гриф конфиденциальности, составляться и обрабатываться в соответствии с требованиями действующей в организации Инструкции по организации конфиденциального делопроизводства.

Документы (в том числе договоры, контракты и др.), предназначенные для раздачи участникам совещания, не должны содержать конфиденциальной информации. Эта информация сообщается участникам совещания устно при обсуждении конкретного вопроса. Цифровые значения конфиденциальной документированной информации (технические и технологические параметры, суммы, проценты, сроки, объемы и т.д.) в проектах решений и других документов не указываются или фиксируются в качестве общепринятой стартовой величины при обсуждении. В проектах не должно быть развернутых обоснований для предоставления льгот и скидок тем или иным партнерам, клиентам или лишения их льгот. Проекты документов, раздаваемые участникам совещания, не должны иметь грифа конфиденциальности.

Список участников совещания составляется отдельно по каждому обсуждаемому вопросу. К участию в обсуждении вопроса привлекаются только те работники организации, которые имеют непосредственное отношение к этому вопросу. В списке участников указываются фамилии, имена и отчества лиц, занимаемые должности, представляемые ими организации и наименования документов, подтверждающих их полномочия вести переговоры и принимать решения. Наименование представляемой организации может при необходимости заменяться ее условным обозначением.

Документом, подтверждающим полномочия лица (если это не руководитель сторонней организации) при ведении переговоров и принятии решения по конкретному вопросу, может служить письмо, доверенность представляемой лицом организации, рекомендательное письмо юридического или физического лица, письменный ответ сторонней организации на запрос о полномочиях представителя, в отдельных случаях телефонное, факсимильное или электронное послание – подтверждение полномочий руководителем сторонней организации. Наименование документа, подтверждаю-

щего полномочия лица, может вноситься в список непосредственно перед началом совещания. Эти документы передаются участниками совещания ответственному организатору для хранения в Службе делопроизводства.

Конфиденциальные документы, составляемые при подготовке конфиденциальных совещаний, на которых предполагается присутствие представителей других организаций, согласовываются с руководством Службы делопроизводства и Службы безопасности. Их предложения по замеченным недостаткам в обеспечении защиты конфиденциальной документированной информации должны быть исправлены ответственным организатором совещания. После этого документы утверждаются руководителем, организующим совещание. Одновременно с визированием подготовленных документов руководство Службы делопроизводства, Службы безопасности и ответственный организатор определяют место проведения совещания, порядок доступа участников совещания в это помещение, порядок документирования хода обсуждения вопросов и принимаемых решений, а также порядок рассылки (передачи) участникам совещания оформленных решений и подписанных документов (см. разд. 3.5).

К помещению, где будет проводиться любое конфиденциальное совещание, предъявляются определенные требования. Оно оборудуется средствами технической защиты информации, имеет кондиционер, так как открытие окон, дверей в ходе проведения совещания не допускается. Окна закрываются шторами, входная дверь оборудуется сигналом, оповещающим о ее неплотном закрытии. В целях звукоизоляции целесообразно иметь двойную дверь (тамбур) или зашторивать двери звукопоглощающей тканью. Проведение совещаний в других или неприспособленных помещениях запрещается.

В помещении для проведения совещаний не должны находиться приборы, оборудование и технические средства, которые непосредственно не используются для обеспечения хода совещания, например мобильные телефоны, компьютеры (ноутбуки), теле-, радиоприемники и др. При необходимости они размещаются в соседней изолированной комнате.

Перед началом совещания сотрудник Службы безопасности обязан убедиться в отсутствии в помещении аудио- и видеозаписывающих или передающих устройств и качественной работе средств технической защиты на всех возможных каналах утечки информации. Аудио- и видеозапись конфиденциальных совещаний, фотографирование ведутся только по письменному указанию руководителя организации и осуществляются одним из работников, готовивших совещание.

Ход конфиденциального совещания документируется одним из готовивших его работников или сотрудником Службы делопроизводства. На особо закрытых совещаниях эту работу выполняет непосредственно ответственный организатор совещания. Составляемый протокол должен иметь гриф конфиденциальности необходимой степени и оформляться в стенографической тетради, зарегистрированной в Службе делопроизводства (см. разд. 2.4). Запись участников хода совещания определяется сотрудником, организовавшим совещание, исходя из содержания той информации, которая оглашается.

При необходимости вызова на проходящее совещание дополнительных лиц (журналистов, консультантов, экспертов, представителей других организаций) факт их участия в совещании фиксируется в протоколе с указанием мотивов их вызова. Присутствие этих лиц на совещании ограничивается временем рассмотрения той ситуации, по которой они были вызваны.

Участникам конфиденциального совещания независимо от занимаемой должности и статуса на совещании не разрешается:

- вносить в помещение, в котором проводится совещание, фото-, кино-, видеоаппаратуру, компьютеры, магнитофоны, радиоприемники, радиотелефоны, мобильные телефоны и другую аппаратуру, пользоваться ею;
- делать выписки из документов, используемых при решении вопросов на совещании и имеющих гриф конфиденциальности;
- обсуждать вопросы, вынесенные на совещание, в местах общего пользования (буфет, туалет, курительная комната);
- информировать о совещании (вопросах повестки дня, составе участников, времени и месте проведения, ходе обсуждения вопросов, содержании решения и т.д.) любых лиц, не связанных с проведением данного совещания, в том числе сотрудников организации.

Участники совещания, замеченные в несанкционированной аудио- или видеозаписи или использовании средств связи, фотографировании, лишаются права дальнейшего присутствия на совещании. По факту составляется акт, копия его направляется в организацию, представителем которой является данное лицо, или передается руководителю – организатору совещания, если это лицо является сотрудником организации. Одновременно носитель несанкционированно записанной информации передается руководителю Службы безопасности для учета и хранения. Устройство записи с уничтоженной несанкционированной записанной на носителе информацией возвращается владельцу.

В процессе совещания его участники не могут оглашать больший объем конфиденциальной информации, чем это было установлено при подготовке совещания, или сообщать информацию, не относящуюся к обсуждаемому вопросу. Состав оглашаемой конфиденциальной информации регламентируется работником, организовавшим совещание.

При проведении переговоров по заключению, продлению или прекращению какого-либо договора сотрудникам организации, участвующим в переговорах, не разрешается раскрывать стратегию и желаемые результаты переговоров, итоги аналогичных переговоров с другими партнерами. В процессе неофициальной части переговоров обсуждение вопросов, связанных с темой совещания, не допускается.

По окончании конфиденциального совещания помещение, в котором оно проходило, осматривается сотрудниками Службы безопасности, запирается, опечатывается и сдается под охрану. Документы, принятые на совещании, оформляются, подписываются, при необходимости размножаются и рассылаются (передаются) участникам совещания в соответствии с требованиями организации к работе с конфиденциальной документированной информации. Все экземпляры этих документов должны иметь отметку конфиденциальности.

7.4. Проверка наличия носителей конфиденциальной информации

7.4.1. Назначение, виды и принципы проведения проверок

Проверки наличия конфиденциальной документированной информации являются важной составной частью конфиденциального документооборота. Цель проверок состоит в обеспечении контроля за сохранностью документов и дел и достигается путем установления соответствия фактического наличия конфиденциальных документов учетным и регистрационным данным, выявления отсутствующих документов и принятия мер по их розыску [209].

В процессе учета и регистрации документов могут быть допущены ошибки, следствием которых становится искажение учетных и регистрационных данных.

Часть зарегистрированных конфиденциальных документов может быть отправлена, уничтожена, подшита в дела, переведена в другую автоматизированную информационную систему, возвращена после отправления, переведена на другой вид учета. При проставлении

в учетных и регистрационных формах отметок о таком движении документов также могут случаться ошибки, которые при определенных обстоятельствах создают основу для утраты конфиденциальных документов и (или) несвоевременного обнаружения утрат. Поэтому проверки правильности учета и проставления отметок о движении конфиденциальных документов и дел должны быть составляющими частями проверок их наличия.

Проверки направлены также на выявление неучтенных и незарегистрированных по каким-либо причинам конфиденциальных документов, установление причин этого и взятие документов для учета и регистрации. Проверками должны быть охвачены не только документы и дела, но и носители конфиденциальной информации, в том числе электронные (см. разд. 2.4 и 3.7).

Проверки правильности регистрации и фактического наличия конфиденциальных документов частично проводятся в процессе выдачи их пользователям и последующего возврата. Однако такие проверки не охватывают все документы и все необходимые для этого операции. Поэтому необходимо проводить комплексные плановые проверки фактического наличия документов, дел и носителей и правильности отметок об их учете, регистрации и движении. Оптимальными видами проверок и сроками их проведения являются:

- проверки правильности учета и регистрации носителей, документов, дел, учетных и регистрационных журналов (картотек), в том числе электронных – сразу после учета и регистрации;
- проверки правильности проставления отметок о движении конфиденциальных носителей, документов и дел, независимо от времени их учета и регистрации, – сразу после проставления отметок или, при невозможности проведения их сразу после проставления отметок, по истечении каждого квартала;
- проверки фактического наличия всех носителей и всех не подшитых в дела и не переведенных на учет инвентарного (выделенного) хранения (см. разд. 3.6) созданных/изданных (внутренних) и поступивших документов, независимо от времени их регистрации, – один раз в квартал по истечении квартала;
- проверка фактического наличия всех дел, а также документов выделенного хранения и журналов (картотек) учета, в том числе электронных, зарегистрированных в истекшем и предыдущих годах, – один раз в год по истечении года.

Перечисленные виды проверок и сроки их проведения позволяют своевременно выявлять ошибки, допущенные при учете и регистрации конфиденциальной документированной информации

и производстве отметок о ее движении, а также осуществлять систематический контроль за ее наличием, при этом более тщательный в отношении документов, не сброшюрованных и не подшитых в дела, а следовательно, подвергающихся большей опасности утраты. В то же время такой состав проверок и такая периодичность их проведения дают возможность избежать повтора проверочных операций, за исключением проверок фактического наличия части носителей и не подшитых в дела документов.

Существуют так называемые нерегламентные проверки фактического наличия конфиденциальной документированной информации, которые проводятся по мере возникновения необходимости в них.

Проверочные операции может осуществлять сотрудник Службы делопроизводства, учитывающий конфиденциальные документы и производящий отметки о их движении.

Нерегламентную проверку целесообразно использовать при проверках правильности учета носителей, документов, дел, учетных и регистрационных журналов (картотек), в том числе при проверках отметок о возврате ранее отправленных документов, а также при проверках их фактического наличия, так как учетные данные и количество листов дополнительно проверяются в процессе передачи-приема носителей, документов и дел между исполнителями и Службой делопроизводства.

Проверки правильности проставления отметок о движении документов, дел и носителей (отправлении, уничтожении, переводе на другой вид учета и др.) следует возлагать на другого сотрудника, не принимавшего участия в проставлении отметок о движении конфиденциальной документированной информации.

В целях обеспечения контроля за проведением всех необходимых проверочных операций и избежания их дублирования следует проставлять соответствующие отметки о проверках.

Отметки о проверках правильности учета и регистрации носителей, документов, дел и учетных и регистрационных журналов (картотек), в том числе электронных, а также правильности записей о возврате документов проставляются условным обозначением, например, «+» или «*».

Отметки о проверках фактического наличия носителей, документов, дел и учетных и регистрационных журналов (картотек) целесообразно проставлять датами проверок, поскольку, как уже отмечалось, такие проверки частично повторяются и по дате можно отличить одну проверку от другой.

Проверки правильности производства отметок об отправлении, уничтожении, переводе на другой вид учета, подшивке в дело заверяются подписями проверявших (при проведении проверок одним сотрудником – одной подписью) с проставлением даты.

При проведении проверок необходимо руководствоваться следующими принципами:

- охват проверочными операциями всех подлежащих проверке документов, дел и носителей, всех учетных и регистрационных форм, в которых зафиксированы проверяемые реквизиты, и всех необходимых сопроводительных материалов о движении документов;
- проведение проверок наличия конфиденциальной документированной информации по схеме: сначала указанная информация и ее носители, затем учетные и регистрационные данные на них;
- фиксация конечных результатов проверок.

По результатам проверок составляется акт по форме 5.

Форма 5

УТВЕРЖДАЮ

Наименование должности
руководителя организации

_____ _____
(подпись, инициалы, фамилия, дата)

АКТ

_____№ _____
о проверке наличия конфиденциальных документов за_____
Составлен: _____
(инициалы, фамилии лиц, проводивших проверку)

В период с _____по _____201_ г. проведена проверка:

1) правильности проставления учетных данных носителей, документов, дел и журналов (картотек) учета;

2) правильности произведения отметок о движении носителей, документов и дел, независимо от времени их регистрации;

3) фактического наличия всех дел и документов выделенного хранения (без просчета листов);

4) фактического наличия всех носителей, внутренних (созданных/изданных) и поступивших документов с просчетом количества листов, независимо от времени их регистрации *(если рабочие и стенографические тетради проверялись без просчета количества листов, то это фиксируется в скобках или примечаниях)*;

5) фактического наличия журналов (картотек) учета (без просчета количества листов, карточек);

6) закрытия всех учетных номеров в журналах (картотеках) учета внутренних (созданных/изданных) поступивших документов и носителей.

В результате проверки установлено, что:

1. Все подлежащие проверке дела, документы инвентарного (выделенного) хранения и журналы (картотеки) учета находятся в наличии. (*Если в наличии не все, то пишется слово «кроме», с указанием учетных номеров документов или индексов (номеров) и года дел (журналов)*).

2. Все учетные номера в журналах (картотеках) закрыты.

3. Номера дел (документов инвентарного (выделенного) хранения, документов по другим формам учета) не учтены*.

4. Все учетные данные, проставленные на носителях, документах, делах, журналах (картотеках) учета, соответствуют данным, проставленным в учетных формах. (*Если в процессе проверки были обнаружены факты несоответствия, то пишется «кроме», с указанием по каждому документу (носителю, делу), в чем они проявились*).

5. Все отметки о движении документов, дел и носителей соответствуют сопроводительным (оправдательным) материалам и фактическому местонахождению документов. (*Если в процессе проверки были обнаружены факты несоответствия, то пишется «кроме», с указанием по каждому документу (носителю, делу), в чем они проявились*).

6. Имеются следующие ошибки и нарушения в учете и хранении документов. (*Перечисляются ошибки, нарушения и меры, принятые по их устранению. Пункт включается в акт при выявлении ошибок и нарушений*).

7.4.2. Проверка учета и регистрации носителей конфиденциальной информации

Для проверки правильности учета носителей должны привлекаться журнал учета носителей и сами носители (см. разд. 2.4 и 3.1).

Если носители в момент их заведения регистрируются не в журнале учета носителей, а в журнале учета конфиденциальной документированной информации инвентарного (выделенного) хранения (рабочие тетради, калька и др.), то для проверки правильности их регистрации привлекаются журнал учета документов инвентарного (выделенного) хранения (см. разд. 3.6, форма 1) и носители. В контрольном журнале (см. разд. 3.1, форма 1) и на носителе проверяются записи об учетном или регистрационном номере и отметке конфиденциальности носителя, дате регистрации, виде и наименовании носителя, наименовании подразделения, номерах экземпляров, количестве листов в экземпляре. На носителе проверяется правильность нумерации листов. Отметка о проверке проставляется в журнале рядом с номером носителя (см. разд. 3.1, форма 1, графа 4).

* Указываются раздельно носители, дела, документы по каждому виду учета. Пункт включается в акт при наличии неучтенных дел или документов.

Для проверки правильности учета внутренних (созданных/изданных) документов привлекаются журнал учета конфиденциальных распорядительных документов (см. разд. 3.3), сами документы и черновики. В журнале и на документе проверяются записи об учетном номере, отметке конфиденциальности, дате и заголовке документа, местонахождении документа. На самом документе проверяются в реквизите «Отметка об исполнителе» количество экземпляров – по их фактическому наличию, количество листов в экземпляре. Также в конфиденциальном документе проверяются правильность нумерации листов, проставление регистрационных номеров на каждом листе документа, проставление номера экземпляра на каждом экземпляре. В журнале учета бумажных носителей (см. разд. 2.4, форма 1) и на черновике проверяется соответствие номера носителя и номеров листов черновика.

Проверка правильности проставления реквизитов поступившей конфиденциальной документированной информации осуществляется в журнале (картотеке) учета поступивших конфиденциальных документов (см. разд. 3.2.2) и в журнале учета конфиденциальной документированной информации инвентарного (выделенного) хранения (см. разд. 3.6).

Для проверки правильности учета поступивших документов привлекаются журнал учета поступивших пакетов (см. разд. 3.2.1), журнал учета поступивших документов (см. разд. 3.2.2) и сами конфиденциальные документы. В журнале учета пакетов проверяется соответствие количества поступивших пакетов (см. разд. 3.2.1) количеству учтенных поступивших документов (см. разд. 3.2.2). В журнале учета пакетов и журнале учета и регистрации поступивших конфиденциальных документов проверяется соответствие данных о присвоении регистрационного номера, дате поступления документа регистрационному номеру организации-отправителя. В журнале учета и регистрации поступивших конфиденциальных документов и на документе проверяется соответствие регистрационного номера, отметки конфиденциальности, даты поступления, вида и заголовка документа организации-отправителя, регистрационного номера организации-отправителя, даты документа, количества листов (с просчетом их в документе). В документе, имеющем приложения, дополнительно проверяется соответствие регистрационных номеров, отметок конфиденциальности, номеров экземпляров, количества листов в экземпляре данным, содержащимся в реквизите «Отметка о наличии приложения». Отметки о проверке проставляются в журнале учета пакетов

(см. разд. 3.2.1, форма 3, графа 10) и журнале учета поступивших конфиденциальных документов рядом с номером документа (см. разд. 3.2.1, форма 3, графа 1).

Для проверки правильности учета документов инвентарного (выделенного) хранения (см. разд. 3.6, форма 1) привлекаются журнал учета поступивших пакетов, журнал учета поступивших конфиденциальных документов и сами конфиденциальные документы. В журналах учета пакетов и учета поступивших документов проверяется соответствие учетных и регистрационных данных. В журнале учета документов инвентарного (выделенного) хранения и на самом документе проверяется соответствие учетных данных и реквизитов документа.

Отметки о проверке проставляются в журнале учета пакетов (см. разд. 3.2.1, форма 3, графа 10) рядом с номерами документов, переведенных на инвентарное (выделенное) хранение, и в журнале учета конфиденциальных документов инвентарного (выделенного) хранения рядом с номерами документов.

Для проверки правильности регистрации дел и журналов (картотек) учета привлекаются номенклатура дел (см. гл. 5), дела и журналы (картотеки) учета. В номенклатуре и на обложке дела или на картотеке (в журнале) проверяется соответствие сделанных в ней записей индекса (номера) дела (журнала, картотеки), грифа конфиденциальности, заголовка (наименования), срока хранения и номеров статей по перечням документов и дел со сроками хранения. По журналам регистрации и учета, кроме того, проверяется соответствие количества листов в деле. Отметка о проверке проставляется в номенклатуре рядом с индексом (номером) дела, журнала или картотеки.

7.4.3. Проверка правильности проставления отметок о движении носителей конфиденциальной информации

Для проверки правильности проставления отметок об отправлении конфиденциальных документов привлекаются журнал учета и распределения внутренних (созданных/изданных) конфиденциальных документов (см. разд. 3.5.1), журнал учета отправляемых пакетов (см. разд. 3.5.2), а также сопроводительные материалы, по которым отправлены документы (реестры, расписки, квитанции, сопроводительные письма).

В журнале и сопроводительном документе проверяется соответствие сделанных в них записей о номере, отметке конфиденциальности, виде и наименовании документа, адресате, номерах отправленных экземпляров (по документам, зарегистрированным в журнале учета внутренних (созданных/изданных) конфиденциальных документов (вместо номеров экземпляров проверяется количество отправленных листов), наименовании, номере и дате сопроводительного документа.

Для проверки правильности проставления отметок о возврате ошибочно присланных конфиденциальных документов привлекаются журнал учета поступивших пакетов (см. разд. 3.2.1, форма 3), копии сопроводительных писем, с которыми отправлены документы. В журнале и сопроводительном письме проверяется соответствие записей о номере и отметке конфиденциальности документа, адресате, номере и дате сопроводительного письма. Для проверки правильности проставления отметок об отправлении дел привлекаются номенклатура дел и сопроводительные документы, по которым отправлены дела. В номенклатуре дел и сопроводительном документе проверяется соответствие записей об индексе (номере) и грифе конфиденциальности дела, заголовке дела, номере тома, количестве листов в томе, адресате, номере и дате сопроводительного документа.

Для проверки правильности отметок об отправлении документов, изъятых из дел, привлекаются дела, из которых изъяты документы, и сопроводительные документы, по которым отправлены изъятые документы. В сопроводительном документе, описи документов дела и справке-заместителе проверяется соответствие записей о номере, грифе конфиденциальности и количестве листов документа, адресате, номере и дате сопроводительного документа.

Кроме того, в процессе проверок наличия отметок об отправлении документов и дел в сопроводительном документе (за исключением сопроводительных писем) проверяется наличие подписи лица за получение пакетов.

Для проверки правильности проставления отметок об уничтожении документов выделенного хранения привлекаются журнал учета документов выделенного хранения и акты об уничтожении дел и документов. В журнале и акте проверяется соответствие записей об учетном номере, грифе конфиденциальности, виде и заголовке документа, номерах экземпляров, количестве листов в экземпляре, номере и дате акта об уничтожении.

Для проверки правильности проставления отметок об уничтожении дел и журналов (картотек) учета привлекаются номенклатура дел и акты об уничтожении дел и документов. В номенклатуре и акте проверяется соответствие записей об индексе (номере) и грифе конфиденциальности дела (журнала, картотеки), его заголовке, номере тома, количестве листов в томе (по картотеке вместо номера тома и количества листов проверяется количество карточек), номере и дате акта об уничтожении.

Для проверки правильности проставления отметок об уничтожении документов, изъятых из дел, привлекаются дела, из которых изъяты документы, и акт об уничтожении дел и документов. В акте, описи документов дела и справке-заместителе проверяется соответствие записей о номере, грифе конфиденциальности и дате документа, количестве листов, номере и дате акта об уничтожении.

Кроме того, в процессе проверок правильности проставления отметок об уничтожении документов и дел в акте об уничтожении проверяется наличие отметок о физическом уничтожении документов и дел, заверенных подписями лиц, производивших уничтожение.

Для проверки правильности проставления отметок о переводе внутренних и поступивших конфиденциальных документов на учет документов выделенного хранения привлекаются журналы учета внутренних (созданных/изданных) конфиденциальных документов; поступивших конфиденциальных документов и конфиденциальной документированной информации инвентарного (выделенного) хранения. В журналах и документах проверяется соответствие учетного номера, присвоенного при создании (издании) или поступлении документа, учетному номеру, присвоенному по журналу учета документов инвентарного (выделенного) хранения, отметки о конфиденциальности, вида, заголовка и номеров экземпляров документа, количества листов в экземпляре с просчетом листов. В журнале учета конфиденциальной документированной информации инвентарного (выделенного) хранения рядом с номером документа проставляется отметка о проверке правильности учета и регистрации.

В журналах проверяется соответствие учетного номера и отметки конфиденциальности документа, вида и наименования документа, количества листов. В журнале учета конфиденциальной документированной информации инвентарного (выделенного) хранения и на документе проверяется соответствие учетного номера, грифа конфи-

денциальности, вида и заголовка документа, подразделения, разработавшего документ, номера экземпляра, количества листов в экземпляре с просчетом их в документе.

Для проверки правильности проставления отметок о подшивке документов в дела привлекаются дела, в которых подшиты документы, и журналы учета, в которых зарегистрированы документы. В деле и журнале проверяется соответствие учетного номера, отметки о конфиденциальности, вида и наименования документа, индекса (номера) дела, количества листов в документе, номеров листов дела. Кроме того, в описи документов дела и документе проверяется соответствие даты, номера, грифа конфиденциальности, вида и наименования документа, отправителя (по поступившим документам) или адресата (по отправленным документам), номеров листов дела.

Для проверки правильности проставления отметок о подшивке документов в другие дела привлекаются дела, из которых изъяты документы, и дела, в которые документы перешиты. В описи документов дела, в которое перешит документ, и на документе проверяется соответствие данных, перечисленных в предыдущем абзаце. В справке-заместителе и описи документов дела, из которого изъят документ, проверяется наличие данных о новом местонахождении документа и их соответствие данным описи документов дела, в которое подшит документ.

Для проверки правильности проставления отметок об изъятии из дела документов, с которых снят гриф конфиденциальности, привлекаются дела и акт передачи документов. В описи документов дела, справке-заместителе и акте проверяется соответствие данных о номере, дате и количестве листов документа, дате и номере акта о передаче.

При любом изъятии документов из дел в учетных формах, в которых документы были зарегистрированы, отметки о новом местонахождении или уничтожении документов не производятся.

Для проверки правильности проставления отметок о передаче на архивное хранение дел и документов выделенного хранения привлекаются номенклатура дел, журнал учета документов инвентарного (выделенного) хранения и описи дел и документов, переданных на архивное хранение. В описи и номенклатуре проверяется соответствие индекса (номера), отметки о конфиденциальности, заголовка дела, номера тома дела, количества листов в томе, архивного шифра (номеров фонда, описи, единицы хранения).

В журнале учета конфиденциальных документов инвентарного (выделенного) хранения и описи проверяется соответствие номера, отметки о конфиденциальности, вида и заголовка документа, номера экземпляра, количества листов в экземпляре, архивного шифра.

Для проверки правильности проставления отметок о передаче документов инвентарного (выделенного) хранения, с которых снята отметка о конфиденциальности, привлекаются номенклатура дел, журнал учета документов выделенного хранения и акт передачи. В номенклатуре и акте проверяется соответствие индекса (номера), заголовка дела, номера тома, количества листов, номера и даты акта [209].

ГЛАВА 8

СИСТЕМА ЗАЩИЩЕННОГО ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

8.1. Особенности конфиденциального электронного документооборота

Правительство Российской Федерации утвердило Положение о системе межведомственного электронного документооборота [74]. Федеральная информационная система обеспечивает в автоматизированном режиме защищенный обмен электронными сообщениями, в том числе сообщениями, содержащими информацию, отнесенную к сведениям, составляющим служебную тайну [117].

Защищенный электронный документооборот, как отмечалось во введении, можно разделить на два вида: внутренний (ВЭД) организации и межведомственный (межсетевой) (МЭД) между организациями различного уровня.

Почтовый обмен электронными сообщениями по защищенным каналам связи при МЭД осуществляется с помощью специального программного обеспечения – комплекс программ «Почтовая служба», предназначенного для организации.

Электронное сообщение состоит из двух частей: сопроводительной, предназначенной для адресации сообщения, и содержательной, представляющей собой текст сообщения либо текст сообщения с присоединенными файлами, содержащими электронную копию (электронный образ) документа или электронный документ, и их реквизиты, описанные с помощью языка XML. Формат файлов, используемых при осуществлении МЭД, должен соответствовать национальным или международным стандартам либо иметь открытый исходный код и открытую структуру. Язык XML – расширяемый язык гипертекстовой разметки, используемый для создания и размещения документов в среде WWW. Язык позволяет автоматизировать обмен данными, не прибегая к существенному объему программирования [331].

Стандарт на представление данных – ориентированный, в частности на обмен информацией между независимыми участниками. Формат XML предполагает структурную, а не оформительскую разметку информации. Поэтому XML-файл легко обрабатывать, загружать в базы данных, а также «накладывать» на него любой *дизайн*, необходимый для представления данных в удобной потребителю форме. Именно это делает XML форматом, удобным для трансляций.

Следует отметить, что одни и те же данные в рамках формата XML можно представить разными, несовместимыми друг с другом способами. В тех областях, где обмен информацией – частое и устойчивое явление, разработаны XML-форматы представления данных, которым рекомендуется следовать по мере возможности.

Электронный документ – информационный объект, также состоящий из двух частей:

реквизитной, содержащей идентифицирующие атрибуты (имя, время и место создания, данные об авторе и т.д.) и электронную цифровую подпись;

содержательной, включающей в себя текстовую, числовую и/или графическую информацию, которая обрабатывается в качестве единого целого [149].

Технические требования к организации взаимодействия системы межведомственного электронного документооборота с системами электронного документооборота федеральных органов исполнительной власти утверждены распоряжением Правительства Российской Федерации от 2 октября 2009 г. №1403-р. Основные требования к взаимодействию данных систем других организаций (государственных и негосударственных структур) изложены в разд. 8.3.2.

Правилами делопроизводства в федеральных органах исполнительной власти [76] определено, что электронные документы создаются, обрабатываются и хранятся в системе электронного документооборота федерального органа исполнительной власти (в нашем случае ВЭД организации). Правилами установлен перечень обязательных сведений о документах, используемых в целях учета и поиска документов в системах электронного документооборота. В соответствии с данным перечнем обязательным сведением является отметка о конфиденциальности электронного документа.

Для подписания электронных документов используются электронные цифровые подписи. *Электронная цифровая подпись* – реквизит электронного документа, который предназначен для его защиты от подделки, получен в результате криптографического преобразования информации с использованием закрытого ключа ЭЦП и по-

зволяет идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе [37, ст. 3].

Средства ЭЦП представляют собой аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций:

- создание ЭЦП в электронном документе с использованием закрытого ключа ЭЦП;
- подтверждение с использованием открытого ключа ЭЦП подлинности в электронном документе;
- создание закрытых и открытых ключей ЭЦП.

Используемые средства электронной цифровой подписи должны быть сертифицированы. Сертификат средств ЭЦП – это документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия этих средств установленным требованиям. Рекомендуемый типовой порядок использования электронных документов, подписанных ЭЦП, организации приведен в приложении 7.

При рассмотрении и согласовании электронных документов в системе электронного документооборота могут использоваться способы подтверждения, при которых ЭЦП не используется.

Прием и отправка конфиденциальных электронных документов осуществляются Службой делопроизводства организации. При получении электронных документов Служба делопроизводства осуществляет проверку подлинности ЭЦП.

При передаче поступивших электронных документов на рассмотрение руководству, их направлении в структурные подразделения и ответственным исполнителям, отправке электронных документов для их хранения вместе с электронными документами передаются (хранятся) их регистрационные данные.

Единицей учета электронного документа является электронный документ, зарегистрированный в системе ВЭД организации. Электронный документ — документ, в котором информация представлена в электронно-цифровой форме [Там же].

Исполненные электронные документы систематизируются в дела в соответствии с номенклатурой дел организации (см. гл. 5). При составлении номенклатуры дел указывается, что дело ведется в электронном виде.

Электронные документы после их исполнения подлежат хранению в установленном порядке в организации в течение сроков, предусмотренных для аналогичных документов на бумажном носителе.

По истечении срока, установленного для хранения электронных дел (электронных документов), на основании акта о выделении их к уничтожению, утверждаемого руководителем организации, указанные электронные дела (электронные документы) подлежат уничтожению (см. разд. 6.3, приложение 7).

Защите подлежит информация, имеющая различную структуру и обрабатываемая средствами вычислительной техники, представленная в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитооптической и иной основе.

В нашем случае автоматизированная информационная система и информация, включая конфиденциальную, циркулирующую в системе, рассматриваются как конфиденциальный электронный документооборот.

Информационная безопасность – это защита конфиденциальности, целостности и доступности информации [147]. Конфиденциальность информации: обеспечение доступа к информации только авторизованным пользователям. Целостность информации: обеспечение достоверности и полноты информации и методов ее обработки. Доступность информации: обеспечение доступа к информации и связанным с ней активам авторизованных пользователей по мере необходимости.

Информационная безопасность при осуществлении МЭД и ВЭД обеспечивается комплексом технических и организационных мероприятий. К техническим мероприятиям относятся:

- организация и использование средств защиты информации в полном объеме их функциональных возможностей;
- обеспечение целостности обрабатываемых данных;
- обеспечение антивирусной защиты информации.

К организационным мероприятиям относятся:

- контроль выполнения требований нормативных документов, регламентирующих обеспечение защиты информации;
- определение должностных лиц участников и организатора МЭД, ответственных за обеспечение информационной безопасности;
- установление порядка резервного копирования, восстановления и архивирования баз данных, находящихся на головном узле, а также порядка обновления антивирусных баз;
- установление порядка допуска для проведения ремонтно-восстановительных работ программно-технических средств;
- организация режимных мероприятий в отношении помещений, в которых размещены узлы участников ВЭД и МЭД, и технических средств этих узлов.

Технические средства узла участника включают в себя серверное и коммуникационное оборудование, средства защиты информации, автоматизированные рабочие места (АРМ) и передаются организатором МЭД участнику на безвозмездной основе во временное пользование. Передача оформляется актом приема-передачи технических средств. Технические средства должны быть расположены в помещениях, обеспечивающих их сохранность и конфиденциальность передаваемой и принимаемой информации.

В случае возникновения необходимости размещения у участников дополнительных технических средств и (или) их переноса в другие помещения финансирование выполнения комплекса работ по прокладке объектовых линий связи, приобретения оборудования и программного обеспечения, а также проведения и выполнения специальных работ осуществляется за счет средств участника. Указанные работы для обеспечения конфиденциальности и безопасности производятся поставщиком услуг, имеющим соответствующую лицензию. Спецификация на приобретаемое оборудование, программное обеспечение и материалы, а также техническое задание на выполнение специальных работ согласуются с организатором МЭД.

Настройку технических средств и средств защиты, а также установку специального программного обеспечения выполняет организатор МЭД. Финансирование приобретения расходных материалов (съемные носители информации, картриджи к принтерам и др.) осуществляется участниками МЭД.

Основными функциями узлов участников МЭД являются:

- обеспечение защиты обрабатываемой, хранимой и передаваемой информации от несанкционированного доступа и искажения до передачи ее в защищенный канал связи;
- доставка электронных сообщений, полученных из головного узла, в автоматизированные информационные системы ВЭД адресатов или, иными словами, их автоматизированные информационные системы;
- отправка электронных сообщений из автоматизированных информационных систем ВЭД на головной узел МЭД;
- хранение электронных сообщений до передачи на головной узел МЭД или в автоматизированную информационную систему ВЭД адресата.

Обмен электронными сообщениями при МЭД осуществляют уполномоченные сотрудники. Отправитель электронного сообщения, содержащего электронную копию документа, несет ответственность за соответствие содержания электронной копии содержанию подлинника документа на бумажном носителе.

Регистрация (учет) электронных сообщений в автоматизированной информационной системе ВЭД участника осуществляется в соответствии с инструкцией по делопроизводству этого участника.

Автоматизированная информационная система внутреннего электронного документооборота участника должна обеспечивать подготовку уведомлений о ходе рассмотрения электронных сообщений этим участником.

Требования по защите информации и мероприятия по их выполнению, а также конкретные средства защиты должны определяться и уточняться в зависимости от установленного класса защищенности на основании разрабатываемой модели угроз и действий нарушителя (см. разд. 8.2). Общее описание организации взаимодействия системы МЭД с системой ВЭД приведено в приложении 8.

Защита информации, циркулирующей в АИС организации, или, иными словами, внутреннем электронном документообороте, осуществляется в соответствии с российским законодательством и требованиями нормативно-технических документов в области защиты информации.

Основными задачами обеспечения защиты информации, циркулирующей в АИС, и самих систем на уровне единой информационной среды организации являются:

- формирование технической политики организации в области защиты информационно-коммуникационных технологий;
- координация деятельности структурных подразделений организации в сфере защиты информации и АИС, а также оценка эффективности принимаемых мер;
- взаимодействие с уполномоченными федеральными и региональными государственными органами в области защиты информации (ФСО России, ФСТЭК России, ФСБ России);
- организация исследований и анализа состояния защиты информации организации;
- организация учета конфиденциальной информации, циркулирующей в АИС, самих систем и других носителей (см. разд. 3.7);
- организация мониторинга и контроля эффективности защиты информации, циркулирующей в АИС, и самих систем (см. разд. 8.6);
- аттестация АИС на соответствие требованиям защиты информации, предусматривающей комплексную проверку (аттестационные испытания) в реальных условиях эксплуатации в целях оценки соответствия используемого комплекса мер и средств защиты требуемому уровню (см. разд. 8.7);
- планирование работ по созданию и совершенствованию систем защиты информации на конкретных объектах;

• управление защитой информации на конкретных объектах;

• анализ и прогнозирование потенциальных угроз для конкретных объектов (см. разд. 8.2);

• оценка возможного ущерба от реализации угроз;

• контроль эффективности принимаемых защитных мер и разбор случаев нарушения.

Для обеспечения информационной безопасности в организации создается служба (подразделение) информационной безопасности или отдельные должности штатного расписания организации, укомплектованные специалистами, ответственными за обеспечение информационной безопасности. Подразделение информационной безопасности может подчиняться непосредственно Службе безопасности организации или входить в состав подразделения информационных технологий. Варианты могут быть различными в зависимости наличия в организации Службы безопасности или Службы информационных технологий. Но в любом случае подразделение информационной безопасности должно быть предусмотрено штатным расписанием в целях обеспечения системы защиты электронного документооборота.

Специалисты подразделения информационной безопасности должны иметь необходимую квалификацию в области защиты информации и проходить периодическую переподготовку (повышение квалификации) в соответствии с программами послевузовского профессионального образования. Квалификационные характеристики главного специалиста по защите информации предусмотрены Квалификационным справочником должностей руководителей, специалистов и других служащих (см. приложение 9).

Для проведения работ по созданию и эксплуатации системы защиты электронного документооборота могут привлекаться специализированные организации (предприятия), имеющие лицензии и сертификаты на право проведения работ в области защиты информации.

Сертификация средств защиты информации регулируется Постановлением Правительства Российской Федерации от 12.02.1994 № 100 «Об организации работ по стандартизации, обеспечению единства измерений, сертификации продукции и услуг» и Постановлением Правительства Российской Федерации от 25.06.95 г. № 608 «О сертификации средств защиты информации».

Федеральным законом от 8 августа 2001 г. № 128-ФЗ «О лицензировании отдельных видов деятельности», ст. 17, п. 1, п.п. 5 – 13 определен перечень видов деятельности в области защиты информации, на осуществление которых требуются лицензии:

• деятельность по распространению шифровальных (криптографических) средств [80];

• деятельность по техническому обслуживанию шифровальных (криптографических) средств [Там же];

• предоставление услуг в области шифрования информации [там же];

• разработка, производство шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных систем, телекоммуникационных систем [Там же];

• деятельность по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя) [83];

• деятельность по разработке и (или) производству средств защиты конфиденциальной информации [86];

• деятельность по технической защите конфиденциальной информации [87];

• разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации, индивидуальными предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность [96];

• деятельность по изготовлению защищенной от подделок полиграфической продукции, в том числе бланков ценных бумаг, а также торговля указанной продукцией [85].

Подразделение информационной безопасности осуществляет свою деятельность в соответствии с разрабатываемым Положением о подразделении и выполняет основные задачи и функции по обеспечению защиты информации.

Защита информации при ее автоматизированной обработке производится на этапе эксплуатации автоматизированных информационных систем. При выполнении работ по защите информации следует учитывать организационные меры, обусловленные необходимостью проведения технического обслуживания, устранения неисправностей, обновления программного обеспечения и других мероприятий, задаваемых в соответствии с технологиями проведения эксплуатации систем защиты информации в АИС.

Организация и выполнение подготовительных работ по автоматизированной обработке конфиденциальной информации должны проводиться с учетом требований технологий разработки систем

защиты информации. Объектами защиты при этом являются: открытая, общедоступная информация и информация ограниченного доступа – это конфиденциальная информация, составляющая секрет производства, служебный секрет производства, служебную, коммерческую, профессиональную тайну, персональные данные и иные сведения, установленные российским законодательством, за исключением сведений, составляющих государственную тайну (см. гл. 1).

Объекты защиты АИС и циркулирующей в ней информации более подробно рассмотрены в разд. 3.7.

Определение и категорирование подлежащей защите информации осуществляет организация – заказчик создания и эксплуатации АИС в соответствии с действующим российским законодательством (см. гл. 1, приложения 2 и 3, Список источников и литературы), а также Перечня конфиденциальной документированной информации организации (см. разд. 2.3) и разрабатываемого или уже разработанного на его основе классификатора конфиденциальной информации системы (см. разд. 8.5.2, приложение 4).

Технологии и процессы автоматизированной обработки защищаемой конфиденциальной информации должны быть обеспечены стандартизованными машинными носителями информации, их накопителями, программно-техническими средствами глобальных и локальных вычислительных сетей и протоколами межведомственного (межсетевого) взаимодействия АИС.

8.2. Основные виды угроз информационной безопасности организации

Явление, действие или процесс, результатом которых могут быть утечка, хищение, утрата, искажение, подделка, уничтожение, модификация, блокирование информации, определяются как факторы, воздействующие на информацию. Существуют факторы объективные и субъективные, воздействующие на информацию, которые, в свою очередь, делятся на внутренние и внешние и которые определяются перечнями (см. приложение 3) в соответствии с ГОСТ Р 51275 – 99 [160].

Основными видами угроз информационной безопасности организации являются: противоправные действия третьих лиц, ошибочные действия пользователей и обслуживающего персонала, отказы и сбои программных средств, вредоносные программные воздействия на средства вычислительной техники и информацию.

Кроме действий человека (умышленные, ошибочные или случайные) источниками угроз информационной безопасности являются сбои и отказы программных и технических средств вычислительной техники, техногенные катастрофы, акты терроризма, стихийные бедствия и др.

Понятие «утечка» связано только с информацией ограниченного доступа (конфиденциальной) и в общем случае трактуется как выход ее из сферы обращения. Под утечкой понимается несанкционированный доступ (НСД) к информации, т. е. доступ в нарушение правил разграничения доступа к информации, которые устанавливает обладатель конфиденциальной информации или автоматизированной информационной системы, в которой эта информация циркулирует. При этом рассматривается только доступ к информации посредством применяемых в автоматизированных системах информационных технологий и непосредственный доступ к носителям информации.

В отличие от утечки информации блокирование, модификация, искажение и уничтожение объекта защиты могут произойти как вследствие несанкционированного доступа человека к информации, циркулирующей в АИС, так и по причинам, не зависящим от человека. При этом искажение и уничтожение объекта защиты, например изменение или замена программ управления вычислительным процессом, также могут привести к утечке информации.

НСД не всегда влечет за собой утечку, блокирование, искажение или уничтожение объекта защиты, что, в свою очередь, не всегда приводит к значимому ущербу. Тем не менее НСД к информации определяется как основополагающий фактор нарушения информационной безопасности при рассмотрении проблем обеспечения защиты информации и противодействия угрозам.

Угроза информационной безопасности может быть обусловлена только наличием уязвимостей объекта защиты. *Уязвимость* — это свойство АИС или ее компонентов, используя которое реализуются угрозы. Уязвимость возникает в основном, из-за недоработок или ошибок, содержащихся в продуктах информационных технологий, а также вследствие ошибок при проектировании автоматизированных информационных систем, которые могут привести к поведению, неадекватному целям обеспечения ее безопасности. Кроме того, уязвимости могут появляться в результате неправильной эксплуатации системы.

Для конкретной АИС как объекта защиты характерна своя совокупность угроз, зависящая от условий, в которых создается или функционирует система (табл. 8.1).

Таблица 8.1

Общий классификатор угроз безопасности информационно-коммуникационных технологий (конфиденциального электронного документооборота)

№ п/п	Классификационный признак угроз безопасности	Содержание классификатора
1	*2*	*3*
1	Источник угроз	Внешние Внутренние
2	Цель воздействия	Нарушение конфиденциальности Нарушение целостности Нарушение доступности Нарушение штатного режима функционирования
3	Принцип воздействия	Использование существующих (штатных) каналов доступа Использование скрытых каналов доступа Формирование новых каналов доступа
4	Способ воздействия	Нарушение структур данных Нарушение текстов, объектных и загрузочных кодов программ Нарушение функций общего программного обеспечения (ПО) Нарушение функций специального ПО Нарушение протоколов обмена данными или искажение информации в каналах связи
5	Характер воздействия	Активное воздействие (нарушение, разрушение, искажение) Пассивное воздействие (сбор информации, наблюдение, анализ) Интерактивный режим нарушителя с объектом (субъектом) доступа Воздействие при осуществлении информационно-вычислительного процесса обработки данных
6	Объект и субъект воздействия	Подчиненные подразделения Внешние абоненты — пользователи Обслуживающий персонал Лица, принимающие решения в органах управления

Продолжение табл. 8.1

1	*2*	*3*
7	Средства воздействия	Несанкционированный доступ Воздействие компьютерными вирусами Специальное программно-техническое воздействие Проявление недекларированных возможностей Имитовоздействие на информацию Побочные электромагнитные излучения и наводки Сбои и отказы в программах и техническом оборудовании, ошибки оператора (проявление непреднамеренных дефектов)
8	Используемая ошибка	Ошибки в организационно-технических мероприятиях Ошибки в проекте системы обеспечения безопасности информации Ошибки в выборе средств защиты информации (СЗИ) в соответствии с грифом защищаемой информации и характеристиками АИС Недостаточное качество средств защиты Ошибки в работе администратора локальной сети и администратора безопасности информации Ошибки в работе автоматизированных рабочих мест Ошибки и (или) недекларированные возможности в алгоритмах и программах Ошибки в структурах данных (использование избыточных, ложных или искаженных данных) Ошибки сертификационных испытаний
9	Состояние нарушаемых технологических процессов	Сбор, прием, передача данных, обмен информацией по сетям Осуществление информационно-вычислительного процесса Запись, считывание, хранение информации
10	Тип нарушения (нарушение конфиденциальности информации)	Несекретно Служебная, коммерческая, профессиональная тайны, персональные данные, секрет производства и др. (конфиденциальная информация)

Окончание табл. 8.1

1	*2*	*3*
11	По типу воздействия	Программное Программно-техническое Техническое Побочные электромагнитные излучения и наводки (радиоперехват и радиоэлектронное подавление)
12	Потенциальный ущерб	Низкий ущерб (несущественный, на уровне административных решений) Средний ущерб (требует материальных затрат) Высокий ущерб (значительный материальный ущерб) Катастрофический ущерб (ущерб на уровне затрат, приводящих к корректировке расходования бюджетных средств государства)
13	Соответствие требованиям к средствам защиты информации	Класс защищенности для автоматизированных систем Класс защищенности для средств вычислительной техники (СВТ) Класс защищенности для межсетевых экранов Класс защищенности для антивирусных средств Класс по контролю отсутствия недекларированных возможностей
14	Сценарии воздействия субъекта доступа	Внешний злоумышленник Санкционированный пользователь Санкционированный абонент удаленного доступа Зарегистрированный пользователь внешней системы Администратор АИС Администратор безопасности информации Программист-разработчик
15	Этапы жизненного цикла АИС	Технологические угрозы Эксплуатационные угрозы
16	Характер возникновения	Преднамеренные воздействия Непреднамеренные воздействия
17	Вид совершенного компьютерного преступления	Неправомерный доступ к компьютерной информации Создание, использование и распространение вредоносных программ Нарушение правил эксплуатации СВТ, АИС

8.3. Основные требования и меры по защите конфиденциальной информации, циркулирующей в эксплуатируемой автоматизированной информационной системе

8.3.1. Основные требования по защите конфиденциальной информации

Основные требования по защите информации должны основываться на положениях Федерального закона «Об информации, информационных технологиях и защите информации», РД «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)», РД «Автоматизированные системы. Защита от НСД к информации. Классификация АС и требования по защите информации» и других стандартах и руководящих документов. Эксплуатация АИС и системы защиты информации в ее составе также осуществляется в полном соответствии с утвержденной проектной, организационно-распорядительной и эксплуатационной документацией.

Требования по защите информации устанавливаются в зависимости от состава (категории) конфиденциальной информации и потенциальных угроз. При этом минимально необходимая совокупность требований по системе защиты ВЭД организации, или, иными словами, АИС и информации, циркулирующей в ней, устанавливается стандартами и руководящими документами.

В зависимости от состава (категории) информации и потенциальных угроз для определения требуемых мероприятий по защите информации, а также для минимизации затрат на защиту информации устанавливаются два уровня информационной безопасности АИС.

Первый (базовый) уровень информационной безопасности устанавливается для АИС, в которых обрабатывается общедоступная информация, второй уровень – для АИС, в которых циркулирует конфиденциальная информация, или, иначе, осуществляется конфиденциальный электронный документооборот.

Конкретные требования по защите информации и мероприятия по их выполнению определяются для АИС в целом в зависимости от уровня информационной безопасности, устанавливаемого объекту защиты.

Требования к информационной безопасности при организации взаимодействия системы МЭД и с ВЭД организации приведены в разд. 8.3.2. Общее описание организации взаимодействия этих систем приведено в приложении 8.

Требования по защите информации и мероприятия по их выполнению, а также конкретные средства защиты должны определяться и уточняться в зависимости от установленного класса защищенности на основании разрабатываемой модели угроз и действий нарушителя (см. разд. 8.2).

8.3.2. Основные технические требования к организации защищенного взаимодействия систем МЭД и ВЭД

Организация защищенного взаимодействия систем МЭД и ВЭД предусматривает максимальное использование программно-технических средств и возможность поэтапного подключения. Для организации взаимодействия используются следующие компоненты:

- *существующие компоненты* – системы ВЭД и МЭД;
- *внедряемый компонент* – шлюз системы МЭД (далее – шлюз), который является программно-техническим комплексом, выполняющим функции по обеспечению обмена электронными сообщениями с системой ВЭД и обеспечивающим хранение, просмотр, поиск и выгрузку (загрузку) электронных сообщений. Шлюз состоит из объединенных в локальную информационно-телекоммуникационную сеть сервера базы данных и автоматизированного рабочего места шлюза, в составе которого развертывается клиентское программное обеспечение комплекса программ «Почтовая служба системы».

Разрабатываемый компонент – адаптер ВЭД, который является специализированным программным обеспечением, разрабатываемым для каждого типа ВЭД (адаптер системы предназначен для преобразования передаваемых или получаемых данных, входящих в состав электронных сообщений, в формат представления данных, используемый в системе ВЭД, или в стандартный формат данных при обмене электронными сообщениями).

Требования к шлюзу. Программно-технические средства шлюза должны обеспечивать выполнение следующих функций:

- отправку и прием электронных сообщений с использованием клиентского комплекса программ «Почтовая служба»;
- хранение документов в электронном виде и их реквизитов;
- поиск хранимых документов в электронном виде по их реквизитам и просмотр как реквизитов, так и электронных образов документов;
- возможность выгрузки и загрузки документов и их реквизитов в электронном виде с использованием съемного носителя информации;

• обработка ошибок, протоколирование работы и минимальное разграничение доступа к данным и сервисам, предоставляемым шлюзом.

Требования к взаимодействию шлюза и адаптера системы ВЭД. Взаимодействие шлюза и адаптера системы ВЭД должно осуществляться с использованием сертифицированных средств защиты, обеспечивающих возможность обмена электронными сообщениями в автоматизированном режиме. При этом предусматривается размещение на технических средствах шлюза узла электронной почты, обеспечивающего передачу электронных сообщений участникам системы МЭД и между абонентами.

Требования к системе МЭД. Система должна обеспечивать:

• защищенный обмен электронными сообщениями между участниками системы МЭД;

• доставку электронных сообщений адресатам с отсылкой отправителю квитанций о времени их получения;

• целостность электронных сообщений;

• поддержку справочников (лиц, подписывающих документы (код), подразделений (код), адресатов документов (код) и т.д.);

• выгрузку электронных сообщений из комплекса программ «Почтовая служба» для последующей загрузки в систему ВЭД – получателей электронных сообщений;

• загрузку электронных сообщений из системы ВЭД в шлюз для последующей передачи адресатам с использованием комплекса программ «Почтовая служба».

Требования к системе ВЭД. Система должна обеспечивать возможность:

• хранения документов в электронной форме и их реквизитов;

• взаимодействия с адаптером системы ВЭД при отправке и приеме электронных сообщений.

Требования к информационной безопасности при организации взаимодействия системы МЭД с системой ВЭД. При организации взаимодействия указанных систем должна обеспечиваться антивирусная защита (ст. 9.8). Для защиты конфиденциальной информации должны использоваться сертифицированные по требованиям безопасности информации технические и (или) программные средства защиты информации. Автоматизированные рабочие места шлюза и выделенные персональные ЭВМ с адаптером системы ВЭД должны аттестовываться на соответствие требованиям технической защиты конфиденциальной информации (см. разд. 8.7). Требования по защите информации и мероприятия по их выполнению, а также конкретные средства защиты должны определяться и уточняться в зависимости от установленного класса защищенности на основании разрабатываемой модели угроз и действий нарушителя (см. разд. 8.2).

8.3.3. Основные меры по защите конфиденциальной информации

Защита информации АИС и самих систем различного уровня и назначения является неотъемлемой составной частью научной, производственной и управленческой деятельности организации — заказчика создания (эксплуатации) автоматизированной системы и осуществляется во взаимосвязи с другими мерами обеспечения защиты информации.

Обеспечение защиты, соответствующей уровню информационной безопасности объекта защиты, содержащего конфиденциальную информацию, должно предусматривать комплекс организационных, программных, технических средств и мер по защите информации ограниченного доступа и распространения.

К основным мерам защиты информации с ограниченным доступом относятся:

- выделение конфиденциальной информации, средств и систем защиты информации или их компонентов, подлежащих защите на основе ограничительных перечней конфиденциальной документированной информации (см. разд. 2.3), разрабатываемых в организации и в ее структурных подразделениях с учетом особенностей автоматизированной обработки информации, а также определение порядка отнесения информации к категории конфиденциальной;
- реализация разрешительной системы допуска исполнителей (пользователей, обслуживающего персонала, персонала других организаций) к работам, документам и информации с ограниченным доступом (см. гл. 4);
- ограничение доступа персонала и посторонних лиц в помещения, где размещены средства информатизации и коммуникации, на которых обрабатывается (хранится, передается) конфиденциальная информация, непосредственно к самим средствам информатизации и коммуникациям;
- разграничение доступа пользователей и обслуживающего персонала к информации, программным средствам обработки (передачи) и защиты информации;
- учет документов, информационных массивов, регистрация действий пользователей АИС и обслуживающего персонала, контроль за санкционированным и несанкционированным доступом и действиями пользователей, обслуживающего персонала и посторонних лиц;
- надежное хранение традиционных и машинных носителей информации, ключей (ключевой документации) и их обращение, исключающее их хищение, подмену, изменение (модификацию) и уничтожение;

• необходимое резервирование технических средств и дублирование массивов и носителей информации;

• использование сертифицированных средств защиты информации при обработке конфиденциальной информации ограниченного доступа;

• использование технических средств, удовлетворяющих требованиям стандартов по электромагнитной совместимости;

• проверка эффективности защиты технических средств и систем в реальных условиях их размещения и эксплуатации в целях определения достаточности мер защиты с учетом установленной категории;

• физическая защита помещений и собственно технических средств АИС с помощью сил охраны и технических средств, предотвращающих или существенно затрудняющих проникновение в здания, помещения посторонних лиц, хищение документов и информационных носителей;

• криптографическое преобразование информации, обрабатываемой и передаваемой средствами вычислительной техники и связи (при необходимости), определяемой особенностями функционирования конкретных автоматизированных систем;

• исключение возможности визуального (в том числе с использованием оптических средств наблюдения) несанкционированного просмотра обрабатываемой информации;

• предотвращение внедрения в автоматизированные системы программ-вирусов, программных закладок;

• использование волоконно-оптических линий связи для передачи конфиденциальной информации;

• использование защищенных каналов связи.

В целях дифференцированного подхода к защите информации, осуществляемого для разработки и применения необходимых и достаточных средств защиты информации, а также обоснованных мер по достижению требуемого уровня информационной безопасности, проводится классификация автоматизированных систем, обрабатывающих конфиденциальную информацию, либо разрабатываются профили защиты в соответствии с ГОСТ Р ИСО/МЭК 15408-1–2002 [152; 185]. *Профиль защиты* – это не зависящая от реализации совокупность требований безопасности для некоторой категории объекта оценки, отвечающая специфическим запросам потребителя.

Классификации подлежат все действующие, но ранее не классифицированные, а также разрабатываемые АИС, предназначенные для обработки информации с ограниченным доступом. Если си-

стема, классифицированная ранее, включается в состав вычислительной сети или системы и соединяется с другими техническими средствами линиями связи различной физической природы, то образующаяся при этом АИС более высокого уровня классифицируется в целом, а в отношении системы нижнего уровня классификация не производится.

Если объединяются автоматизированные системы различных классов защищенности, то интегрированная АИС должна классифицироваться по высшему классу защищенности входящих в нее систем, за исключением случаев их объединения посредством межсетевого экрана, когда каждая из объединяющихся автоматизированных систем может сохранять свой класс защищенности. Межсетевой экран представляет собой локальное (однокомпонентное) или функционально-распределенное средство (комплекс), реализующее контроль за информацией, поступающей в АИС и (или) выходящей из системы, и обеспечивающее ее защиту посредством фильтрации информации, т. е. ее анализа по совокупности критериев и принятия решения о ее распространении в (из) системы [198].

В соответствии с требованиями руководящих документов ФСТЭК России, конфиденциальная информация автоматизированной системы является объектом защиты. Определение объектов защиты проводится на предпроектной стадии, на этапах проектирования и приемо-сдаточных испытаний системы, а также в ходе инвентаризации и доработок, аттестационных испытаний и других контрольных мероприятий, проводимых в процессе эксплуатации АИС.

Категории конфиденциальной информации как объекта защиты устанавливаются до начала ее автоматизированной обработки, с использованием документально оформленного Перечня конфиденциальной документированной информации (КДИ) организации (см. разд. 2.3), за исключением государственной тайны, подлежащей защите в соответствии с законодательством Российской Федерации. Этот Перечень может носить обобщающий характер в области деятельности организации или иметь отношение к какому-либо отдельному направлению работ, связанному с созданием АИС. Все исполнители и, при необходимости, представители сторонних организаций, привлекаемых к проведению работ с использованием сведений конфиденциального характера, должны быть ознакомлены с этим Перечнем. При отсутствии в организации Перечня КДИ допускается разработка специализированного перечня для конкретной АИС организации или системы структурного подразделения.

Для идентификации и кодирования конфиденциальной информации при ее структурировании, автоматизированной обработке, в том числе в системах управления базами данных (СУБД), предусмотрен Классификатор конфиденциальной информации организации (см. разд. 8.5.2). Примерный классификатор конфиденциальной информации, содержащейся в АИС организации приведен в приложении 4.

Каждый реквизит таблицы базы данных, предназначенной для хранения конфиденциальной информации, должен иметь уникальный идентификатор.

В процессе автоматизированной обработки по завершении очередного установленного календарного периода (не менее года) эксплуатации организация (заказчик) организует определение текущего уровня защиты в целях контроля его соответствия требуемому уровню.

В организации разрабатываются документы (трудовые договоры, контракты, соглашения), регулирующие отношения между организацией – работодателем и ее работниками, организацией со сторонними организациями по порядку обращения с конфиденциальной информацией и ее обмена (приема-передачи) (см. гл. 4). Должностным лицам и работникам организации, использующим сведения конфиденциального характера, в организации обеспечиваются необходимые условия для соблюдения установленного порядка обращения с такой информацией при ее автоматизированной обработке.

Организация эксплуатации АИС и системы защиты информации в ее составе осуществляется в соответствии с установленным в организации порядком, в том числе в соответствии с инструкциями по эксплуатации системы защиты информации для пользователя, оператора, администратора системы, администратора безопасности.

Порядок обеспечения защиты информации в процессе эксплуатации, учитывающий особенности реализации АИС, технологии обработки информации и доступа исполнителей к ее техническим средствам, накопителям и носителям информации, определяется Инструкцией по защите информации организации, составленной на основании действующих документов ФСТЭК России, других стандартов и нормативных документов.

Ответственность за обеспечение защиты информации в процессе эксплуатации АИС возлагается на руководство эксплуатирующей организации и Службу безопасности или информационной безопасности. Подразделение информационной безопасности также может

входить, как уже говорилось, в состав подразделения по информационным технологиям организации. Ответственность за соблюдение установленных требований по защите информации при разработке АИС возлагается на непосредственных исполнителей.

8.3.4. Особенности и основные требования защиты персональных данных в АИС

В соответствии со ст. 19 Федерального закона «О персональных данных» Правительство Российской Федерации своим постановлением [82] установило требования к обеспечению безопасности персональных данных при их обработке в информационных системах. На основе данного постановления ФСТЭК России своим приказом [118] утвердило Положение о методах и способах защиты информации в информационных системах персональных данных, в котором не рассматриваются вопросы обеспечения безопасности персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну, а также вопросы применения криптографических методов и способов защиты информации. Анализ основных разделов и приложения данного Положения, показывает, что его можно применять не только для информационных систем персональных данных, но и для АИС, в которых циркулирует любая другая информация. Разделы Положения после тщательного анализа рассмотрены в приложении 10.

Работы по обеспечению безопасности персональных данных при их обработке в АИС являются неотъемлемой частью работ по созданию этих систем (см. разд. 8.4, а также ГОСТ 34.601–90 [180] и ГОСТ Р 51583–2000 [156]).

Требования по обеспечению безопасности и защиты персональных данных при их обработке в АИС представляют собой совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации.

Под техническими средствами, позволяющими обрабатывать персональные данные, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы 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 и др.), средства защиты информации, применяемые в АИС.

Безопасность персональных данных при их обработке в АИС обеспечивается с помощью системы защиты, включающей как организационные меры, так и технические, программные средства, которые должны удовлетворять устанавливаемым требованиям, обеспечивающим защиту информации (см. разд. 8.1.1, приложение 10). Средства защиты информации включают в себя также: шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа и утечки информации по техническим каналам, средства предотвращения программно-технических воздействий на технические средства обработки персональных данных, а также информационные технологии, используемые в АИС персональных данных.

Для обеспечения безопасности персональных данных при их обработке в АИС, осуществляется защита речевой информации и информации, обрабатываемой техническими средствами, а также информации, представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитно-оптической и иной основе (см. приложение 10, разд. III).

Обмен персональными данными при их обработке в АИС осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) применения технических средств (см. приложение 10, разд. III).

Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, соблюдения условий безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц. Возможные каналы утечки информации при обработке персональных данных в информационных системах определяются ФСТЭК России, ФСБ России и ФСО России в пределах их полномочий [63–65].

Безопасность персональных данных при их обработке в АИС обеспечивает оператор или лицо, которому на основании договора оператор поручает обработку персональных данных. Существенным условием договора является обязанность уполномоченного лица обеспечить конфиденциальность персональных данных и их безопасность при обработке в информационной системе.

При обработке персональных данных в АИС должны быть обеспечены:

• проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

• своевременное обнаружение фактов несанкционированного доступа к персональным данным;

• недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

• возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

• постоянный контроль за обеспечением уровня защищенности персональных данных.

Мероприятия по обеспечению безопасности персональных данных при их обработке в АИС включают в себя:

• определение угроз информационной безопасности персональных данных при их обработке, формирование на их основе модели угроз (см. разд. 8.2, приложение 3);

• разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса АИС (см. приложение 10, разд. VI);

• проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

• установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

• обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

• учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных (см. разд. 3.7);

• учет лиц, допущенных к работе с персональными данными в АИС;

• контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

• разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к на-

рушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, а также разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

• описание системы защиты персональных данных.

Для разработки и осуществления мероприятий по обеспечению безопасности персональных данных при их обработке оператором или уполномоченным лицом может назначаться структурное подразделение или должностное лицо (работник), ответственные за обеспечение безопасности персональных данных.

Должностные лица допускаются для выполнения служебных (трудовых) обязанностей к соответствующим данным на основании списка, утвержденного оператором АИС или уполномоченным лицом.

Запросы пользователей информационной системы на получение персональных данных, включая лиц, доступ которых необходим для выполнения служебных (трудовых) обязанностей, а также факты предоставления персональных данных по этим запросам регистрируются автоматизированными средствами системы в электронном журнале обращений. Содержание электронного журнала обращений периодически проверяется соответствующими должностными лицами (работниками) оператора или уполномоченного лица.

При обнаружении нарушений порядка предоставления персональных данных оператор или уполномоченное лицо незамедлительно приостанавливают предоставление персональных данных пользователям АИС до выявления причин нарушений и устранения этих причин.

Реализация требований по обеспечению информационной безопасности в средствах защиты информации возлагается на их разработчиков.

В отношении разработанных шифровальных (криптографических) средств защиты информации, предназначенных для обеспечения безопасности персональных данных, проводятся тематические исследования и контрольные тематические исследования в целях проверки выполнения требований по безопасности информации. При этом под тематическими исследованиями понимаются криптографические, инженерно-криптографические и специальные исследования средств защиты информации и специальные работы с техническими средствами АИС, а под контрольными тематическими исследованиями – периодически проводимые тематические исследования (см. разд. 8.6; 8.7). Конкретные сроки проведения контрольных тематических исследований определяются ФСБ России.

Результаты соответствия и (или) тематических исследований средств защиты информации, предназначенных для обеспечения безопасности персональных данных, оцениваются в ходе экспертизы, осуществляемой ФСБ России и ФСТЭК России в пределах их полномочий.

К средствам защиты информации, предназначенным для обеспечения безопасности персональных данных, прилагаются правила пользования этими средствами, согласованные с ФСБ России и ФСТЭК России в пределах их полномочий.

Средства защиты информации, предназначенные для обеспечения безопасности персональных данных, подлежат учету с использованием индексов или условных наименований и регистрационных номеров. Перечень индексов, условных наименований и регистрационных номеров определяется ФСБ России и ФСТЭК России.

Порядок разработки, производства, реализации и эксплуатации шифровальных (криптографических) средств защиты информации и предоставления услуг по шифрованию персональных данных при их обработке в информационных системах устанавливаются ФСБ России.

Автоматизированные информационные системы персональных данных должны классифицироваться операторами – государственными органами, муниципальными органами, юридическими или физическими лицами, организующими и (или) осуществляющими обработку персональных данных, а также определяющими цели и содержание обработки персональных данных в зависимости от объема обрабатываемых ими персональных данных и угроз безопасности жизненно важным интересам личности, общества и государства. Порядок проведения классификации информационных систем персональных данных установлен совместно ФСТЭК России, ФСБ России и Министерством информационных технологий и связи Российской Федерации.

Проведение классификации АИС персональных данных включает в себя следующие этапы:

- сбор и анализ исходных данных по информационной системе;
- присвоение системе соответствующего класса и его документальное оформление [122; 166, 200].

При проведении классификации учитываются такие исходные данные как:

- категория обрабатываемых в системе персональных данных – $X_{\text{пд}}$;

• объем обрабатываемых персональных данных (количество субъектов, персональные данные которых обрабатываются в системе) – $X_{\text{нпд}}$;

• заданные оператором характеристики безопасности персональных данных, обрабатываемых в системе;

• структура системы;

• наличие подключений информационной системы к сетям связи общего пользования и (или) сетям международного информационного обмена;

• режим обработки персональных данных;

• режим разграничения прав доступа пользователей АИС;

• местонахождение технических средств информационной системы.

Определяются следующие категории обрабатываемых в информационной системе персональных данных ($X_{\text{пд}}$):

• категория 1 – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;

• категория 2 – персональные данные, позволяющие идентифицировать субъекта этих данных и получить о нем дополнительную информацию, за исключение данных, относящихся к категории 1;

• категория 3 – персональные данные, позволяющие идентифицировать субъекта этих данных;

• категория 4 – обезличенные и (или) общедоступные персональные данные.

Категории персональных данных $X_{\text{нпд}}$ могут принимать следующие значения:

1 – в системе одновременно обрабатываются персональные данные более чем 100 000 физических лиц или в пределах субъекта Российской Федерации или Российской Федерации в целом;

2 – в системе одновременно обрабатываются персональные данные от 1000 до 100 000 физических лиц или работающих в отрасли экономики Российской Федерации, в органе государственной власти, проживающих в пределах муниципального образования;

3 – в системе одновременно обрабатываются данные менее чем 1000 физических лиц или персональные данные субъектов в пределах конкретной организации.

В зависимости от характеристик безопасности персональных данных, обрабатываемых в АИС, информационные системы подразделяются на типовые и специальные. *Типовые АИС* – это систе-

мы, в которых требуется обеспечение только конфиденциальности персональных данных. *Специальные АИС* – это системы, в которых вне зависимости от необходимости обеспечения конфиденциальности персональных данных требуется обеспечить хотя бы одну из характеристик их безопасности, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий).

Специальные АИС, в свою очередь, подразделяются на два типа:

1) системы, в которых обрабатываются персональные данные, касающиеся состояния здоровья их субъектов;

2) системы, в которых предусмотрено принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении физического лица или иным образом затрагивающих его права и законные интересы.

По структуре АИС подразделяются на три типа:

1) на автономные (не подключенные к иным информационным системам) комплексы технических и программных средств, предназначенные для обработки персональных данных (АРМ);

2) комплексы АРМ, объединенных в единую информационную систему средствами связи без использования технологии удаленного доступа (локальные системы);

3) комплексы АРМ и (или) локальных систем, объединенных в единую информационную систему средствами связи с использованием технологии удаленного доступа (распределенные информационные системы).

По наличию подключений к сетям связи общего пользования и (или) сетям международного информационного обмена АИС подразделяются на системы, имеющие подключения, и системы, не имеющие подключений. В зависимости от режима обработки персональных данных АИС подразделяются на системы одно- и многопользовательские. По разграничению прав доступа пользователей АИС подразделяются на системы без разграничения прав доступа и системы с разграничением прав доступа.

В зависимости от местонахождения технических средств АИС подразделяются на системы, все технические средства которых находятся в пределах Российской Федерации, и системы, технические средства которых частично или целиком находятся за пределами Российской Федерации.

По результатам анализа исходных данных типовой информационной системе присваивается один из следующих классов:

• класс 1 (К1) – системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов персональных данных;

• класс 2 (К2) – системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к средним негативным последствиям для субъектов персональных данных;

• класс 3 (К3) – системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов персональных данных;

• класс 4 (К4) – системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, не приводит к негативным последствиям для субъектов персональных данных.

Класс типовой информационной системы определяется в соответствии с табл. 8.2.

Таблица 8.2

Класс типовой информационной системы

$X_{пд}$ / $X_{нпд}$	3	2	1
Категория 4	К4	К4	К4
Категория 3	К3	К3	К2
Категория 2	К3	К2	К1
Категория 1	К1	К1	К1

По результатам анализа исходных данных класс специальной АИС определяется на основе модели угроз безопасности персональных данных (см. разд. 8.2).

В случае выделения в составе АИС подсистем, каждая из которых является информационной системой, всей АИС в целом присваивается класс, соответствующий наиболее высокому классу входящих в нее подсистем.

Результаты классификации АИС оформляются соответствующим актом оператора. Класс АИС может быть пересмотрен:

• по решению оператора на основе проведенных им анализа и оценки угроз безопасности персональных данных с учетом особенностей и (или) изменений конкретной системы;

• по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности персональных данных при их обработке в информационной системе.

8.3.5. Примерный состав и функции службы комплексного администрирования АИС

Служба комплексного администрирования АИС обеспечивает администрирование: защиты информации, операционных систем и сетей (локальных и глобальных вычислительных систем и сетей), баз данных и систем управления базами данных.

Администратор защиты информации обеспечивает: регистрацию пользователей; формирование матрицы доступа к вычислительным и информационным ресурсам системы; учет наступления системных событий, связанных с инициализацией функций АИС, изменением ее конфигурации, а также изменением прав доступа; формирование параметров входа в систему (идентификатора) и шифрключей; контроль системы текущего функционального состояния.

Администратор операционных систем отвечает за генерацию операционных систем и их сопровождение (тестирование работоспособности, восстановление и т. д.), обновление версий операционных систем (анализ необходимости перехода на новые версии, разработку перечня мероприятий по переходу на новую версию).

Администратор сети отвечает за ее функционирование, создает структуру каталога сети; обеспечивает необходимый уровень защиты, следит за рациональным использованием информационных ресурсов, определяет политику развития сети, ведет описание технической конфигурации сети, ее функциональной структуры, структуры клиентов, имеющих доступ к информации, циркулирующей в АИС, а также формирует список пользователей, допущенных к работе в системе.

Администратор баз данных отвечает за генерацию систем управления базами данных; сопровождение информации и управление информацией, в том числе конфиденциальной; создание и ведение классификаторов; ввод и модификацию нормативно-справочной информации; сохранение резервных копий; восстановление искаженной информации; архивирование информации и организацию поступления информации из архива; обработку и анализ статистической информации о характере и интенсивности использования данных, о распределении нагрузки на различные компоненты структуры баз данных; внесение изменений в структуру баз данных в процессе эксплуатации системы в целях повышения производительности; обеспечивает ввод и поддержание в актуальном состоянии общих разделов баз данных (классификаторов).

При увольнении или изменении должностных обязанностей пользователей, операторов, администраторов систем по согласованию со Службой безопасности или Службой информационных технологий

(информационной безопасности) организации должны быть приняты в установленном в организации порядке меры по оперативному изменению соответствующих паролей. Порядок ведения паролей необходимо определить Инструкцией по использованию паролей.

Восстановление функционирования АИС и обеспечение доступности к конфиденциальной информации на требуемом уровне и в требуемые сроки после прерывания или отказа оборудования и (или) программного обеспечения осуществляется в соответствии с порядком, указанным в эксплуатационной документации. Неисправности должны регистрироваться, анализироваться, и в их отношении должны приниматься соответствующие действия.

Резервное копирование (архивирование) баз данных осуществляется в соответствии с планом проведения резервного копирования (архивирования), который включает перечень баз данных, подлежащих резервному копированию (архивированию), и график его проведения.

Эксплуатация антивирусных средств защиты осуществляется в соответствии с разрабатываемой в организации Инструкцией по антивирусной защите, определяющей порядок установки, обновления, использования антивирусных средств защиты, а также меры по восстановлению работоспособности системы в случае проникновения вируса. Инструкция может быть составлена на основании [165; 196].

Все пользователи и эксплуатационный персонал АИС должны сообщать в Службу безопасности (информационной безопасности) о любых наблюдаемых или предполагаемых событиях, связанных с недостатками обеспечения защиты конфиденциальной информации.

За нарушение установленных требований по защите информации руководитель структурного подразделения организации, отвечающий за эксплуатацию АИС (подразделение информационных технологий), и (или) непосредственный исполнитель привлекаются к административной или уголовной ответственности в соответствии с действующим российским законодательством (см. приложение 6).

Доступ к защищаемой конфиденциальной информации лиц, работающих в автоматизированной системе, производится в соответствии с порядком, установленным разрешительной системой доступа (гл. 4).

Все виды работ, связанных с автоматизированной обработкой информации, проводятся в регламентном режиме или по разовым запросам непосредственно пользователями или операторами. В последнем случае должны быть определены лица, имеющие право подписывать разовые запросы на обработку информации. Перечень

регламентных работ и их исполнители определяются соответствующей организационно-распорядительной и эксплуатационной документацией.

На период обработки защищаемой информации в помещениях, где размещаются необходимые для этого средства, могут находиться только лица, допущенные к обрабатываемой информации в установленном порядке. Допуск в эти помещения других лиц для проведения профилактических или ремонтных работ может осуществляться только с санкции руководителя организации или руководителя структурного подразделения, эксплуатирующего определенную тематику, по согласованию со Службой безопасности или Службой информационных технологий (информационной безопасности) организации. При этом должны быть соблюдены меры, исключающие их ознакомление с конфиденциальной информацией.

В целях исключения предоставления доступа к излишнему объему информации в процессе эксплуатации АИС должен осуществляться периодический пересмотр прав доступа пользователей к информации.

В случае размещения в одном помещении различных технических средств одной или нескольких автоматизированных систем должен быть исключен несанкционированный просмотр конфиденциальной информации. Учет, хранение накопителей и носителей информации на бумажной, магнитной, оптической и иной основе и обращение с ними должны осуществляться в соответствии с требованиями, изложенными в документе «Порядок хранения накопителей и носителей информации и обращения с ними».

Запись конфиденциальной информации в незашифрованном виде производится только на предварительно учтенные накопители и носители информации, а в зашифрованном — с помощью сертифицированных средств криптографической защиты информации.

Распечатка на принтере (вывод на графопостроитель) конфиденциальной информации может осуществляться двумя способами: либо на предварительно учтенном бумажном носителе (см. разд. 2.4), либо на неучтенном бумажном носителе с использованием сертифицированных средств защиты информации, реализующих печать учетных реквизитов, полученных предварительно.

По окончании обработки конфиденциальной информации пользователь (оператор) обязан произвести стирание информации в оперативной памяти путем выключения питания компьютера, если иное не предусмотрено технологическим процессом.

Контроль за состоянием и эффективностью защиты конфиденциальной информации осуществляется Службой информационных технологий (информационной безопасности), Службой безопасно-

сти организации, отраслевыми и федеральными органами контроля и заключается в оценке выполнения требований нормативных документов, обоснованности принятых мер и проверке соблюдения норм защиты конфиденциальной информации. Вопросы обеспечения контроля за АИС и циркулирующей в ней конфиденциальной информации, иными словами защиты электронного документооборота рассмотрено в разд. 8.6.

8.4. Организация работ при создании системы защиты электронного документооборота

8.4.1. Основные требования по разработке системы защиты информации

Организация, — заказчик автоматизированной информационной системы должна выполнить на основании ряда руководящих документов комплекс мероприятий по защите конфиденциальной информации соответствующей категории, исходя из требуемого уровня информационной безопасности объекта защиты, задаваемого на стадии создания автоматизированной системы.

Разработка АИС и системы защиты информации в ее составе может осуществляться как самой организацией, так и специализированными предприятиями, имеющими лицензию на соответствующий вид деятельности в области защиты информации (см. разд. 8.1).

Организация работ по защите информации возлагается на руководителя организации, руководителей подразделений, разрабатывающих и эксплуатирующих АИС, Службы информационных технологий (подразделения информационной безопасности), а контроль за обеспечением защиты информации – на руководителя Службы безопасности, если она за это ответственна.

Если разработка системы защиты информации или ее отдельных составляющих производится специализированным предприятием в организации-заказчике, определяются подразделения (или отдельные специалисты), ответственные за проведение (внедрение и эксплуатацию) мероприятий по защите информации.

Разработка и внедрение системы защиты информации должны осуществляться разработчиком совместно со Службой безопасности организации и Службой информационных технологий (информационной безопасности), принимающими участие в подготовке методического руководства и конкретных требований по защите информа-

ции, аналитического обоснования необходимости создания системы защиты информации, в выборе средств вычислительной техники и связи, средств защиты, в организации работ по выявлению возможностей и предупреждению утечки и нарушения целостности защищаемой информации, в согласовании технических заданий на проведение работ, а также в проведении аттестации АИС (см. разд. 8.7).

8.4.2. Стадии и этапы разработки системы защиты конфиденциальной информации

Автоматизированные информационные системы, обеспечивающие защиту информации ограниченного распространения, могут создаваться по одному из трех типовых сценариев: первый – в действующую АИС, предназначенную для обработки открытой информации, добавляют функцию защиты, позволяющую обеспечивать обработку информации ограниченного распространения; второй – АИС создается, так сказать, «с нуля», где вместе с прикладной обрабатывающей системой сопрягается на стадии разработки система защиты; третий – реализуется типовой проект. Естественно, последний сценарий самый простой в реализации и мы не будем его рассматривать. Более сложным является второй сценарий, который предусматривает набор и стыковку прикладного обеспечения, с одной стороны, и систем защиты с базовыми операционными системами и базами данных – с другой.

Опыт создания АИС с обеспечением защиты информации показывает следующее. Самые безопасные АИС – это те, которые не работают, т.е. не реализуют никаких прикладных функций. Самыми опасными являются те АИС, которые позволяют осуществлять пользователю любые действия и использовать любое программное обеспечение. Мы видим два полюса противоречий: полная безопасность и полная свобода действий пользователя. Естественно, реально возможными оказываются АИС, в которых соблюден баланс между безопасностью и применением достаточного объема прикладного программного обеспечения, отвечающего требованиям безопасности обработки информации.

Поиск АИС, позволяющей сбалансировать указанные противоречия, является основой диалектической составляющей процесса построения информационно-защищенных систем. Как правило, поиск баланса осуществляется на основе компромисса между ограничениями на функциональные возможности программного обеспечения и переносом части функций безопасности из технических реали-

заций в организационные меры. Несмотря на определенную сложность второго сценария построения защищенных АИС, стоимость его реализации оказывается существенно ниже, чем построение защищенной АИС по первому сценарию, т.е. на основе уже действующей незащищенной. В последнем случае требуется, как правило, доработка или переработка действующих программ, а также создание новых средств обеспечения информационной безопасности.

Как при втором, так и при третьем сценарии создания защищенных АИС можно выделить следующие стадии и этапы разработки. Разница будет заключаться в сложности, а следовательно, и в стоимости реализации этапов.

Существуют следующие стадии создания системы защиты АИС и циркулирующей в ней конфиденциальной информации или, другими словами, электронного конфиденциального документооборота:

- предпроектная, включающая предпроектное обследование объекта информатизации, разработку аналитического обоснования необходимости создания системы защиты информации и технического (частного технического) задания на ее создание;
- проектирования (разработки проектов) и реализации АИС, включающая разработку системы защиты информации в ее составе;
- ввода в действие системы защиты информации, включающая опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также аттестацию АИС на соответствие требованиям информационной безопасности.

Предпроектное обследование может быть поручено специализированному предприятию, имеющему соответствующую лицензию, но и в этом случае анализ информационного обеспечения в части состава и структуры конфиденциальной информации целесообразно выполнять представителям организации-заказчика при методической помощи специализированного предприятия. На этой стадии разрабатываются аналитическое обоснование и техническое задание на создание системы или частное техническое задание на подсистему информационной безопасности АИС.

На предпроектной стадии по обследованию объекта, для которого создается АИС, определяются:

- (уточняются) угрозы безопасности информации – факторы, влияющие на конфиденциальную информацию (см. разд. 8.2 и приложение 3);
- модель вероятного нарушителя применительно к конкретным условиям функционирования АИС (см. разд. 8.2 и приложение 3);
- необходимость обработки конфиденциальной информации в АИС, оцениваются ее объемы, характер и условия использования;

• конфигурация и топология АИС в целом и ее отдельных составляющих, а также физические, функциональные и технологические связи как внутри разрабатываемой системы, так и с другими АИС;

• технические средства и системы, предполагаемые к использованию в разрабатываемой АИС, условия их расположения, общесистемные и прикладные программные средства, имеющиеся на рынке и предлагаемые к разработке;

• режимы обработки конфиденциальной информации в АИС;

• данные и компоненты АИС, которые являются важными и должны дублироваться;

• класс защищенности АИС;

• степень участия персонала в обработке (передаче, хранении) конфиденциальной информации, характер их взаимодействия между собой и со Службой информационных технологий (информационной безопасности), а также Службой безопасности организации;

• мероприятия по защите информации в процессе разработки системы.

По результатам предпроектного обследования разрабатывается аналитическое обоснование необходимости создания системы защиты конфиденциальной информации, которое должно содержать:

• информационную характеристику создаваемой АИС и организационную структуру, для которой система создается;

• характеристику комплекса технических средств, программного обеспечения, режимов работы, технологического процесса обработки информации;

• перечень угроз информационной безопасности и мероприятий по их предупреждению и предотвращению (см. разд. 8.2 и приложение 3);

• перечень предлагаемых к использованию сертифицированных средств защиты или обоснование необходимости их разработки (адаптации под конкретные условия функционирования АИС);

• обоснование необходимости привлечения специализированных предприятий для разработки системы защиты информации;

• оценку материальных, трудовых и финансовых затрат на разработку и внедрение системы защиты информации;

• ориентировочные сроки разработки и внедрения системы защиты информации;

• перечень мероприятий по обеспечению конфиденциальности информации при создании АИС.

Аналитическое обоснование подписывается руководителем предпроектного обследования, согласовывается с разработчиком АИС, руководителями Службы информационных технологий (инфор-

мационной безопасности) и Службы безопасности организации-заказчика, после чего утверждается руководителем этой организации.

Результаты предпроектного обследования в части наличия конфиденциальной информации должны базироваться на документально оформленном Перечне конфиденциальной документированной информации (см. разд. 2.3). Конфиденциальность исходной информации, подлежащей автоматизированной обработке, а также выходной информации, получаемой в результате обработки, определяется организацией – заказчиком АИС на основании Перечня конфиденциальной документированной информации и документально, за подписью руководителя организации, представляется разработчику системы защиты информации.

В целях определения конфиденциальности промежуточной информации, циркулирующей (обрабатываемой, хранимой и передаваемой) в АИС, а также оценки достаточности предлагаемых средств и мер защиты информации приказом по организации создается экспертная комиссия, в состав которой включаются представители организации – заказчика и предприятия – разработчика АИС.

Экспертная комиссия может проводить свою работу в несколько этапов и при этом рассматривает аналитическое обоснование, техническое задание, проектную и эксплуатационную документацию, а также устанавливает конфиденциальность информации, подлежащей обработке, в том числе накопителей, носителей и массивов информации, предложенной организацией – заказчиком и разработчиком АИС. Правильность и обоснованность сроков хранения накопителей и носителей информации и их рассылки, достаточность предлагаемых мер защиты должны соответствовать Перечню конфиденциальной документированной информации (см. разд. 2.3) и Реестру конфиденциальной информации и АИС (см. разд. 3.7.1). Результатом работы Экспертной комиссии является заключение, утверждаемое руководителем организации, при которой она создана.

На стадии ввода в действие АИС и системы защиты информации в ее составе осуществляются:

- опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе АИС и отработки технологического процесса обработки (передачи) информации;
- приемо-сдаточные испытания средств защиты информации по результатам опытной эксплуатации с оформлением приемо-сдаточного акта, подписываемого разработчиком и заказчиком;
- аттестация АИС на соответствие требованиям безопасности информации (см. разд. 8.7).

На этой стадии оформляются: акты внедрения средств защиты информации по результатам их приемо-сдаточных испытаний; предъявительский акт о проведении аттестационных испытаний; заключение по результатам аттестационных испытаний; аттестат соответствия.

Эксплуатация АИС осуществляется на основе утвержденной организационно-распорядительной и эксплуатационной документации.

Состояние и эффективность защиты информации контролируются службой информационных технологий (информационной безопасности), Службой безопасности организации-заказчика, отраслевыми и федеральными органами контроля. По результатам контроля дается оценка выполнению требований нормативных документов, обоснованности принятых мер и проверке соблюдения норм защиты конфиденциальной информации (см. разд. 8.6).

8.5. Организация проведения работ по защите конфиденциальной информации при ее автоматизированной обработке

8.5.1. Общие положения

Для защиты конфиденциальной информации, циркулирующей в АИС, от несанкционированного доступа, за исключением систем, использующих информационную технологию со съемными накопителями информации большой емкости, должны использоваться сертифицированные по требованиям информационной безопасности программные (программно-аппаратные) средства защиты информации.

Для защиты конфиденциальной информации от утечки по техническим каналам рекомендуется использовать сертифицированные по защите информации средства вычислительной техники либо средства, удовлетворяющие требованиям стандартов по электромагнитной совместимости.

Для передачи информации за пределы контролируемой зоны организации необходимо использовать защищенные линии связи, в том числе волоконно-оптические, оборудованные средствами защиты информации, либо предназначенные для этого средства криптографической защиты информации, например электронную цифровую подпись. Накопители и носители информации на бумажной, магнитной (магнитооптической) и иной основе должны учитываться и храниться в установленном порядке (см. разд. 3.7).

Доступ пользователей к конфиденциальной информации осуществляется в соответствии с разрешительной системой допуска исполнителей к документам и сведениям конфиденциального характера, действующей в организации (см. гл. 4).

Требования по защите конфиденциальной информации при ее автоматизированной обработке для различных видов АИС имеют свои особенности, зависящие от технической реализации средств обработки данных. Так, в зависимости от технологии защиты информации, циркулирующей в системе и технической реализации средств обработки данных определяются АИС уровня: автоматизированного рабочего места; локальной вычислительной сети; распределенной информационно-коммуникационной системы, а также сочетания АИС систем МЭД и ВЭД, определяющие обмен конфиденциальной информацией.

8.5.2. Классификатор конфиденциальной информации

Классификатор конфиденциальной информации (далее — Классификатор) как документ предназначен для классификации и кодирования конфиденциальной информации, циркулирующей в АИС, или, иными словами, конфиденциального электронного документооборота.

Классификатор составляется на основании нормативно-правовых и нормативно-технических документов в области информационной безопасности и защиты информации, содержащей сведения конфиденциального характера, с учетом методов кодирования информации. Он служит также исходной информацией для программистов и специалистов по информационным технологиям, осуществляющих работы по созданию и эксплуатации АИС.

Классификатор оперирует основными видами конфиденциальной информации в соответствии с Указом Президента Российской Федерации «Об утверждении перечня сведений конфиденциального характера» [68] и нормативной правовой базой, рассмотренной в гл. 1.

Виды конфиденциальной информации являются объектами классификации, поэтому структурное описание объекта классификации включает три блока: идентификации; наименования и примечаний [66; 182].

Блок идентификации строится с использованием иерархического метода классификации и последовательного метода кодирования. Три уровня иерархической классификации объектов выделяют:

• укрупненные группы видов конфиденциальной информации;
• подгруппы видов конфиденциальной информации;
• виды конфиденциальной информации. Укрупненные группы и подгруппы объединяют совокупности видов конфиденциальной информации. Виды конфиденциальной информации выделяют в рамках групп (подгрупп).

Структура кодового обозначения включает три цифровых десятичных знака и имеет следующий вид:

XXX — три знака.

Первый знак соответствует укрупненным группам видов конфиденциальной информации; второй – подгруппе видов конфиденциальной информации (при отсутствии подгруппы этот знак не рассматривается, имеет значение «0» или может быть использован для идентификации вида конфиденциальной информации); третий – виду конфиденциальной информации.

В случае, если при использовании Классификатора в нем отсутствует необходимый вид (виды) конфиденциальной информации, ему присваивается знак «9» — «Прочие виды информации». *Блок наименований* содержит наименования укрупненных групп, подгрупп и видов конфиденциальной информации. Для удобства пользования наименования укрупненных групп в блоке наименований выделяются полужирным шрифтом, а наименования подгрупп – курсивом.

Блок примечаний служит для размещения сведений, поясняющих и уточняющих при необходимости содержание блока наименований. Кодирование информации с помощью Классификатора выполняется в организациях в ходе работ по учету конфиденциальной информации и ведению Реестра конфиденциальной информации и АИС (см. разд. 3.7).

Примерный Классификатор конфиденциальной информации, содержащейся в АИС организации, приведен в приложении 4.

8.5.3. Особенности защиты конфиденциальной информации на автоматизированных рабочих местах на базе автономных персональных ЭВМ

Автоматизированные рабочие места на базе автономных персональных ЭВМ, включая мобильные, например, ноутбуки, – это автоматизированные информационные системы, обладающие всеми их основными признаками. Информационным каналом обмена между такими АИС являются в основном съемные накопители и носители информации на различной основе: магнитные, магнитоопти-

ческие, лазерные диски и кассеты с магнитной лентой, электронные USB-накопители, карты памяти, а также носители на традиционной бумажной основе (ввод через сканер). Автономные персональные ЭВМ (компьютеры) могут содержать также средства беспроводной связи: радио- и инфракрасной связи. Такой канал информационного обмена не должен использоваться средствами вычислительной техники, на которых обрабатывается конфиденциальная информация. В связи с этим порядок разработки и эксплуатации АРМ на базе автономных компьютеров по составу и содержанию проводимых работ по защите информации, организационно-распорядительной, проектной и эксплуатационной документации должны полностью отвечать требованиям по защите информации АИС.

Технология съемных накопителей информации большой емкости для АРМ на базе автономных компьютеров предусматривает установку на съемном накопителе информации большой емкости одновременно общесистемной системы управления базами данных и прикладного программного обеспечения, а также запись на него данных (обрабатываемой информации) для одного пользователя или группы. Для обмена информацией с другими АРМ и архивирования информации могут использоваться носитель на гибких магнитных дисках и второй накопитель информации большой емкости. При этом все используемые на АРМ накопители информации должны быть учтены как «Для служебного пользования».

Все другие несъемные накопители информации должны быть исключены из состава компьютера, а неиспользуемые порты (интерфейсы) – из конфигурации компьютера любым способом, предотвращающим обращение к ним.

Основной особенностью применения данной информационной технологии для АРМ на базе автономных персональных ЭВМ с точки зрения защиты информации является исключение этапа хранения на них в нерабочее время информации, подлежащей защите. Эта особенность может быть использована для обработки конфиденциальной информации без применения сертифицированных средств защиты информации от несанкционированного доступа и без использования технических средств охраны для помещений, в которых размещены такие АРМ.

С использованием данной информационной технологии на АРМ может быть создано несколько АИС для обработки конфиденциальной и общедоступной информации в зависимости от используемых съемных накопителей информации большой емкости.

Условия и порядок применения такой процедуры должны быть отражены в технологии обработки информации, использующей съемные накопители информации большой емкости.

8.5.4. Особенности защиты информации в локальных вычислительных сетях

Характерными особенностями локальной вычислительной сети (ЛВС) являются распределенные по узлам сети данные и файлы, предназначенные для хранения, обработки и передачи (включая электронную почту). Это усложняет проведение контроля за работой пользователей и состоянием общей информационной безопасности сети. Средства защиты информации от несанкционированного доступа должны использоваться во всех узлах ЛВС, независимо от конфиденциальности обрабатываемой в узле информации, и требуют постоянного квалифицированного сопровождения со стороны администратора информационной безопасности.

Для управления ЛВС и распределения системных ресурсов в сети, включая управление средствами защиты конфиденциальной информации, в дополнение к администраторам АИС должны быть назначены администраторы информационной безопасности, имеющие необходимые привилегии доступа к защищаемой информации ЛВС. Состав пользователей ЛВС должен устанавливаться по приказу руководителя организации (структурного подразделения организации) в установленном порядке и строго контролироваться. Все изменения состава пользователей, их прав и привилегий должны регистрироваться.

Каждый администратор и пользователь должен иметь уникальные идентификаторы и пароли, а в случае использования средств криптографической защиты информации – ключи шифрования для криптографических средств, используемых для защиты информации при передаче ее по каналам связи и хранения, и для систем электронной цифровой подписи (см. приложение 7).

8.5.5. Особенности защиты информации при использовании технологии терминальной системы

Особенностью терминальных систем, или, другими словами, «тонкого клиента», являются централизованные обработка и хранение информации только на терминальных серверах, без применения системного блока персональной ЭВМ, а также наличие регламентированных потоков информации между сервером терминалов и терминалами (терминальными рабочими станциями), задаваемых исполняемой на сервере терминалов прикладной программой.

В сторону терминала передаются данные «окна» выполняющегося на сервере терминалов приложения. От терминала в сторону сервера терминалов передаются данные от клавиатуры и манипулятора «мышь».

Терминал представляет собой бездисковый компьютер, в состав которого входят дисплей, клавиатура, мышь. Использование бездисковых рабочих станций в терминальной системе предполагает удаленную загрузку операционных систем (их образа) с соответствующего сервера терминалов или из флэш-памяти самого терминала. Используемые средства защиты информации от НСД терминальных систем должны быть сертифицированы по требованиям безопасности информации.

При использовании в таких АИС в качестве оконечных устройств (терминалов) компьютеров, в состав которых входят накопители информации, следует руководствоваться особенностями технологий защиты информации на АРМ, оборудованных автономными персональными ЭВМ (см. разд. 8.5.4).

8.5.6. Особенности технологий защиты информации при межсетевом взаимодействии

Особенности технологий защиты конфиденциальной информации определяются взаимодействием локальных и неоднородных вычислительных сетей, ни одна из которых не имеет выхода в сети общего пользования Интернет.

При взаимодействии АИС с другими вычислительными сетями последние также должны контролироваться с точки зрения защиты конфиденциальной информации. Коммуникационное оборудование и все соединения с периферийными устройствами ЛВС должны располагаться в пределах контролируемой зоны организации.

Подключение ЛВС системы к другой АИС (локальной или неоднородной вычислительной сети) иного класса защищенности должно осуществляться с использованием межсетевого экрана, требования к которому определяются Руководящим документом Гостехкомиссии [198]. При этом такое подключение не должно снижать класс защищенности соединяемых систем.

При передаче информации за пределами контролируемой территории организации, должны использоваться защищенные линии связи (в том числе волоконно-оптические), оборудованные средствами защиты информации, либо средства контроля защиты информации, предназначенные для передачи конфиденциальной информации. Применяемые при этом средства защиты информации должны быть сертифицированы.

8.5.7. Особенности защиты информации в корпоративных информационно-коммуникационных системах

Комплекс организационно-технических мер и средств контроля защиты информации в автоматизированных информационно-коммуникационных системах (ИКС) включает в себя средства и меры выявления попыток несанкционированного физического доступа в помещения и к техническим средствам ИКС, нарушения работоспособности или режима функционирования средств защиты информации, а также получения несанкционированного доступа к защищаемой информации и средствам управления техническими и программными средствами с целью своевременного закрытия возможных каналов утечки информации.

Средства защиты информации от несанкционированного доступа используются во всех узлах автоматизированных ИКС, независимо от наличия (отсутствия) конфиденциальной информации в данном узле. В связи с большим количеством разнородных систем в каждой из них необходимо применение автоматизированных средств контроля и анализа защищенности информации.

Технические средства (серверное, коммуникационное и другое оборудование ИКС), с которыми администраторы и обслуживающий персонал постоянно не работают, выполняя только периодическое техническое обслуживание (проверка работоспособности, изменение настроек программного обеспечения и т. д.), должны располагаться в помещениях, в отношении которых реализован оперативный контроль доступа.

Защита входящих в состав автоматизированных ИКС локальных подсетей, функционально выделенных в отдельные АИС, может осуществляться с использованием механизмов безопасности, реализующих виртуальные локальные сети. При этом соответствующие средства разграничения доступа должны быть сертифицированы по требованиям информационной безопасности.

При использовании в АИС системы электронной почты (e-mail) должны быть предусмотрены средства проверки электронных сообщений, входящих в систему и исходящих из нее, на предмет наличия в ней вредоносного программного обеспечения.

В целях уменьшения нагрузки на оборудование и избежания отказов в обслуживании целесообразно использовать средства фильтрации нежелательных электронных сообщений.

Для управления, контроля защищенности и распределения системных ресурсов в автоматизированных ИКС, включая управление средствами защиты конфиденциальной информации, обрабатывае-

мой, хранимой и передаваемой в системе, используются соответствующие средства защиты информации от несанкционированного доступа, сертифицированные по требованиям информационной безопасности.

При взаимодействии ИКС с другими вычислительными сетями ведется постоянный контроль за возможными попытками вторжения с использованием средств автоматизированного контроля (средств мониторинга сети, обнаружения вторжений и т. д.).

Для обнаружения неправомерных действий внутренних пользователей и аномальной активности сетевых узлов, инфицированных вредоносным программным обеспечением, должны применяться средства обнаружения нетипичной сетевой активности и активного аудита.

Для выявления возможных уязвимостей в используемом программном обеспечении (с учетом текущих настроек механизмов безопасности) следует применять программно-технические средства мониторинга и анализа защищенности (сетевые и системные сканеры безопасности).

Для информационного обмена территориально разнесенных структур организации, т.е. удаленных абонентов, могут использоваться незащищенные каналы связи, в частности информационные сети общего пользования, различные виды выделенных и коммутируемых линий связи. При этом все потоки информации, поступающие в систему и (или) выходящие из нее по данным каналам, должны фильтроваться на специализированных сертифицированных межсетевых экранах. Используемые межсетевые экраны должны соответствовать общим требованиям к ним.

При подключении внешних ЛВС к центральному узлу ИКС через сеть общего пользования необходимо использовать сертифицированные средства защиты информации, обеспечивающие защищенную передачу данных (электронная почта, доступ к базам данных и т. д.).

Сетевые ресурсы (почтовые серверы, веб-серверы и т. д.), к которым разрешен доступ из сетей общего пользования, подключаются к отдельному «открытому» сетевому сегменту, организуемому с использованием сертифицированного межсетевого экрана. Хранение, обработка или передача конфиденциальной информации в данном сетевом сегменте недопустимы.

Установление соединения «открытого» сегмента с другими сетевыми сегментами ИКС, в которых возможна обработка конфиденциальной информации, должно быть исключено. В системе реализуется разграничение доступа пользователей к сервисам и ин-

формационным ресурсам. Выбор сервисов и протоколов для использования в ИКС производится из соображений обеспечения полноты и эффективности реализации соответствующих функций и минимизации уровня уязвимости информации в системе.

Для контроля целостности и достоверности циркулирующей в АИС информации при необходимости используются сертифицированные средства ЭЦП.

Для использования в АИС средств, обеспечивающих юридическую силу электронных конфиденциальных документов и юридически значимый конфиденциальный электронный документооборот, в соответствии с Федеральным законом «Об электронно-цифровой подписи» [37] необходимо наличие Удостоверяющего центра. Для обеспечения юридически значимого электронного конфиденциального документооборота целесообразно использовать защищенную электронную почту.

Администрирование в автоматизированной ИКС планируется и проводится централизованно, на основе принципа минимизации полномочий пользователей при обеспечении требуемого уровня функциональности. За всеми программно-аппаратными составляющими должен быть закреплен администратор, отвечающий за их функционирование, а также администратор безопасности, отвечающий за безопасность обрабатываемой информации.

На технических средствах АИС устанавливается программное обеспечение только той конфигурации, которая необходима для выполнения штатных работ. Установка, настройка и эксплуатация программного обеспечения проводятся в соответствии с утвержденной документацией. Установка произвольных программных средств не допускается. Из программного обеспечения необходимо удалить ненужные для работы и не включенные в обоснование прикладные сервисы (протоколы). Модификация конфигурации программного обеспечения должна быть доступна только администратору, ответственному за его эксплуатацию.

Во все фрагменты, входящие в состав ИКС, устанавливаются и должны исправно функционировать антивирусное программное обеспечение, а также средство контроля сетевой активности, средство контроля приложений, персональный межсетевой экран, средство криптографической защиты конфиденциальной информации для обеспечения возможности ее передачи по открытым каналам связи.

Для доступа к информации АИС пользователей, рабочие места которых размещены в пределах контролируемой территории организации, используются сертифицированные средства защиты ин-

формации от несанкционированного доступа. В случае, если пользователи размещены за пределами контролируемой территории организации и их доступ к ресурсам АИС осуществляется по незащищенным каналам связи, должны использоваться сертифицированные средства криптографической защиты информации, обеспечивающие возможность обмена конфиденциальной информацией в этих условиях.

Защита речевой информации при ее передаче по открытым каналам связи должна осуществляться с помощью средств защиты, сертифицированных по требованиям безопасности информации [188].

8.6. Обеспечение контроля защиты электронного документооборота

Определенные эксплуатационной документацией на АИС требования к процессам автоматизированной обработки конфиденциальной информации сопровождаются технологией контроля состояния защиты информации в системе.

В соответствии с требованиями защиты информации дополнительным проверкам и испытаниям подвергаются средства автоматизированной обработки конфиденциальной информации, или, иными словами, средства конфиденциального электронного оборота.

Контроль проводится в целях своевременного выявления и предотвращения утечки, НСД к конфиденциальной информации, преднамеренных программно-технических воздействий на объект защиты. Определение и оценка уровня информационной безопасности, адекватности создаваемых или готовых решений защиты задаваемым требованиям к уровню информационной безопасности АИС должны выполняться специалистами, прошедшими квалификационный отбор.

Контроль состояния защиты конфиденциальной информации – это оценка требуемого уровня информационной безопасности и эффективности средств защиты, что является неотъемлемой составной частью работ по защите информации при эксплуатации АИС.

Контроль проводится аналогично выполнению контроля защищенности АИС. Требуемый уровень информационной безопасности АИС при автоматизированной обработке конфиденциальной информации представляет собой минимально необходимую совокупность требований к нормативно-правовому, техническому и организационному видам обеспечения информационной безопасности.

Состояние защиты информации в АИС контролируется в целях своевременного выявления и предотвращения утечки, несанкционированного доступа к информации, преднамеренных программно-технических воздействий на объект защиты.

Основной задачей контроля является проверка соответствия принятых и принимаемых мер по защите конфиденциальной информации требованиям по обеспечению защиты АИС, а также своевременности и полноты выполнения требований нормативных документов, регламентирующих организацию и порядок осуществления мероприятий по защите информации.

При проведении контроля проверяемая организация должна обеспечить подтверждение того, что:

- созданная система обеспечивает выполнение требований по защите конфиденциальной информации при эксплуатации АИС;
- меры, средства и мероприятия, проводимые в целях защиты конфиденциальной информации, соответствуют предъявляемым к АИС требованиям информационной безопасности;
- средства защиты информации настроены и используются правильно;
- рекомендации предшествующих проверок реализованы.

Эффективность защиты информации в АИС контролируется на внешнем и внутреннем уровнях. Внешний контроль эффективности защиты информации в АИС на государственном уровне, обрабатывающих конфиденциальную информацию, осуществляется ФСО России, ФСБ и ФСТЭК России, на территориальном уровне – уполномоченными территориальными органами ФСО, ФСБ и ФСТЭК России.

По инициативе организации может быть проведен аудит информационной безопасности (контроль эффективности защиты информации) с привлечением третьей стороны — предприятия (организации), имеющего лицензию ФСТЭК России на этот вид деятельности.

Внутренний контроль осуществляется Службой информационных технологий (информационной безопасности) совместно со Службой безопасности организации. Основными составляющими этого контроля являются:

- автоматизированный контроль на основе контроля (мониторинга) событий защиты информации;
- проверка правильности и полноты проводимых мероприятий по обеспечению соответствия АИС требованиям защиты;
- проверка своевременности внесения изменений в проектную, техническую и нормативно-техническую документацию по обеспечению безопасности информации (предупреждению угроз информации и факторов, влияющих на информацию);

• принятие на основании результатов контроля мер по устранению последствий нарушения требований защиты информации вплоть до полного или частичного приостановления эксплуатации АИС, приостановления или прекращения действия, если иными мерами невозможно устранить нарушения этих требований;

• проведение в ходе мероприятий по государственному контролю разъяснительной работы по применению требований законодательства Российской Федерации и нормативных документов в области обеспечения защиты информации.

Контроль может быть плановым и внеплановым. Государственный и ведомственный контроль проводится в соответствии с планами ведомств, осуществляющих этот контроль. Проверяемая организация должна быть проинформирована о времени проведения контроля.

Подразделение Службы информационных технологий (информационной безопасности) совместно со Службой безопасности организации проводит как плановый (периодический), так и внеплановый контроль. Время проведения внепланового контроля проверяемым не сообщается. Порядок его проведения определяется эксплуатационными документами и соответствующими методиками.

Оперативный контроль за выполнением требований по защите информации осуществляют лица, ответственные за обработку информации, администратор информационной безопасности и другие уполномоченные лица. Оперативный, можно считать повседневный, контроль, в том числе автоматизированный, включает контроль (мониторинг) событий информационной безопасности с использованием средств контроля сети и аудита, обнаружения вторжений, нетипичной сетевой активности и т. д. Аудит информационной безопасности организации проводится по решению руководства.

Контроль эффективности защиты информации, циркулирующей в АИС, осуществляет экспертная комиссия, образованная по распорядительному документу (приказу) руководителя организации, проводящей контроль. Результаты контроля оформляются актами, заключениями и записями в специальных журналах и доводятся до сведения руководителя организации и работников в соответствии с уровнем контроля.

Эксперты, которые контролируют эффективность защиты информации, циркулирующей в АИС, обрабатывающей конфиденциальную информацию, обязаны заключить с владельцем АИС договор (контракт) о неразглашении конфиденциальной информации, с которой они могут ознакомиться в процессе выполнения контроля (см. разд. 4.3.2 и 4.3.3).

Представители органов, проводящие государственный и ведомственный контроль (эксперты), имеют право:

- знакомиться с организацией работ по защите информации;
- получать документацию, касающуюся функционирования АИС;
- получать доступ во все места, где размещены технические средства АИС и хранятся носители информации;
- требовать демонстрации режимов функционирования систем, конфигурации аппаратных и программных средств, их настроек и других параметров, влияющих на безопасность ресурсов АИС;
- получать доступ через представителя проверяемой организации к журналам регистрации событий, происходящих в АИС;
- получать информацию о нарушениях безопасности в АИС и результатах разбора этих нарушений при наличии таковых;
- знакомиться с работой пользователей АИС и другого персонала.

Проверяемая организация должна содействовать проверяющим в реализации указанных выше прав. Представители органов, осуществляющих государственный и ведомственный контроль (эксперты), обязаны соблюдать правила и распорядок работы проверяемой организации.

8.7. Аттестация автоматизированных информационных систем по требованиям безопасности информации

8.7.1. Особенности организация проведения аттестации

Аттестация АИС по требованиям безопасности информации организации (далее – аттестация) проводится на основе действующих на сегодняшний день нормативных документов и руководящих документов ФСТЭК России и ФСО России.

Аттестация является составной частью государственной системы защиты информации и действует под руководством уполномоченного органа по управлению системой аттестации ФСТЭК России, ФСО России и ФСБ России. Аттестация предусматривает комплексную проверку (аттестационные испытания) АИС в реальных условиях эксплуатации в целях оценки соответствия используемого комплекса мер и средств защиты требуемому уровню безопасности информации.

Обязательной аттестации подлежат автоматизированные системы организаций, в которых обрабатывается конфиденциальная информация. Расходы по проведению всех видов работ и услуг по аттеста-

ции осуществляются за счет финансовых средств, выделенных на разработку (доработку, совершенствование, развитие) и ввод в действие защищаемой АИС.

Общее руководство системой аттестации осуществляет уполномоченный орган по управлению ею, который выполняет следующие функции:

- организует, финансирует разработку и утверждает отраслевые организационно-распорядительные, нормативные и методические документы по аттестации АИС по требованиям безопасности информации;
- рассматривает спорные вопросы, возникающие в процессе аттестации;
- формирует и поддерживает в актуальном состоянии фонд документации, используемой при аттестации;
- планирует работы по аттестации и контролирует сроки их проведения;
- разрабатывает типовые программы, а при необходимости и конкретные методики аттестационных испытаний;
- регистрирует аттестаты соответствия на АИС организаций и ведет информационную базу аттестованных систем;
- осуществляет ведомственный надзор за проведением аттестации;
- реализует взаимодействие с ФСТЭК и ФСО России и информирует их о своей деятельности в области аттестации.

Аттестацию проводит аттестационная комиссия, организуемая на основании приказа руководителя организации – заказчика создания или эксплуатации АИС. В приказе обязательно указываются: объект аттестации; сроки проведения аттестации, согласованные с уполномоченным органом по управлению системой аттестации; состав аттестационной комиссии.

В состав аттестационной комиссии по согласованию с соответствующими перечисленными далее организациями могут привлекаться представители: ФСО России, ФСТЭК России, в том числе ее территориальных органов; ФСБ России, в том числе ее территориальных органов; уполномоченного органа по управлению системой аттестации субъектов Российской Федерации; аккредитованных органов по аттестации.

Комиссия проводит аттестационные испытания, по результатам которых оформляет заключение о соответствии АИС требованиям безопасности информации и готовит проект аттестата соответствия. Аттестация может проводиться параллельно с приемо-сдаточными испытаниями АИС.

8.7.2. Подготовка к проведению аттестации

Перед аттестацией руководитель организации назначает ответственного (ответственных) за подготовку АИС к ее проведению.

В обязанности ответственного входит подготовка предложений по формированию аттестационной комиссии, а также исходных данных по аттестуемой АИС, которые зависят от названия автоматизированной системы, определенной организацией-разработчиком и организацией-заказчиком. Исходные данные готовятся на основе следующего перечня вопросов:

- полное и точное наименование АИС и ее назначение;
- характеристика обрабатываемой конфиденциальной информации с указанием соответствующего Перечня конфиденциальных сведений;
- организационная структура АИС;
- состав комплекса технических средств, входящих в АИС, на которых (в которых) обрабатывается конфиденциальная информация;
- структура программного обеспечения (общесистемного и прикладного), используемого в аттестуемой АИС и предназначенного для обработки защищаемой информации;
- общая функциональная схема АИС, включая схему информационных потоков и режимы обработки защищаемой информации;
- наличие и характер взаимодействия с другими АИС;
- состав и структура системы защиты информации в аттестуемой АИС;
- перечень средств защиты и контроля, используемых в аттестуемой АИС и имеющих соответствующий сертификат;
- сведения о разработчиках системы защиты информации и о наличии у них соответствующих лицензий;
- наличие в организации, в которой расположена АИС, Службы информационных технологий (информационной безопасности), а также Службы безопасности, администраторов защиты информации, операционных систем, сетей (локальных и глобальных вычислительных систем и сетей), баз данных и систем управления базами данных;
- наличие и основные характеристики физической защиты объекта (помещений, где обрабатывается защищаемая информация и хранятся информационные носители);
- наличие и готовность проектной и эксплуатационной документации на АИС и другие исходные данные, влияющие на безопасность информации.

Этап подготовки завершается подписанием приказа на проведение аттестации. В приказе указывается перечень организационно-технических мероприятий по подготовке АИС к проведению аттестации. Указанные мероприятия должны быть направлены на устранение недостатков, обнаруженных при проведении приемосдаточных испытаний АИС.

8.7.3. Проведение аттестации

По результатам предварительного ознакомления с аттестуемой АИС аттестационная комиссия разрабатывает программу испытаний, предусматривающую перечень работ и их продолжительность, методики испытаний (или типовых методик). Затем проводится распределение работ среди членов аттестационной комиссии и определяется необходимость использования инструментальных средств контроля защиты.

Порядок, содержание, условия и методы испытаний для оценки характеристик и показателей, проверяемых при аттестации, соответствия их установленным требованиям, а также применяемые в этих целях инструментальные средства определяются в методиках испытаний АИС.

При проведении аттестационных испытаний АИС аттестационная комиссия:

- проводит анализ организационной структуры указанной АИС, информационных потоков, состава и структуры комплекса технических средств и программного обеспечения, системы защиты информации, разработанной документации и ее соответствия требованиям нормативной документации по защите информации;
- определяет правильность установления требований по безопасности информации для аттестуемой АИС, выбора и применения сертифицированных и несертифицированных средств и систем защиты информации;
- проверяет уровень подготовки кадров и распределение ответственности персонала за обеспечение выполнения требований по безопасности информации;
- проводит комплексные аттестационные испытания АИС в реальных условиях эксплуатации путем проверки фактического выполнения установленных требований на различных этапах технологического процесса обработки защищаемой информации, протоколируя все операции и процедуры проверок;

• подготавливает заключение по результатам аттестации с краткой оценкой соответствия АИС требованиям безопасности информации, выводом о возможности выдачи аттестата соответствия и (или) необходимости выполнения рекомендаций. Заключение подписывается членами аттестационной комиссии. К заключению прилагаются протоколы испытаний, подтверждающие полученные при испытаниях результаты и обосновывающие приведенный в заключении вывод. Протоколы испытаний подписываются экспертами – членами аттестационной комиссии, проводившими испытания.

При полном соответствии АИС предъявляемым к ней требованиям аттестационная комиссия подготавливает проект аттестата по следующей форме, который подписывает председатель аттестационной комиссии.

Регистрационный № _____

АТТЕСТАТ СООТВЕТСТВИЯ

_____

(указывается полное наименование АИС)

ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

№_____

Действителен до «___» _____ _____ г.

1. Настоящим **АТТЕСТАТОМ** удостоверяется, что _____

_____

(приводится полное наименование АИС)

соответствует требованиям нормативной и методической документации по безопасности информации.

1. Состав комплекса технических средств объекта информатизации (с указанием заводских номеров, модели, изготовителя, номеров сертификатов), схема размещения в помещениях и относительно границ контролируемой зоны, перечень используемых программных средств, а также средств защиты (с указанием изготовителя и номеров сертификатов) прилагаются.

2. Организационная структура, уровень подготовки специалистов, нормативное, методическое обеспечение и техническая оснащенность службы безопасности информации обеспечивают контроль эффективности мер и средств защиты и поддержание уровня защищенности АИС в процессе эксплуатации в соответствии с установленными требованиями.

3. Аттестация АИС выполнена в соответствии с программой и методиками аттестационных испытаний, утвержденными «___»_____ ____ г. №_____ .

4. С учетом результатов аттестационных испытаний на объекте информатизации разрешается обработка

_____

(указывается, общедоступная или конфиденциальная)

информации.

5. При эксплуатации объекта информатизации запрещается: _____

_____

(указываются ограничения, которые могут повлиять на эффективность мер и средств защиты информации)

6. Контроль за эффективностью реализованных мер и средств защиты возлагается на Службу информационных технологий (информационной безопасности информации) и Службу безопасности.

7. Подробные результаты аттестационных испытаний приведены в заключении аттестационной комиссии (№ _____, «___»_____ г.) и протоколах испытаний.

8. Аттестат соответствия выдан на _____ года, в течение которых должна быть обеспечена неизменность условий функционирования АИС и технологии обработки защищаемой информации, могущих повлиять на характеристики, указанные в п. 9.

9. Перечень характеристик, об изменениях которых требуется обязательно извещать орган по аттестации:

9.1_____

9.2_____

Руководитель аттестационной комиссии

_____

(должность с указанием наименования организации)

_____

(подпись ФИО)

«___» _____20___ г.

При выявлении нарушений или несоответствия требованиям безопасности информации аттестационная комиссия подготавливает проект распоряжения по организации об устранении недостатков, обнаруженных при проведении аттестации. После устранения этих недостатков аттестационная комиссия проводит дополнительные проверки, по результатам которых подготавливает проект аттестата соответствия АИС требованиям безопасности информации.

Аттестат выдается на период времени, в течение которого должна обеспечиваться неизменность условий функционирования АИС и технологий обработки защищаемой информации, могущих повлиять на характеристики, определяющие безопасность информации (состав и структура технических средств, используемое программное обеспечение, режимы обработки информации, средства и меры защиты), но не более чем на три года. Организация, эксплуатирующая аттестованную АИС, несет ответственность за выполнение установленных условий ее функционирования, технологий обработки защищаемой информации и требований по безопасности информации.

В случае необходимости внесения изменений в условия и технологии обработки защищаемой информации эти изменения внедряются с последующей дополнительной проверкой эффективности системы защиты АИС, осуществляемой в порядке, предусмотренном для проведения аттестации, но в части, касающейся внесенных изменений. Аттестат направляется в уполномоченный орган по управлению системой аттестации для регистрации в базе данных АИС, аттестованных на соответствие требованиям безопасности информации. На аттестате соответствия проставляется регистрационный номер, после чего аттестат возвращается организации, где проводилась аттестация.

Государственный надзор за проведением аттестации проводится Инспекцией ФСТЭК России и ФСБ России как в процессе, так и по завершении аттестации, а за эксплуатацией аттестованных АИС – периодически, в соответствии с планами работы по контролю. Надзор за эксплуатацией аттестованных АИС осуществляется в соответствии с основными положениями, изложенными в разд. 8.6.

В случае грубых нарушений при проведении аттестации требований стандартов или иных нормативных документов по безопасности информации, выявленных органом надзора, он может предложить организации расформировать аттестационную комиссию и создать новую. При этом аттестат, выданный комиссией, допускающей нарушения при проведении аттестации, будет недействительным.

8.8. Защита от вредоносных программ*

8.8.1. Пути распространения вирусных угроз

Развитие современных информационных и телекомунникационных технологий – процессов, методов поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов дает возможность злоумышленникам – хакерам использовать различные источники распространения вредоносных программ и вирусных угроз, а имен-

* Раздел создан на основе материалов сайта «Лаборатория Касперского» – http://www.kaspersky.ru [325].

но неправомерный доступ, уничтожение, модифицирование, блокирование, копирование, а также от других неправомерных действий в отношении информации и ее обладателя.

Вредоносные программы – вирусы могут распространяться различными путями. В данном разделе эти пути рассмотрены более подробно.

Интернет – глобальная сеть «Интернет» уникальна тем, что не является чьей-то собственностью и не имеет территориальных границ. Это во многом способствует развитию многочисленных веб-ресурсов и обмену информацией. Сейчас любой человек может получить доступ к данным, хранящимся в сети Интернет, или создать свой собственный веб-ресурс.

Однако эти же особенности глобальной сети предоставляют злоумышленникам возможность совершения преступлений в Интернете, затрудняя их обнаружение и наказание. Злоумышленники размещают вирусы и другие вредоносные программы на веб-ресурсах, «маскируют» их под полезное и бесплатное программное обеспечение, которое может выполнять вредоносные действия на компьютере, в системах межведомственного (межсетевого) электронного документооборота ВЭД, включая изменение системного реестра, кражу персональных данных и другой информации, установку вредоносного программного обеспечения.

Используя сетевые технологии, злоумышленники реализуют атаки на удаленные частные компьютеры и серверы организаций – государственных и негосударственных структур. Результатом таких атак может являться выведение информационного ресурса из строя, получение полного доступа к ресурсу организации, а следовательно, к хранящейся на нем информации, использование ресурса.

В связи с появлением кредитных карт, электронных денег и возможностью их использования через Интернет (интернет-магазины, аукционы, персональные страницы банков и т.д.) компьютерное мошенничество стало одним из наиболее распространенных преступлений, которые наказуемы (см. приложение 6).

Локальная сеть – это внутренняя сеть (специалисты также называют ее сетью Интранет), специально разработанная для управления информацией внутри организации – государственной и негосударственной структуры. Локальная сеть является единым пространством для хранения, обмена и доступа к информации для всех компьютеров сети. Поэтому, если какой-либо из компьютеров сети заражен, остальные компьютеры подвергаются значительному риску зараже-

ния. Во избежание возникновения таких ситуаций необходимо защищать не только периметр локальной сети, но и каждый отдельный компьютер.

Электронная почта – наличие электронных почтовых приложений есть практически на каждом компьютере, и то, что вредоносные программы полностью используют содержимое электронных адресных книг для выявления новых пострадавших, обеспечивает благоприятные условия для распространения вредоносных программ. Пользователь зараженного компьютера, сам того не подозревая, рассылает зараженные письма адресатам, которые, в свою очередь, отправляют новые зараженные письма и т.д. Нередки случаи, когда зараженный файл-документ по причине недосмотра попадает в списки рассылки информации какой-либо организации – государственной и негосударственной структуры. В этом случае страдают сотни – тысячи абонентов таких рассылок, которые затем разошлют зараженные файлы десяткам тысяч своих абонентов.

Помимо угрозы проникновения вредоносных программ существует проблема внешней нежелательной почты рекламного характера (спама – в переводе с англ. мусор). Не являясь источником прямой угрозы, нежелательная корреспонденция увеличивает нагрузку на почтовые серверы, создает дополнительный трафик, засоряет почтовый ящик пользователя, ведет к потере рабочего времени и тем самым наносит значительный временной и соответственно материальный и финансовый урон.

Важно отметить также то, что злоумышленники стали использовать так называемые спамерские технологии массового распространения и методы социального менеджмента, чтобы заставить пользователя открыть письмо, перейти по ссылке из письма на какой-либо сайт или Интернет-ресурс. Из этого следует, что возможности фильтрации спама важны не только сами по себе, но и для противодействия некоторым новым видам интернет-мошенничества, а также распространению вредоносных программ и вирусов.

Съемные носители информации – дискеты, CD/DVD-диски, флеш-карты – широко используются для хранения и передачи информации.

При запуске файла, содержащего вредоносный код, со съемного носителя вы можете повредить данные, хранящиеся на компьютере, и распространить вирус на другие диски компьютера или компьютеры сети. Поэтому съемные носители в организации необходимо учитывать. Более подробно это рассмотрено в разд. 3.7.

8.8.2. Виды вирусов

В приложении 7 отмечается, что антивирусное программное обеспечение должно быть типа «Kaspersky Business Space Security» [117]. Поэтому в данном подразделе подробнее остановимся на угрозах, блокируемых Антивирусом Касперского.

Черви (Worms) – вредоносные программы, которые для распространения используют в основном уязвимости операционных систем. Название этого класса программ было дано исходя из способности червей «переползать» с компьютера на компьютер, используя сети и электронную почту. Благодаря этому многие черви обладают достаточно высокой скоростью распространения.

Черви проникают на компьютер, осуществляют поиск сетевых адресов других компьютеров и рассылают по этим адресам свои копии. Помимо сетевых адресов часто используются данные адресной книги почтовых клиентов. Представители этого класса вредоносных программ иногда создают рабочие файлы на дисках системы, но могут вообще не обращаться к ресурсам компьютера (за исключением оперативной памяти).

Вирусы (Viruses) – программы, которые заражают другие программы: добавляют в них свой код, чтобы получить управление при запуске зараженных файлов. Это простое определение дает возможность выявить основное действие, выполняемое вирусом – заражение.

Троянские программы (Trojans) – выполняют на поражаемых компьютерах несанкционированные пользователем действия, т.е. в зависимости от каких-либо условий уничтожают информацию на дисках, приводят систему к «зависанию», воруют конфиденциальную информацию и т.д. Данный класс вредоносных программ не является вирусом в традиционном понимании этого термина (т.е. не заражает другие программы или данные); троянские программы не способны самостоятельно проникать на компьютеры и распространяются злоумышленниками под видом «полезного» программного обеспечения. При этом вред, наносимый ими, может во много раз превышать потери от традиционной вирусной атаки.

В последнее время наиболее распространенными типами вредоносных программ, портящими компьютерные данные, стали черви. Далее по распространенности следуют вирусы и троянские программы. Некоторые вредоносные программы совмещают в себе характеристики двух или даже трех из перечисленных выше классов.

Программы-рекламы (Adware) — программный код, без ведома пользователя включенный в программное обеспечение с целью демонстрации рекламных объявлений. Как правило, программы-рекламы встроены в программное обеспечение, распространяющееся бесплатно. Реклама располагается в рабочем интерфейсе. Зачастую данные программы также собирают и переправляют своему разработчику персональную информацию о пользователе, изменяют различные параметры браузера (стартовые и поисковые страницы, уровни безопасности и т.д.), а также создают неконтролируемый пользователем трафик. Все это может привести как к нарушению политики безопасности, так и к прямым финансовым потерям.

Программы-шпионы (Spyware) – программное обеспечение, позволяющее собирать сведения об отдельно взятом пользователе или организации без их ведома. О наличии программ-шпионов на своем компьютере можно и не догадываться. Как правило, целью программ-шпионов является:

- отслеживание действий пользователя на компьютере;
- сбор информации о содержании жесткого диска; в этом случае чаще всего речь идет о сканировании некоторых каталогов и системного реестра с целью составления списка программного обеспечения, установленного на компьютере;
- сбор информации о качестве связи, способе подключения, скорости модема и т.д.

Потенциально опасные приложения (Riskware) – это приложения, которые не имеют вредоносных функций, но могут являться частью среды разработки вредоносного программного обеспечения или использоваться хакерами-злоумышленниками в качестве вспомогательных компонентов вредоносных программ. К категории таких программ относятся программы, имеющие бреши и ошибки, а также некоторые утилиты удаленного администрирования, программы автоматического переключения раскладки клавиатуры, серверы, всевозможные утилиты для остановки процессов или скрытия их работы.

Еще одним видом вредоносных программ, являющимся пограничным для таких программ, как Adware, Spyware и Riskware, являются программы, встраивающиеся в установленный на компьютере браузер и перенаправляющие трафик. Например, если при запросе одного адреса веб-сайта открывается совсем другой.

Программы-шутки (Jokes) – программное обеспечение, не причиняющее компьютеру какого-либо прямого вреда, но выводящее сообщения о том, что такой вред уже причинен либо будет причинен при каких-либо условиях. Такие программы часто предупреждают

пользователя о несуществующей опасности, например, выводят сообщения о форматировании диска (хотя никакого форматирования на самом деле не происходит), обнаруживают вирусы в незараженных файлах и т.д.

Руткиты (Rootkit) – утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами. Руткиты модифицируют операционную систему на компьютере и заменяют основные ее функции, чтобы скрыть свое собственное присутствие и действия, которые предпринимает злоумышленник на зараженном компьютере.

Прочие опасные программы – программы, созданные для организации атак на удаленные серверы, взлома других компьютеров, а также являющиеся частью среды разработки вредоносного программного обеспечения. К таким программам относятся хакерские утилиты (Hack Tools), конструкторы вирусов, сканеры уязвимостей, программы для взлома паролей, прочие виды программ для взлома сетевых ресурсов или проникновения в атакуемую систему.

Обнаружение и блокирование данных видов угроз антивирусом Касперского возможно с помощью двух методов:

1) реактивного – метода, основанного на поиске вредоносных объектов с помощью постоянно обновляемых баз приложения. Для реализации данного метода необходимо хотя бы одно заражение, чтобы добавить в базы и распространить обновление баз;

2) проактивного – метода, в отличие от реактивной защиты, строящегося на анализе не кода объекта, а его поведения в системе. Этот метод нацелен на обнаружение новых угроз, информации о которых еще нет в базах.

Применение обоих методов в антивирусе Касперского обеспечивает комплексную защиту компьютера от известных, а также новых угроз.

8.8.3. Признаки заражения

Есть ряд признаков, свидетельствующих о заражении компьютера или АИС. Если заметно, что с компьютером происходят «странные» вещи, а именно:

- на экран выводятся непредусмотренные сообщения, изображения либо воспроизводятся непредусмотренные звуковые сигналы;
- неожиданно открывается и закрывается лоток CD/DVD-ROM-устройства;

• произвольно на компьютере запускаются какие-либо программы;

• на экран выводятся предупреждения о попытке какой-либо из программ компьютера выйти в Интернет, хотя вы никак не инициировали такое его поведение, то с большой степенью вероятности можно предположить, что компьютер поражен вирусом.

Существуют некоторые характерные признаки поражения вирусом через электронную почту:

• другие пользователи АИС информируют об электронных сообщениях от вас, которые вы не отправляли;

• в электронном почтовом ящике находится большое количество сообщений без обратного адреса и заголовка.

Следует отметить, что не всегда такие признаки вызываются присутствием вирусов. Иногда они могут быть следствием других причин. Например, в случае с электронной почтой зараженные сообщения могут рассылаться с вашим обратным адресом, но не с вашего компьютера.

Косвенными признаками заражения компьютера являются следующие:

• частые зависания и сбои в работе;

• медленная работа при запуске программ;

• невозможность загрузки операционной системы;

• исчезновение файлов и каталогов или искажение их содержимого;

• частое обращение к жесткому диску (часто мигает лампочка на системном блоке);

• веб-браузер, например Microsoft Internet Explorer, «зависает» или ведет себя неожиданным образом (например, окно программы невозможно закрыть).

В 90% случаев наличие косвенных признаков вызвано сбоем в аппаратном или программном обеспечении. Несмотря на то что подобные симптомы с малой вероятностью свидетельствуют о заражении, при их появлении рекомендуется провести полную проверку компьютера или АИС.

8.8.4. Проактивная защита от вредоносных программ

Антивирус Касперского защищает не только от известных угроз, но и от новых, информация о которых отсутствует в базах приложения. Это обеспечивает специально разработанный компонент – проактивная защита.

Необходимость в проактивной защите назрела с тех пор, как скорость распространения вредоносных программ стала превышать скорость обновления антивирусной защиты, способной обезвредить эти угрозы. Реактивные технологии, на которых построена антивирусная защита, требуют как минимум одного фактического заражения новой угрозой, время на анализ вредоносного кода, на добавление его в базы приложения и на обновление этих баз на компьютерах пользователей. За это время новая угроза может нанести огромный ущерб.

Превентивные технологии, на которых построена проактивная защита антивируса Касперского, позволяют избежать потери времени и обезвредить новую угрозу еще до того, как она нанесет вред вашему компьютеру. За счет чего это достигается? В отличие от реактивных технологий, где анализ выполняется на основании записей баз приложений, превентивные технологии распознают новую угрозу на вашем компьютере по последовательности действий, выполняемых некоторой программой. В поставку программы включен набор критериев, позволяющих определять, насколько активность той или иной программы опасна. Если в результате анализа активности последовательность действий какой-либо программы вызывает подозрение, антивирус Касперского применяет действие, заданное правилом для активности подобного рода.

Опасная активность определяется по совокупности действий программы. Например, при обнаружении таких действий, как самокопирование некоторой программы на сетевые ресурсы, в каталог автозапуска, системный реестр, а также последующая рассылка копий, можно с большой долей вероятности предположить, что это программа – червь. К опасным действиям также относятся:

- изменения файловой системы;
- встраивание модулей в другие процессы;
- скрытие процессов в системе;
- изменение определенных ключей системного реестра Microsoft Windows.

• Все опасные операции отслеживаются и блокируются проактивной защитой. В процессе работы проактивная защита использует набор правил, включенных в поставку программы, а также сформированных пользователем при работе с приложением. Правило – это набор критериев, определяющих совокупность подозрительных действий и реакцию антивируса Касперского на них. Отдельные правила предусмотрены для активности приложений, контроля изменений системного реестра и запускаемых на компьютере программ.

При этом можно изменять правила по своему усмотрению, добавляя, удаляя или изменяя их. Правила могут быть запрещающими или разрешающими.

Рассмотрим алгоритм работы проактивной защиты. Сразу после запуска компьютера проактивная защита анализирует следующее.

Действия каждого запускаемого на компьютере приложения. История выполняемых действий и их последовательность фиксируется и сравнивается с последовательностью, характерной для опасной активности (база видов опасной активности включена в поставку антивируса Касперского и обновляется вместе с базами приложения).

Целостность программных модулей, установленных на компьютере приложений, что позволяет избежать подмены модулей приложения, встраивания в них вредоносного кода.

Каждую попытку изменения системного реестра (удаление, добавление ключей системного реестра, ввод значений для ключей в недопустимом формате, препятствующем их просмотру и редактированию, и т.д.).

Анализ производится на основании разрешающих и запрещающих правил проактивной защиты. В результате анализа возможны следующие варианты поведения:

- если активность удовлетворяет условиям разрешающего правила проактивной защиты либо не подпадает ни под одно запрещающее правило, она не блокируется;
- если активность описана в запрещающем правиле, дальнейшая последовательность действий компонента соответствует инструкциям, указанным в правиле. Обычно такая активность блокируется. На экран выводится уведомление, где указывается приложение, тип его активности, история выполненных действий. Необходимо самостоятельно принять решение, запретить или разрешить такую активность. Можно создать правило для такой активности и отменить выполненные действия в системе.

В том случае, если при появлении уведомления проактивной защиты пользователь не производит никаких действий, через некоторое время приложение применяет действие по умолчанию, рекомендуемое для данной угрозы. Рекомендуемое действие может быть различным для разных типов угроз.

Вердикты проактивной защиты. Необходимо обратить внимание, что не все вердикты должны однозначно восприниматься как угроза. Некоторые из этих операций являются нормальным поведением приложений, выполняющихся на компьютере, либо реакцией

операционной системы на работу данных приложений. Однако в некоторых случаях эти же операции могут быть вызваны деятельностью злоумышленников либо вредоносных программ.

Вердикты, опасность которых очень высока, выделены по тексту раздела красным цветом. Вердикты, которые не всегда свидетельствуют об угрозе, отмечены черным цветом.

Переполнение буфера (Stack overflow) – одна из самых широко распространенных в настоящее время технологий получения несанкционированного доступа к системе.

Суть уязвимости заключается в следующем: для работы программы обычно необходим стек – структура в памяти, в которую можно помещать промежуточные значения и доставать их оттуда в обратном порядке. Когда программа вызывает процедуру (подпрограмму), она помещает адрес возврата в стек, в результате чего процедура знает, куда возвращать управление после того, как она завершится. Проблема переполнения стека заключается в том, что в стек передается блок данных, превышающий его объем. Лишние данные записываются как раз в ту часть стека, которая предназначена для корректного возврата из процедуры. Таким образом, переполнение изменяет обычный ход выполнения программы и вместо корректного возврата к ее дальнейшему выполнению происходит переход по адресу, который, благодаря переполнению стека, был перезаписан в командном указателе.

Для вызова переполнения стека злоумышленники используют эксплойты (от англ. exploit – использовать в своих целях) – это программы, содержащие машинные инструкции, исполняемые процессором. Адрес, по которому перейдет процессор в результате переполнения стека, будет указывать на эти инструкции.

Вероятность переполнения стека при работе обычных программ в штатном режиме крайне мала. Обнаружение факта переполнения стека с большой вероятностью означает попытку использования этой уязвимости в злонамеренных целях.

Выполнение данных (Data execution). Эта технология использует ошибки в программном обеспечении, установленном на компьютере или АИС. Суть используемых ошибок – замещение корректной информации данными, предоставленными вредоносным объектом, в результате чего они неправильно обрабатываются. Самый распространенный объект атаки с использованием Data execution – это браузеры, многие из которых во время работы с веб-страницами, изображениями и мультимедиа-объектами не выполняют необходимых проверок, и внедрившийся в объекты на веб-страницах вредоносный код может получить управление.

Компания Microsoft для защиты исполняемого кода в Microsoft Windows использует решение DEP (Data Execution Prevention – предотвращение выполнения данных). Решение входит в пакеты обновления для Microsoft Windows XP и Microsoft Windows Server 2003.

Скрытая установка (Hidden Install) – это процесс установки вредоносной программы или запуск исполняемых файлов без уведомления об этом пользователя. Процесс скрытой установки можно обнаружить обычными средствами (например, диспетчером задач Microsoft Windows), но, поскольку во время установки вредоносной программы на экране нет стандартных окон установки, пользователю вряд ли придет в голову отслеживать процессы, происходящие в системе.

Скрытый процесс (Hidden Object) – это процесс, который нельзя обнаружить обычными средствами (диспетчер задач Microsoft Windows, Process Explorer и др.). Руткит (от англ. «*root kit*» – набор для получения прав суперпользователя «root») – программа или набор программ для скрытого контроля взломанной системы. В контексте операционной системы Microsoft Windows под термином «руткит» принято подразумевать программу, которая внедряется в систему, перехватывает и искажает системные сообщения, содержащие информацию о запущенных в ней процессах, а также о содержимом папок на диске. Другими словами, руткит работает аналогично серверу, пропуская через себя одну информацию и не пропуская или искажая другую. Кроме того, как правило, руткит может маскировать присутствие в системе любых описанных в его конфигурации процессов, каталогов и файлов на диске, ключей в реестре. Многие руткиты устанавливают в систему свои драйверы и службы, которые, естественно, являются «невидимыми» как для средств управления системой, таких как диспетчер задач или Process Explorer, так и для антивирусных программ.

Контроль удаленного доступа (Root Shell). Суть уязвимости заключается в запуске командной строки с перенаправленным вводом/выводом (обычно в сеть), что, как правило, используется для получения удаленного доступа к компьютеру. Вредоносный объект пытается получить доступ к командной строке на компьютере-жертве, из которой будут исполняться дальнейшие команды. Обычно доступ бывает получен в результате удаленной атаки и запуска скрипта, использующего данную уязвимость. Скрипт запускает интерпретатор командной строки с компьютера, подключенный по TCP-соединению. В результате злоумышленник может удаленно управлять системой.

Запуск браузера с параметрами (Starting Internet Browser). Контроль запуска браузера с параметрами позволяет перехватить скрытый запуск браузера с переданными ему данными, которые потом могут быть использованы злоумышленниками. Обычно запуск браузера с параметрами (содержащими, к примеру, пользовательские пароли) происходит каждый раз, когда пользователь «кликает» по ссылке в письме в почтовой программе, что не является подозрительным действием. Если внести почтовую программу в доверенную зону, т. е. если разрешить запуск браузера с параметрами только определенным программам, то в остальных случаях, когда осуществляется передача данных через браузер от лица злоумышленника, а не пользователя компьютера, данное действие может расцениваться как подозрительное.

Обнаружение необычного поведения (Strange Behaviour). Данный аспект подразумевает под собой обнаружение не опасного или подозрительного поведения какого-либо конкретного процесса, а изменение состояния самой операционной системы, например прямой доступ к памяти.

Обнаружение опасного поведения (Generic-детекты). К данной группе распознавателей вредоносных действий относятся Trojan.generic, Worm.generic и Worm.P2P.generic – довольно сложные алгоритмы распознавания опасного поведения. Вердикт о том, что какой-либо процесс является, скорее всего, неизвестным вредоносным процессом, принимается на основе анализа совокупности действий, а не какого-то одного или двух признаков. Вердикт Generic не присваивается при первой же попытке совершения подозрительного действия. С каждым совершаемым подозрительным действием «рейтинг подозрительности» процесса растет. Как только он достигает критической отметки, проактивная защита срабатывает. Этим достигается крайне низкий уровень ложных срабатываний. Вероятность того, что «хорошая» программа проявляет сразу несколько аспектов вредоносности, крайне мала.

Действия, влияющие на рейтинг подозрительности:

- действия, характерные для заражения и укрепления вредоносного объекта в системе;
- непосредственно вредоносные действия;
- действия, характерные для распространения (размножения) вредоносного объекта.

Изменение исполняемого файла (Application Changed). Данное событие означает, что исполняемый файл контролируемого приложения был изменен с момента предыдущего запуска. Следует помнить, что его изменение могло произойти в результате как внедрения

в приложение вредоносного кода, так и обычного обновления программы (например, исполняемый файл браузера Microsoft Internet Explorer может измениться из-за обновления Microsoft Windows).

Нарушение целостности (Intergity Violation). Нарушение целостности заключается в том, что с момента предыдущего запуска один или несколько модулей контролируемого приложения могли быть изменены. Помимо изменений в результате внедрения в приложение вредоносного кода, могли произойти изменения и из-за обновления программы (например, библиотеки, используемые браузером Microsoft Internet Explorer, могут измениться вследствие обновления Microsoft Windows).

Контроль запуска приложений (Critical Application). Модуль контроля целостности приложений обладает дополнительной возможностью – контролем запуска приложений. В этом режиме антивирус Касперского выдает предупреждение всякий раз, когда запускается указанное пользователем приложение. Предупреждение появляется только в том случае, если для контролируемого приложения настроено правило *Запуск: Запросить действие*. По умолчанию этот режим отключен.

Запуск дочернего процесса (Running as child). Существует ряд вредоносных программ, которые используют известные программы для организации утечки данных или загрузки вредоносного кода из Интернета. Для этого известная программа, для которой правилами сетевого экрана и других средств защиты разрешен доступ в Интернет (например, веб-браузер), запускается вредоносной программой. Контролируемое приложение при этом запускается как дочерний процесс. Предупреждение появляется только в том случае, если для контролируемого приложения настроено правило *Запуск процесса как дочернего: Запросить действие*. Поскольку запуск одних программ другими в качестве дочерних процессов – это достаточно распространенное явление, по умолчанию показ предупреждений о таких событиях отключен, однако эти события протоколируются в отчетах проактивной защиты.

Изменение файла hosts (Hosts file modification). Файл hosts – это один из важных системных файлов операционной системы Microsoft Windows. Он предназначен для перенаправления доступа к интернет-ресурсам за счет преобразования URL-адресов в IP-адреса не на DNS-серверах, а непосредственно на локальном компьютере. Файл hosts является обычным текстовым файлом, каждая строка которого определяет соответствие символьного имени (URL) сервера и его IP-адреса. Вредоносные программы часто используют данный файл для переопределения адресов серверов обновлений антивирусных

приложений, чтобы заблокировать возможность обновления и предотвратить обнаружение вредоносной программы сигнатурным методом, а также для других целей.

Внедрение в процесс (Invader / Loader). Существует множество разновидностей вредоносных программ, которые маскируются под исполняемые файлы, библиотеки или модули расширения известных программ и внедряются в стандартные процессы. Таким образом, можно, например, организовать утечку данных с компьютера пользователя. Сетевой трафик, инициированный вредоносным кодом, будет свободно пропускаться сетевыми экранами, поскольку, с точки зрения сетевого экрана, этот трафик принадлежит приложению, которому разрешен доступ в Интернет.

Внедрение в другие процессы широко используется троянскими программами. Однако такая активность характерна также для некоторых безобидных программ, пакетов обновлений и программ установки. Следует разрешать этот вид активности только в том случае, если вы уверены, что внедряемая программа безобидна.

Обнаружение клавиатурных перехватчиков (Keylogger). Клавиатурный перехватчик – это программа, перехватывающая все нажатия клавиш на клавиатуре. Вредоносная программа такого типа может отправлять информацию, набираемую на клавиатуре (логины, пароли, номера кредитных карт) злоумышленнику. Однако перехват нажатий клавиш может использоваться и обычными программами. Часто перехват нажатий клавиш применяется для вызова функций программы из другого приложения с помощью «горячих клавиш».

Мониторинг системного реестра (Registry access). Контроль системного реестра (монитор реестра) отслеживает изменения ключей реестра. Вредоносные программы модифицируют реестр с целью регистрации себя для автоматического запуска при старте операционной системы, подмены стартовой страницы Microsoft Internet Explorer и других деструктивных действий. Однако следует помнить, что доступ к системному реестру может осуществляться и обычными приложениями. Модуль содержит предустановленный список из шести групп критических ключей. Кроме того, пользователь может добавить свои группы ключей и настроить правила доступа к ним для различных приложений.

Контроль подозрительных значений в реестре (Registry strange). Модуль позволяет перехватить попытку создания «скрытых» ключей в реестре, не отображаемых обычными программами (типа regedit). Создаются ключи с некорректными именами, чтобы редактор реестра не смог отобразить эти значения, в результате чего диагностика на присутствие в системе вредоносного программного обеспечения затрудняется.

Обнаружение доставки вредоносных программ (Trojan Downloader). Trojan Downloader – это программа, основным назначением которой является скрытая несанкционированная загрузка программного обеспечения из Интернета. Наиболее известным источником Trojan Downloader являются хакерские сайты. Сама по себе Trojan Downloader не несет прямой угрозы для компьютера – она опасна именно тем, что производит неконтролируемую загрузку и запуск программного обеспечения. Trojan Downloader применяется в основном для загрузки и запуска вирусов, троянских и шпионских программ.

8.9. Защита системы электронных сообщений*

8.9.1. Система электронных сообщений

Система электронных сообщений или, иными словами, система электронной почты – один из наиболее широко используемых видов сервиса, как в системах ВЭД и МЭД, так и в сети Интернет. Система электронных сообщений (СЭС) является не просто способом доставки сообщений, а важнейшим средством коммуникации, распределения информации и управления различными процессами в организации, государственных и негосударственных структур. Роль СЭС становится очевидной, если рассмотреть функции, которые выполняет система:

- обеспечивает внутренний и внешний информационный обмен;
- является компонентом систем электронного документооборота;
- формирует транспортный протокол приложений;
- является средством образования инфраструктуры электронного документооборота.

Выполняя эти функции, СЭС решает одну из важнейших задач – формирует единое информационное пространство. В первую очередь это касается создания общей коммуникационной инфраструктуры, которая упрощает обмен информацией между отдельными людьми, подразделениями одной организации и различными организациями.

Использование СЭС для обмена информацией между сотрудниками как внутри организации, так и за ее пределами способно коренным образом изменить технологии и методы ведения дел. Переход

---

* Раздел создан на материалах сайта Jet Info информационный бюллетень – http://www.jetinfo.ru/2003.

к обмену документами в электронном виде повышает эффективность труда и экономию средств и времени.

Система электронных сообщений обладает рядом преимуществ по сравнению с обычными способами передачи сообщений (традиционная почта или факсимильная связь). К ним относятся следующие.

Оперативность и легкость использования. СЭС — это глобальная система, позволяющая передавать сообщения в любую точку мира за считанные секунды, независимо от времени суток. Отправка и прием электронных сообщений не требуют глубоких знаний информационных технологий, благодаря чему этот сервис широко применяется не только в любых организациях, но также и для личного общения. Современные условия требуют оперативного реагирования на процессы, происходящие в организации. СЭС позволяет собирать информацию, принимать решения и доводить их до различных подразделений организации, других организаций, участников межведомственного (межсетевого) электронного документооборота.

Доступность практически в любом месте. Главное преимущество СЭС — ее доступность. Развитие электронных коммуникаций и средств связи (мобильной связи) привело к тому, что электронное сообщение можно отправить и получить с любой точки земного шара.

Универсальность форматов сообщений и вложений. Удобство использования СЭС состоит в том, что она способна «переносить» большие объемы информации различных форматов данных. В одном сообщении могут быть одновременно переданы графическая, видео, текстовая информация, файлы баз данных, приложений и др.

Дешевизна. Отправить электронное сообщение дешевле, чем обычное, или сделать междугородный, или тем более международный телефонный звонок. СЭС позволяет рассылать сообщения сразу нескольким адресатам без дополнительных затрат.

Надежность и скорость инфраструктуры доставки. Электронные сообщения пересылаются непосредственно с сервера отправителя на сервер получателя по каналам Интернет. Этот процесс протекает быстро, даже если эти серверы расположены на противоположных районах России. Фактически на передачу текстового сообщения, например, из России в Америку требуется не более одной минуты.

Использование для обработки электронных сообщений специального программного обеспечения. Электронный характер сообщения позволяет проводить его обработку при помощи дополнительного программного обеспечения. При этом виды обработки зависят от

характера деятельности организации. Это может быть создание базы данных СЭС, формирование различных отчетов, проведение анализа деятельности организации и т.д. Все это позволяет создать единую систему управления документооборотом, полностью интегрированную с остальными информационными технологиями организации.

8.9.2. Угрозы, связанные с использованием системы электронных сообщений

Система электронных сообщений обладает многочисленными достоинствами, но именно из-за этих достоинств возникают основные угрозы информационной безопасности, связанные с ее использованием. Например, доступность СЭС превращается в недостаток, когда пользователи начинают применять систему для рассылки спама, легкость в использовании и бесконтрольность приводят к утечкам информации, возможность пересылки разных форматов документов — к распространению вирусов и т.д.

В конечном счете любая из этих угроз может привести к серьезным последствиям для организации. Это потеря эффективности работы, снижение качества услуг АИС, а также разглашение и утечка конфиденциальной информации. Недостаточное внимание к данной проблеме грозит значительными потерями, а в некоторых случаях даже привлечением к юридической ответственности в связи с нарушением законодательства (см. приложение 6).

Организация подвергается угрозам в силу ряда свойств системы электронных сообщений. Например, СЭС может переносить большие объемы информации различных форматов данных в виде прикрепленных к сообщениям файлов. Такой возможностью сразу воспользовались злоумышленники. Достоинство СЭС превратилось в угрозу, поскольку система стала представлять собой практически идеальную среду для переноса различного рода «опасных» вложений, а именно компьютерных вирусов, вредоносных программ, троянских программ и т.д. (см. разд. 8.8). Если надлежащий контроль за использованием системы не обеспечен, то это может привести к серьезным последствиям и нанести непоправимый ущерб. Избавиться от данной угрозы можно лишь путем блокировки сообщений с «опасными» вложениями, а также антивирусной проверки прикрепленных файлов. На практике же оптимальным средством может оказаться блокировка определенных типов файлов. Это, как правило, исполняемые файлы (exe, com, bat) и файлы, содержащие макросы и OLE-объекты (файлы, созданные в приложениях MS Office).

Опасность для сети представляют различного рода атаки с целью «засорения» системы электронных сообщений. В первую очередь это пересылка в качестве вложений в сообщениях файлов больших объемов или многократно заархивированных файлов. Открытие таких файлов или попытка «развернуть» архив может привести к зависанию системы. При этом одинаково опасны как умышленные атаки этого типа, например, отказ в обслуживании и «почтовые бомбы», так и неумышленные, когда пользователи отправляют электронные сообщения с вложениями большого объема, не подумав о том, к каким последствиям может привести открытие подобного файла на компьютере адресата. Действенный способ избавиться от засорения СЭС и ее перегрузки – фильтрация по объему передаваемых данных, по количеству вложений электронного сообщения и глубине вложенности архивированных файлов.

Другой особенностью СЭС является ее доступность и простота в использовании. Во многом результатом этого стало широкое и повсеместное применение Интернета. Стихийность развития и отсутствие единых правил функционирования почтового сервиса привели к неконтролируемому использованию электронной почты и, как следствие, к возникновению целого ряда угроз, связанных с неуправляемой циркуляцией электронных сообщений в сети.

Отсутствие контроля за потоком электронных сообщений, как правило, становится причиной того, что сотрудники организации используют СЭС в целях, не связанных с деятельностью организации, например для обмена видеофайлами и графикой, частной переписки, ведения собственного бизнеса с использованием почтовых ресурсов организации, рассылки резюме в различные организации и др. Это приводит к резкому падению производительности труда в целом по организации, поскольку результатом такой деятельности сотрудников является:

- снижение производительности работы АИС (увеличение объема неделового трафика);
- снижение производительности работы отдельного сотрудника (неоправданная потеря рабочего времени);
- засорение ресурсов АИС (занятие дискового пространства под неделовые сообщения).

Кроме того, к такому же результату может привести непродуктивное использование почтовых ресурсов в трудовой деятельности сотрудников (например, чрезмерное увлечение почтовой перепиской в случаях, когда необходимости в такой переписке нет, использование СЭС не по назначению и др.). Причиной этого, как правило, является отсутствие в организации правил, регламентирующих при-

менение системы электронных сообщений. Последствиями непродуктивного использования СЭС являются снижение производительности труда в организации, а также излишние финансовые затраты. Сэкономить средства поможет проведение анализа эффективности использования СЭС, которая основывается на базе статистических данных о функционировании системы. Подобную статистику можно получить лишь в случае ведения архива СЭС. Обработка информации, содержащейся в архиве, позволяет получать отчеты о различных параметрах СЭС, ее объемах и структуре, представить наглядную картину использования почтового трафика сотрудниками организации, а это, в свою очередь, поможет предотвратить использование СЭС, несвязанное с деятельностью организации, и повысить эффективность работы систем ВЭД организации и МЭД.

Передача в электронных сообщениях графических, видео- и звуковых файлов, которые, как правило, имеют большой объем, приводит к значительной перегрузке сети и, соответственно, к дополнительным финансовым затратам на ее обслуживание. Избежать этого, а значит добиться значительной экономии средств организации, поможет так называемая отложенная доставка сообщений. Сообщения больших объемов доставляются в то время, когда загрузка сети не имеет критического значения (например, в ночное время, в выходные дни и т.д.).

К засорению трафика ведет также рассылка спама. Как правило, это сообщения, содержащие навязчивые предложения самых разнообразных услуг, товаров и др. Такого рода сообщения являются «группой риска» с точки зрения переноса вирусов. Большое количество ненужных сообщений загружает каналы, «замусоривает» почтовые ящики, отнимает время на удаление ненужных сообщений и повышает вероятность случайного удаления нужных.

Использование списков рассылки, в которые могут входить все пользователи одной сети, и получение ими одновременно сообщений рекламного характера грозит организации снижением производительности ее сетевых ресурсов. Блокировка спама в первую очередь связана с контекстным анализом сообщений, т.е. с проверкой электронных сообщений на наличие ключевых слов и выражений, которые обычно употребляются в сообщениях рекламного характера.

Переписка с внешними корреспондентами представляет наибольшую угрозу из-за особенностей СЭС: невозможностью контролировать маршрут передачи сообщений, а также их копирование и перенаправление, осуществлять аутентификацию отправителя/получателя, возвращать сообщения после их отправления. Невозможен

либо затруднен контроль количества отправляемых копий сообщения. Содержимое сообщения может быть прочитано в процессе передачи его по Интернету, поскольку заголовки и содержимое часто передаются в открытом виде.

Другой проблемой, связанной с особенностями СЭС, является то, что система допускает неконтролируемое накопление информации в архивах и «почтовых ящиках» и практически неуничтожима. В противоположность бытующему мнению о том, что удалить электронное сообщение легко, сделать это непросто. Резервные копии сообщений могут оставаться на персональных компьютерах отправителя и получателя или в сети организации, где они работают. Если электронное сообщение отправлено через коммерческую службу или Интернет, то оно будет передаваться через несколько различных серверов. Каждый сервер в цепочке между отправителем и получателем может сохранить копию сообщения в своих архивах. Методичное выяснение местонахождения каждой копии электронного сообщения с последующим его удалением не дает никакой гарантии того, что сообщение не осталось на жестком диске компьютера или сервера. С помощью широко доступного программного обеспечения рядовой пользователь сможет восстановить сообщение после того, как его якобы удалили.

Все эти особенности, а также простота копирования электронного сообщения и невозможность проконтролировать данную операцию приводят к тому, что сотрудник может передать информацию любому количеству людей как внутри организации, так и за ее пределами анонимно и без соответствующего разрешения, сразу или по истечении какого-либо времени. При этом такая информация может составлять служебную тайну организации: тексты договоров, сведения о планируемых торгах, пароли, системные данные, исходные коды программ или другую конфиденциальную информацию. Это в конечном счете грозит нарушением конфиденциальности и может привести к отрицательным для организации последствиям.

В отличие от бумажной корреспонденции электронное сообщение легко неумышленно отправить по неверному адресу. Причиной этого может быть как неумелое использование адресных книг, так и ошибка в указании адреса получателя или случайный выбор опции, предусматривающей рассылку сообщения большой группе пользователей, в то время как сообщение является конфиденциальным.

Чтобы обеспечить защиту от утечки конфиденциальной информации из сети, необходимо обеспечить контроль адресатов, фильтрацию передаваемых данных на наличие в текстах сообщений или

в прикрепленных к ним файлах слов и выражений, имеющих отношение к закрытой тематике, разграничение доступа различных категорий пользователей к архивам системы электронных сообщений и т.д.

Одно из основных отличий системы электронных сообщений состоит в формальном к ней отношении (по сравнению с другими видами коммуникаций). Большинство пользователей относятся к СЭС как к чему-то временному, т.е. поступают с ней по принципу «прочитал и выкинул». При таком отношении существует угроза случайного удаления значимой информации. Кроме того, существует опасность потери переписки с партнерами. Формальное отношение к СЭС приводит к тому, что из-за кажущейся недолговечности электронных сообщений люди часто используют их для того, чтобы выразить чувства и мнения в выражениях, которые они никогда не позволили бы себе употребить в традиционных письмах. Публикация таких сообщений в сети может нанести серьезный ущерб репутации организации или явиться причиной юридических исков к ней.

Еще одна область, связанная с возможностью привлечения к юридической ответственности организации и ее сотрудников, – нарушение авторского права. Защищенные этим правом материалы могут содержаться или в электронном сообщении, или в присоединенных файлах. К подобным материалам относятся графическая, аудио, видео и различная текстовая информация, т.е. любая информация, которая может быть представлена в электронном виде и передана по компьютерным сетям. Копирование или распространение этих материалов без предварительного согласия автора или владельца авторских прав является нарушением закона. Если организация допускает, чтобы материалы СЭС, защищенные авторским правом, использовались сотрудниками, не имеющими на это полномочий, то организация может быть привлечена к ответственности за пособничество нарушению авторского права.

Все эти проблемы решаются путем создания в организации архива СЭС.

8.9.3. Защита системы электронных сообщений

Учитывая угрозы, связанные с использованием СЭС, организациям необходимо принять соответствующие защитные меры. Подход к защите должен быть всесторонним и комплексным – необходимо сочетать организационные меры с использованием соответствующих технических средств.

К организационным мерам относятся разработка и внедрение в организации политики использования системы электронных сообщений. Технические средства должны обеспечить выполнение данной политики за счет как мониторинга почтового трафика, так и адекватного реагирования на нарушения.

Порядок использования СЭС первичен по отношению к средствам ее реализации, поскольку составляет основу для формирования комплекса мер по защите АИС от угроз. В начале необходимо сформулировать политику, составить правила использования СЭС, определить, как созданная система должна реагировать на определенные нарушения этих правил и только затем переводить их на компьютерный язык того средства, с помощью которого контролируется выполнение положений использования СЭС.

К техническим средствам относится специальное программное обеспечение, называемое «Система контроля содержимого СЭС». В функции системы входят контроль трафика и ведение архива переписки. К данной системе предъявляются следующие требования:

- проведение текстового анализа;
- фильтрация передаваемых данных – по размеру и объему данных; количеству вложений в сообщения электронной почты; типу файлов, вложенных в электронное сообщение; адресу электронного сообщения;
- контроль использования почтовых ресурсов и разграничение доступа к ним различных категорий пользователей;
- отложенная доставка электронных сообщений по расписанию;
- ведение полнофункционального архива системы электронных сообщений.

Выполнение данных требований обеспечивается применением в средствах защиты определенных механизмов. К таким механизмам могут относиться: рекурсивная декомпозиция (специальный алгоритм, применяемый для разбора электронных сообщений на составляющие компоненты с последующим анализом их содержимого); эвристическое определение кодировок текстов; определение типа файлов по сигнатуре; полнотекстовый поиск по архиву системы электронных сообщений и т.д.

8.9.4. Средства реализации правил использования системы электронных сообщений

Внедрение политики использования СЭС требует от руководства организации понимания того, что наличие только документально оформленных правил не гарантирует ее выполнения. Необходимо

создание соответствующих условий их реализации. При этом важным условием является наличие программно-технических средств контроля за выполнением положений и требований правил. К таким средствам относятся системы контроля содержимого СЭС – программное обеспечение, способное анализировать содержание сообщений по различным компонентам и структуре в целях реализации правил их использования. Отметим также особенности данного программного обеспечения, как:

- применение при анализе содержания специально разработанных правил использования СЭС;
- способность осуществлять «рекурсивную декомпозицию» электронных сообщений;
- возможность распознавания реальных форматов файлов вне зависимости от способов их маскировки (искажение расширения файлов, архивирование файлов и т.д.);
- анализ множества параметров электронных сообщений;
- ведение архива системы электронных сообщений;
- анализ содержимого электронного сообщения и прикрепленных файлов на наличие запрещенных к использованию слов и выражений.

Спектр возможностей всех категорий систем контроля содержимого СЭС достаточно широк и существенно меняется в зависимости от производителя. Однако ко всем системам предъявляются следующие наиболее общие требования, которые позволяют решать задачи, связанные с контролем почтового трафика.

Полнота. Это способность систем контроля обеспечить наиболее глубокую проверку сообщений. Это предполагает, что фильтрация должна производиться по всем компонентам электронного сообщения. При этом ни один из объектов, входящих в структуру электронного сообщения, не должен быть «оставлен без внимания». Условия проверки сообщений должны учитывать все проблемы, риски и угрозы, которые могут существовать в организации, использующей систему электронных сообщений.

Адекватность. Это способность систем контроля содержимого как можно более полно воплощать словесно сформулированную политику использования СЭС, иметь все необходимые средства реализации написанных людьми правил в понятные системе условия фильтрации.

Текстовый анализ (анализ ключевых слов и выражений с помощью встроенных словарей). Позволяет обнаружить и своевременно предотвратить утечку конфиденциальной информации, установить наличие непристойного или запрещенного содержания, остановить

рассылку спама, а также передачу других запрещенных материалов. При этом качественный анализ текста должен предполагать морфологический анализ слов, т. е. система должна иметь возможность генерировать и определять всевозможные грамматические конструкции слова. Эта функция приобретает большое значение в связи с особенностями русского языка, в котором слова имеют сложные грамматические конструкции.

Контроль отправителей и получателей электронных сообщений. Позволяет фильтровать почтовый трафик, тем самым реализуя некоторые функции межсетевого экрана в системе.

Разбор электронных сообщений на составляющие их компоненты (MIME-заголовки, тело сообщения, прикрепленные файлы и т.д.), устранение «опасных» вложений и последующий сбор компонентов сообщения воедино, причем с возможностью добавлять к сообщению необходимые для администраторов безопасности элементы (например, предупреждения о наличии вирусов или запрещенного текста в содержании сообщения).

Блокировка или задержка сообщений большого размера до того момента, когда канал связи будет менее всего загружен, например в нерабочее время. Циркуляция в СЭС организации таких сообщений может привести к перегрузке сети, а блокировка или отложенная доставка позволят этого избежать.

Распознавание графических, видео- и звуковых файлов. Как правило, такие файлы имеют большой размер, и их циркуляция может привести к потере производительности сетевых ресурсов. Поэтому способность распознавать и задерживать данные типы файлов позволяет предотвратить снижение эффективности работы организации.

Обработка сжатых/архивных файлов. Дает возможность проверять сжатые файлы на содержание в них запрещенных материалов.

Распознавание исполняемых файлов. Как правило, такие файлы имеют большой размер и редко относятся к деятельности организации. Кроме того, они являются основным источником заражения вирусами, передаваемыми с электронными сообщениями. В связи с этим способность распознавать и задерживать данные типы файлов позволяет предотвратить снижение эффективности работы организации и избежать заражения АИС.

Контроль и блокирование спама. Циркуляция спама приводит к перегрузке сети и потере рабочего времени сотрудников. Функция контроля и блокирования спама позволяет сберечь сетевые ресурсы и предотвратить снижение эффективности работы организации. Основными способами защиты от спама являются: проверка имен доменов и IP-адресов источников рассылки спама по спискам, за-

прос на указанный адрес отправителя (блокировка в случае отсутствия ответа), текстовый анализ спам-сообщения на наличие характерных слов и выражений в заголовках, проверка заголовков на соответствие спецификации и т.д.

Способность определять число вложений в электронных сообщениях. Пересылка электронного сообщения с большим количеством вложений может привести к перегрузке сети, поэтому контроль за соблюдением определенных политикой информационной безопасности ограничений на количество вложений обеспечивает сохранение ресурсов сети.

Контроль и блокирование программ-закладок, вредоносного мобильного кода (Java, ActiveX, JavaScript, VBScript и т.д.) а также файлов, осуществляющих автоматическую рассылку (так называемые Automatic Mail-to). Эти виды вложений являются опасными и приводят к утечке конфиденциальной информации из сети и систем электронного документооборота.

Категоризация ресурсов системы электронных сообщений организации: управленческий, кадровый, финансовый и т.д. и разграничение доступа сотрудников к различным категориям ресурсов сети (в том числе и в зависимости от времени суток).

Реализация различных вариантов реагирования, в том числе: удаление или временная блокировка сообщения, задержка сообщения и помещение его в карантин для последующего анализа, лечение зараженного вирусом файла, уведомление администратора безопасности или любого другого адресата о нарушении информационной безопасности и т.д.

Возможность модификации данных, которая предусматривает, например, удаление неприемлемых вложений и замену их на тексты заданного содержания. Такая возможность позволит администратору удалять из сообщений прикрепленные файлы, тип которых запрещен. К таким типам могут относиться исполняемые, видео- и звуковые файлы, не имеющие отношения к деятельности организации. В конечном счете это позволит избежать заражения сети и систем ВЭД и МЭД вирусами и добиться от сотрудников продуктивного использования СЭС.

Ведение полнофункционального архива СЭС, способного обеспечить хранение в режиме on-line большого количества электронных сообщений с высоким уровнем доступности данных. На основании хранящейся в архиве информации можно проводить дальнейший анализ информационного потока электронных сообщений организации, корректировать работу системы, осуществлять анализ инцидентов, связанных с злоупотреблением сотрудниками СЭС, и др.

Схема обработки сообщения, как правило, включает в себя следующие этапы: рекурсивную декомпозицию электронного сообщения; анализ содержимого электронного сообщения; «категоризацию» сообщения (отнесение к определенной категории); действие над сообщением по результатам присвоения категории.

Каждое попадающее в систему электронное сообщение должно проверяться на соответствие заданным условиям. При этом по меньшей мере должны выполняться следующие условия отбора сообщений:

- на заголовки сообщений;
- на структуру сообщения (наличие, количество и структура вложений);
- на типы вложений (MS Office, исполняемые, архивы и т.д.);
- на содержимое (текст) сообщений и вложений;
- на результат обработки сообщения.

Кроме того, система должна позволять анализировать сообщения по всем их составляющим: атрибутам конверта, заголовкам сообщения, MIME-заголовкам, телу сообщения, присоединенным файлам.

Следует отметить, что гибкость при фильтрации сообщений особенно необходима, когда это касается такой проблемы, как спам. Одним из главных критериев выбора системы контроля содержимого электронных сообщений в настоящее время является как раз ее способность как можно более качественно справляться с данной проблемой. Существуют четыре основные методики определения того, какое сообщение относится к спаму, а какое нет.

Первая методика используется в антиспамных фильтрах, реализующих способ выявления спама по наличию в сообщении определенных признаков, таких как наличие ключевых слов или словосочетаний, характерное написание темы сообщения, например все заглавные буквы и большое количество восклицательных знаков, а также специфическая адресная информация.

Вторая методика связана с определением адреса отправителя и его принадлежности к так называемым «черным спискам» почтовых серверов (Open Relay Black List – ORBL). В эти списки заносятся те серверы, которые замечены в массовых рассылках спама. Вообще не принимать и не транслировать сообщения, исходящие с этих серверов.

Третья методика включает обе перечисленные, но по продуктивности мало чем отличается от двух первых. Некачественное разделение спама и обычных сообщений обусловлено в том числе и некоторой «однобокостью» стандартных фильтров. При отбраковке сообщений учитываются «плохие» признаки и не учитываются «хорошие», характерные для полезной переписки.

Этих недостатков лишена четвертая методика, которая позволяет автоматически настроить фильтры согласно особенностям индивидуальной переписки, а при обработке учитывает признаки как «плохих», так и «хороших» фильтров. Методика основывается на теории вероятностей. По имеющимся оценкам, этот метод борьбы со спамом является весьма эффективным.

Таким образом, системы контроля содержимого электронных сообщений, которые в своем составе имеют модули фильтрации спама, основанные на четвертой методике, являются в настоящее время наиболее эффективными и отвечающими современным требованиям по борьбе с рассылками рекламного характера. А это в конечном счете и явится еще одним критерием при выборе системы контроля содержимого электронных сообщений.

Требование полного разбора письма следует дополнить требованием устойчивости.

Структура сообщения подчиняется определенным правилам. Разбор сообщения на составляющие основан на применении этих правил к конкретному электронному сообщению.

Система должна надежно определять типы файлов-вложений. Под надежностью имеется в виду определение, не основанное на имени файла, а также на информации, вписываемой в сообщение клиентом при прикреплении файла (mime-type). Такая информация может быть недостоверной в результате либо сознательных попыток обмануть систему контроля, либо неправильных настроек программы электронных сообщений отправителя. Запрещать пересылку файлов типа JPEG бессмысленно, если файл picture.jpg после переименования в page.txt пройдет незамеченным.

Значение для системы имеет полнота проводимых проверок, т.е. количество и разнообразие критериев анализа электронных сообщений. При этом система должна осуществлять фильтрацию по любым атрибутам сообщений: объему сообщений и вложенных файлов; количеству и типу вложений; глубине вложенности, а также уметь анализировать содержимое прикрепленных файлов вне зависимости от того, являются ли эти файлы сжатыми или архивными. Существенным преимуществом многих продуктов является возможность создания собственного сценария обработки сообщений.

По его результатам сообщение будет отнесено к какой-нибудь категории: безопасное, важное, неразрешенное и др. Если такая категоризация проведена, то можно говорить о каких-либо действиях по отношению к проанализированному сообщению, например доставить его адресату, заблокировать и т.д. Другими словами, необходима

возможность задавать системе правила, по которым она обрабатывает сообщения. Любое правило можно представить себе как связку «условие + действие».

Отнесение сообщения к определенной категории уже может рассматриваться как неявное действие. Жесткая категоризация как основа для принятия решений по электронному сообщению оказывается непрактичной. Например, выделили категорию «сообщение, отправленное на запрещенный адрес» для того, чтобы блокировать его доставку. С другой стороны, категория «сообщения руководства организации» говорит о том, что его надо, безусловно, отправлять. Такая «свободная категоризация» позволит системе гибко реагировать на самые различные комбинации данных, содержащихся в сообщениях.

В последнее время большое значение для обеспечения информационной безопасности АИС приобрело наличие в организации архива электронных сообщений. Некоторые разработчики систем контекстного анализа предусматривают прикрепление к своим продуктам специальных модулей архивирования. Именно наличие архива определяет в настоящее время полнофункциональность продуктов этой категории. При этом ведение архива — это не просто автоматическая архивация сообщений в файл, а способность регистрации сообщений и учета необходимой информации на протяжении всего жизненного цикла сообщения, возможность получения любых выборок и статистики из архива по запросам, созданным с использованием любых критериев.

Кроме того, долговременный архив не только предоставляет возможность ретроспективного анализа информационных потоков электронных сообщений и позволяет найти виновных в нарушении принятых в организации правил по прошествии определенного времени, но и дает материал для построения объективных и обоснованных правил использования СЭС.

Отличительным признаком средств контекстного анализа является способность накопления статистики и генерации отчетов. Многие продукты имеют в своем арсенале только встроенные формы отчетов, другие способны осуществлять лишь просмотр статистики работы конкретного пользователя СЭС. Вероятно, наиболее совершенными являются системы, которые способны обеспечить получение любых выборок и статистики из архива по запросам, создание специфических запросов, генерацию любых видов отчетов для анализа эффективности использования почтового сервиса организации.

Существуют несколько систем контроля содержимого СЭС с открытой архитектурой. В стандартный комплект поставки таких систем, как правило, входят несколько модулей, каждый из которых

обеспечивает защиту от определенного вида угроз или решает отдельную задачу безопасности функционирования системы электронных сообщений. Например, в состав системы может входить модуль ЭЦП и шифрования, который обеспечивает конфиденциальность и контроль целостности пересылаемой информации (см. приложение 7).

Большое значение для систем контроля содержимого имеет удобство администрирования системы, что предполагает наличие русскоязычного интерфейса, возможности разделения функций управления и администрирования системы, т.е. разграничения доступа различных категорий пользователей к средствам управления системой.

В настоящее время деятельность организаций, государственных и негосударственных структур все больше зависит от СЭС. Однако нельзя не учитывать проблемы, которые возникают в связи с ее неконтролируемым использованием. Сейчас существуют средства реализации серьезных преимуществ СЭС, которые помогают устранить угрозы надежности, конфиденциальности и продуктивности организации — это системы контроля содержимого СЭС.

Системы контроля, помимо основной своей задачи мониторинга почтового трафика, способны выполнять и другие функции. Практика показала, что в настоящее время такие системы используются в качестве:

- основы систем ВЭД и МЭД;
- средств управления потоком сообщений;
- средств управления доступом;
- средств администрирования и хранения СЭС.
- средств аудита контента, важнейшую функцию которого осуществляет архив электронных сообщений.

В заключение следует отметить, что необходимость систем контроля содержимого электронных сообщений подтверждается «Специальными требованиями и рекомендациями по технической защите конфиденциальной информации», разработанными Гостехкомиссией при Президенте Российской Федерации в 2001 г. (СТР-К). В ст. 6.3.11.5 этого документа определено: «В целях контроля за правомерностью использования абонентских пунктов и выявления нарушения 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 абонентских пунктов для последующего анализа со стороны администратора (службы безопасности)».

Таким образом, все перечисленные выше факты еще раз указывают на необходимость применения в системах информационной безопасности сетей систем контроля содержимого СЭС, или, иными словами, системы электронной почты, которые способны не только обеспечить защиту системы электронных сообщений и стать эффективным элементом управления информационным потоком, но и значительно повысить эффективность деятельности организации.

Приложение 1

Перечень информации, которую в соответствии с законодательством Российской Федерации запрещено относить к информации ограниченного доступа

1. В соответствии с Законом Российской Федерации «О государственной тайне», не подлежит засекречиванию информация:

1.1. О чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях.

1.2. О состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности.

1.3. О привилегиях, компенсациях и льготах, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям.

1.4. О фактах нарушения прав и свобод человека и гражданина.

1.5. О размерах золотого запаса и государственных валютных резервах Российской Федерации.

1.6. О состоянии здоровья высших должностных лиц Российской Федерации.

1.7. О фактах нарушения законности органами государственной власти и их должностными лицами.

2. В соответствии с Федеральным законом «Об информации, информационных технологиях и защите информации» [ст. 8, п. 4], доступ не может быть ограничен:

2.1. К нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления.

2.2. К информации о состоянии окружающей среды.

2.3. К информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну).

2.4. К информации, накапливаемой в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией.

2.5. К иной информации, недопустимость ограничения доступа к которой установлена федеральными законами.

3. В соответствии с Федеральным законом «О коммерческой тайне» [ст. 5] определены следующие виды информации, которые нельзя относить к коммерческой тайне:

3.1. Информация, содержащаяся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры.

3.2. Информация, содержащаяся в документах, дающих право на осуществление предпринимательской деятельности.

3.3. Сведения о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов.

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

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

3.6. Сведения о задолженности работодателей по выплате заработной платы и иным социальным выплатам.

3.7. Сведения о нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений.

3.8. Сведения об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности.

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

3.10. Перечень лиц, имеющих право действовать без доверенности от имени юридического лица.

3.11. Сведения обязательность раскрытия которых или недопустимость ограничения доступа к которым установлена иными федеральными законами (см. п. 1 и 2 данного перечня).

4. В соответствии с Налоговым кодексом Российской Федерации 31 июля 1998 г. № 146-ФЗ [ст. 102] определены следующие виды информации, которые нельзя относить к налоговой тайне:

4.1. Сведения о налогоплательщике, разглашенные им самостоятельно или с его согласия.

4.2. Идентификационный номер налогоплательщика.

4.3. Сведения о нарушениях законодательства о налогах и сборах и мерах ответственности за эти нарушения.

4.4. Сведения о предоставляемых налоговым (таможенным) или правоохранительным органам других государств в соответствии с международными договорами (соглашениями), одной из сторон которых является Российская Федерация, о взаимном сотрудничестве между налоговыми (таможенными) или правоохранительными органами (в части сведений, предоставленных этим органам).

4.5. Сведения, предоставляемые избирательным комиссиям в соответствии с законодательством о выборах, по результатам проверок налоговым органом о размере и источниках доходов кандидата и его супруги, а также об имуществе, принадлежащем кандидату и его супруге на праве собственности.

5. В соответствии с Постановлением Правительства Российской Федерации от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти» [110], могут быть отнесены к служебной информации ограниченного распространения:

5.1. Акты законодательства, устанавливающие правовой статус государственных органов, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации.

5.2. Сведения о чрезвычайных ситуациях, опасных природных явлениях и процессах, экологическая, гидрометеорологическая, гидрогеологическая, демографическая, санитарно-эпидемиологическая и другая информация, необходимая для обеспечения безопасного существования населенных пунктов, граждан и населения в целом, а также производственных объектов.

5.3. Описание структуры органа исполнительной власти, его функций, направлений и форм деятельности, а также его адрес.

5.4. Порядок рассмотрения и разрешения заявлений, а также обращений граждан и юридических лиц.

5.5. Решения по заявлениям и обращениям граждан и юридических лиц, рассмотренным в установленном порядке.

5.6. Сведения об исполнении бюджета и использовании других государственных ресурсов, о состоянии экономики и потребностей населения.

5.7. Документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах организаций, необходимые для реализации прав, свобод и обязанностей граждан.

6. В соответствии с Постановлением Правительства Российской Федерации от 12 февраля 2003 № 98 «Об обеспечении доступа к информации о деятельности Правительства Российской Федерации и федеральных органов исполнительной власти», утверждены перечни сведений о деятельности Правительства Российской Федерации и федеральных органов исполнительной власти, обязательных для размещения в информационно-телекоммуникационной сети Интернет. Нормативные правовые акты, предусмотренные настоящим перечнем, размещаются в информационно-телекоммуникационной сети Интернет с указанием сведений об их официальном опубликовании:

6.1. Сведения о деятельности Правительства Российской Федерации:

6.1.1. Федеральные законы, указы Президента Российской Федерации и иные нормативные правовые акты, составляющие правовую основу деятельности Правительства Российской Федерации, в том числе:

Регламент Правительства Российской Федерации;

Положение об аппарате Правительства Российской Федерации.

6.1.2. Нормативные правовые и иные акты Правительства Российской Федерации, в том числе:

о внесении изменений и дополнений в нормативные правовые акты Правительства Российской Федерации;

о признании утратившими силу нормативных правовых актов Правительства Российской Федерации.

6.1.3. Сведения о решениях судов о признании недействующими актов Правительства Российской Федерации.

6.1.4. Сведения о составе, задачах и деятельности координационных и совещательных органов, образуемых Правительством Российской Федерации.

6.1.5. Общие сведения о принятых Правительством Российской Федерации федеральных целевых программах (наименование, цели, основные задачи, заказчики, головные исполнители, объем финансирования, сроки и ожидаемые результаты реализации).

6.1.6. Сведения о законопроектной деятельности Правительства Российской Федерации:

планы законопроектной деятельности Правительства Российской Федерации, а также сведения об их исполнении;

проекты федеральных законов, внесенных Правительством Российской Федерации в Государственную Думу Федерального Собрания Российской Федерации;

заключения Правительства Российской Федерации по законопроектам;

официальные отзывы Правительства Российской Федерации на законопроекты, рассматриваемые палатами Федерального Собрания Российской Федерации;

поправки к законопроектам.

6.1.7. Сведения о программах и планах деятельности Правительства Российской Федерации.

6.1.8. Сведения об официальных визитах и рабочих поездках Председателя Правительства Российской Федерации и членов Правительства Российской Федерации, а также правительственных делегаций.

6.1.9. Сведения о мероприятиях, проводимых в официальной резиденции Правительства Российской Федерации (заседания, совещания, встречи, пресс-конференции, семинары и брифинги, «круглые столы»), и иная информация о повседневной деятельности Правительства Российской Федерации.

6.1.10. Тексты официальных выступлений и заявлений Председателя Правительства Российской Федерации и членов Правительства Российской Федерации.

6.1.11. Повестка дня заседания Правительства Российской Федерации, а также сведения о материалах к заседанию Правительства Российской Федерации и его итогах.

6.1.12. Сведения о решениях, принятых на заседаниях Правительства Российской Федерации, и об их исполнении.

6.1.13. Сведения о взаимодействии Правительства Российской Федерации с иными органами государственной власти Российской Федерации, общественными объединениями, политическими партиями, профессиональными союзами и другими организациями, в том числе международными.

6.1.14. Перечни и тексты международных договоров и соглашений Российской Федерации, заключенных (подписанных) Правительством Российской Федерации.

6.1.15. Сведения об основных показателях социально-экономического развития Российской Федерации и исполнении федерального бюджета.

6.1.16. Обзоры обращений граждан и организаций в Правительство Российской Федерации, обобщенная информация о результатах рассмотрения таких обращений и о принятых мерах.

6.1.17. Сведения о государственной службе в Аппарате Правительства Российской Федерации:

порядок поступления на государственную службу в Аппарат Правительства Российской Федерации;

квалификационные требования к кандидатам на замещение вакантных государственных должностей государственной службы в Аппарате Правительства Российской Федерации;

перечень вакантных государственных должностей государственной службы в Аппарате Правительства Российской Федерации;

условия и результаты конкурсов на замещение вакантных государственных должностей государственной службы в Аппарате Правительства Российской Федерации.

6.1.18. Сведения о Председателе Правительства Российской Федерации и членах Правительства Российской Федерации, руководителях федеральных органов исполнительной власти, заместителях Руководителя Аппарата Правительства Российской Федерации, руководителях структурных подразделений Аппарата Правительства Российской Федерации, а также руководителях организаций и органов, образованных при Правительстве Российской Федерации (фамилии, имена, отчества и, по согласованию с указанными лицами, — биографические данные).

6.1.19. Сведения о задачах и функциях структурных подразделений аппарата Правительства Российской Федерации, организаций и органов, образованных при Правительстве Российской Федерации.

6.1.20. Телефоны и адресные реквизиты (почтовый адрес, адрес электронной почты и др.) подразделения по работе с обращениями граждан Аппарата Правительства Российской Федерации, сведения о порядке его работы, телефоны справочной службы.

6.2. Сведения о деятельности федеральных органов исполнительной власти:

6.2.1. Федеральные законы, указы Президента Российской Федерации, акты Правительства Российской Федерации и иные нормативные правовые акты, регулирующие сферу деятельности федерального органа исполнительной власти и определяющие задачи, функции, права, обязанности и ответственность федерального органа исполнительной власти и его территориальных органов.

6.2.2. Акты (постановления, приказы, распоряжения, правила, инструкции, положения и др.) федерального органа исполнительной власти, в том числе:

о внесении изменений и дополнений в акты федерального органа исполнительной власти;

о признании утратившими силу актов федерального органа исполнительной власти.

6.2.3. Сведения о решениях судов о признании недействующими актов федерального органа исполнительной власти.

6.2.4. Сведения о государственной регистрации Министерством юстиции Российской Федерации нормативных правовых актов федерального органа исполнительной власти в случаях, установленных законодательством Российской Федерации.

6.2.5. Порядок деятельности федерального органа исполнительной власти, его территориальных органов и подведомственных ему организаций по обеспечению реализации определенных законодательством Российской Федерации прав, свобод и законных интересов граждан.

6.2.6. Сведения о реализации федеральных целевых программ, заказчиком или исполнителем которых является федеральный орган исполнительной власти.

6.2.7. Сведения об официальных визитах и рабочих поездках руководителей и официальных делегаций федерального органа исполнительной власти.

6.2.8. Сведения об официальных мероприятиях, организуемых федеральным органом исполнительной власти и его территориальными органами (заседания, встречи, брифинги, семинары, «круглые столы» и др.).

6.2.9. Тексты официальных выступлений и заявлений руководителя и заместителей руководителя федерального органа исполнительной власти, его территориальных органов.

6.2.10. Перечни и существенные условия договоров гражданско-правового характера, заключенных федеральным органом исполнительной власти с организациями.

6.2.11. Сведения о международных договорах и соглашениях, в реализации которых принимает участие федеральный орган исполнительной власти.

6.2.12. Сведения о проектах федеральных законов, федеральных целевых программ и концепций, разрабатываемых федеральным органом исполнительной власти.

6.2.13. Аналитические доклады и обзоры информационного характера о деятельности федерального органа исполнительной власти.

6.2.14. Сведения о взаимодействии федерального органа исполнительной власти, его территориальных органов и подведомственных ему организаций с иными органами государственной власти

Российской Федерации, общественными объединениями, политическими партиями, профессиональными союзами и другими организациями, в том числе международными.

6.2.15. Обзоры обращений граждан и организаций в федеральный орган исполнительной власти, обобщенная информация о результатах рассмотрения таких обращений и о принятых мерах.

6.2.16. Сведения об основных показателях, характеризующих ситуацию в отрасли, входящей в сферу ведения федерального органа исполнительной власти, и динамику ее развития.

6.2.17. Прогнозы, подготовленные федеральным органом исполнительной власти, его территориальными органами и подведомственными ему организациями в соответствии с их компетенцией.

6.2.18. Официальная статистическая информация, собранная и обработанная федеральным органом исполнительной власти и его территориальными органами.

6.2.19. Сведения об открытых конкурсах, аукционах, тендерах, экспертизах и других мероприятиях, проводимых федеральным органом исполнительной власти, его территориальными органами и подведомственными ему учреждениями, в том числе:

условия их проведения;

порядок участия в них физических и юридических лиц;

составы конкурсных комиссий, создаваемых федеральным органом исполнительной власти, его территориальными органами и подведомственными ему учреждениями для проведения конкурсов на поставку товаров (выполнение работ, оказание услуг) для государственных нужд;

протоколы заседаний конкурсных комиссий;

порядок обжалования решений, принятых федеральным органом исполнительной власти, его территориальными органами и подведомственными ему учреждениями.

6.2.20. Формы заявлений, принимаемых федеральным органом исполнительной власти и его территориальными органами к рассмотрению в соответствии с законодательством Российской Федерации, в том числе с нормативными правовыми актами федерального органа исполнительной власти.

6.2.21. Перечни федеральных информационных систем, банков данных, реестров, регистров, находящихся в ведении федерального органа исполнительной власти, его территориальных органов и подведомственных ему учреждений, а также перечни информационных ресурсов и услуг, предоставляемых гражданам и организациям.

6.2.22. Сведения об исполнении федерального бюджета федеральным органом исполнительной власти.

6.2.23. Сведения о направлениях расходования средств иностранной технической помощи, предоставляемой по проектам, осуществляемым с участием федерального органа исполнительной власти.

6.2.24. Сведения о результатах проверок, проведенных федеральным органом исполнительной власти, его территориальными органами и подведомственными ему учреждениями в пределах их компетенции, а также проверок, проведенных в этих органах и организациях.

6.2.25. Сведения о состоянии защиты населения и территорий от чрезвычайных ситуаций и принятых мерах по обеспечению их безопасности, о прогнозируемых и возникших чрезвычайных ситуациях, о приемах и способах защиты населения от них, а также иные сведения, подлежащие доведению федеральным органом исполнительной власти до граждан и организаций в соответствии с федеральными законами.

6.2.26. Сведения о государственной службе в федеральном органе исполнительной власти:

порядок поступления граждан на государственную службу в федеральный орган исполнительной власти;

перечень вакантных государственных должностей государственной службы в федеральном органе исполнительной власти;

квалификационные требования к кандидатам на замещение вакантных государственных должностей государственной службы в федеральном органе исполнительной власти;

условия и результаты конкурсов на замещение вакантных государственных должностей государственной службы в федеральном органе исполнительной власти.

6.2.27. Сведения о руководителях федерального органа исполнительной власти, его структурных подразделений, зарубежных представительств, территориальных органов и подведомственных ему организаций (фамилии, имена, отчества и, по согласованию с указанными лицами, — биографические данные).

6.2.28. Структура федерального органа исполнительной власти, сведения о задачах и функциях его структурных подразделений, телефоны справочной службы и адресные реквизиты (почтовый адрес, адрес электронной почты и др.) федерального органа исполнительной власти, его структурных подразделений, территориальных органов и подведомственных ему организаций.

6.2.29. Сведения об организациях, подведомственных федеральному органу исполнительной власти (перечень организаций, их почтовые и юридические адреса, телефоны, сведения о создании, реорганизации и ликвидации, основные показатели деятельности).

6.2.30. Телефоны и адресные реквизиты (почтовый адрес, адрес электронной почты и др.) подразделений по работе с обращениями граждан федерального органа исполнительной власти, его территориальных органов и подведомственных ему организаций, сведения о порядке работы этих подразделений.

6.2.31. Перечень зарубежных представительств федерального органа исполнительной власти, их телефоны и адресные реквизиты (почтовый адрес, адрес электронной почты и др.).

6.2.32. Сведения об участии федерального органа исполнительной власти в реализации международных договоров Российской Федерации, межведомственных международных договоров и программ международного сотрудничества.

6.2.33. Перечень международных организаций, в деятельности которых принимает участие федеральный орган исполнительной власти.

6.2.34. Реестры лицензий, ведение которых осуществляется федеральными органами исполнительной власти.

6.2.35. Административные регламенты, стандарты государственных и муниципальных услуг.

Приложение 2

Примерный перечень конфиденциальной документированной информации, составляющей служебную и коммерческую тайны, секрет производства (ноу-хау)

1. Производственная информация

1.1. О структуре производства, производственных мощностях, типе оборудования, запасах сырья и готовой продукции.

1.2. О применяемых производственных технологиях.

1.3. О планах производства новой продукции.

1.4. Конструкторские разработки по производству какой-либо продукции и ее технические параметры.

1.5. Об эффективности и возможности производственных методов, оборудования и систем.

1.6. О рецептурах производства какой-либо продукции.

2. Управленческая информация

2.1. О применяемых методах управления организацией.

2.2. О подготовке, принятии и исполнении решений руководства по производственным, научно-техническим, коммерческим и организационным вопросам.

2.3. Организационные схемы, оргструктура.

2.4. Системы документооборота, включая электронные, разработанные формы документов, положений, инструкций, договоров, номенклатуры дел и т. п.

2.5. О совещаниях по различным вопросам, включая факты проведения совещаний и заседаний органов управления организации.

2.6. О переговорах – целях, задачах, тактике и стратегии ведения переговоров с деловыми партнерами.

2.7. О кадрах и персонале – личные дела сотрудников, контракты и договоры с ними, списки персонала, кадровая отчетность и другая информация о сотрудниках, включая их характеристики. Также образовательных методиках, программах тренингов, оценке персонала и т. д., разработанных в организации.

2.8. Коммерческие контракты, договоры и информация о них – условия заключения, платежи и услуги, протоколы о намерениях и т. д.

2.9. О финансовом состоянии организации, кроме информации, которая, согласно Федеральному закону «О коммерческой тайне», не может составлять коммерческую тайну (охраняется информация о состоянии банковских счетов организации, о долговых обязательствах, о состоянии кредитов, о финансовых операциях и т. д.).

3. Планы, информация и отчетность по ним

3.1. О расширении или свертывании производства различных видов продукции и их технико-экономических обоснованиях.

3.2. Об инвестициях, закупках и продажах.

3.3. О производстве, включая производство новой продукции.

3.4. Бизнес-планы и другие деловые планы.

3.5. Стратегические и тактические планы развития организации.

4. Маркетинговая информация:

4.1. О применяемых методах изучения рынка.

4.2. О маркетинговых исследованиях и их результатах, содержащих оценки состояния и перспективы развития рыночной конъюнктуры.

4.3. О рыночной стратегии и тактике организации.

4.4. О применяемых методах осуществления продаж.

4.5. Об эффективности коммерческой деятельности.

4.6. О регионах сбыта готовой продукции.

4.7. О заинтересованности в приобретении товара.

4.8. О методах расчета, структуре, уровне цен, размеров скидок.

4.9. О подготовке к торгам или аукциону и их результатах.

4.10. Об исследовании рынка, конкурентов, потребителей и т.д., включая оригинальные методики исследования.

4.11. Стратегия и тактика проведения рекламных кампаний.

5. Информация о внутренних и зарубежных партнерах

5.1. О заказчиках.

5.2. О подрядчиках, поставщиках.

5.3. О клиентах, потребителях, покупателях.

5.4. О компаньонах, спонсорах, посредниках и других партнерах.

6. Научная, техническая, технологическая информация

6.1. О целях, задачах и программах научных исследований.

6.2. Ноу-хау, оригинальные идеи НИОКР, научно-исследовательские проекты.

6.3. Конструкционные характеристики создаваемых изделий и их параметры.

6.4. О разрабатываемых технологических процессах (размеры, объемы, конфигурация, процентное содержание компонентов, химические формулы, температура, давление, время и т. д.).

6.5. Аналитические и графические зависимости, отражающие найденные закономерности и взаимосвязи.

6.6. Данные об условиях экспериментов и оборудовании, на котором они проводились.

6.7. О материалах, из которых изготовлены детали.

6.8. Об особенностях конструкторско-технологического и художественно-технического решения изделия (дизайн).

6.9. О методах защиты от всевозможных подделок.

6.10. О состоянии программного и компьютерного обеспечения.

6.11. Заявки на патенты.

6.12. Об особенностях используемых и разрабатываемых технологий и специфике их применения.

7. Информация о безопасности организации

7.1. О порядке, режиме, мерах по защите и охране и состоянии защиты конфиденциальности (секретности) информации (какой-либо тайны, включая коммерческую тайну).

7.2. О порядке и состоянии организации охраны, пропускном режиме, системе сигнализации.

7.3. Коммерческая тайна организаций-партнеров и переданная на доверительной основе организации.

7.4. О конкурентах (информация, которая не содержится в открытых источниках: справочниках, каталогах и др.).

7.5. Об организации защищенного (конфиденциального) документооборота, включая электронный, и технологий конфиденциального делопроизводства.

7.6. Об оборудовании, оргтехнике, компьютерах, используемом программном обеспечении, средствах их защиты, включая технические и технологические (ключи, пароли, руководства пользователей и т. д.).

Приложение 3

Перечень объективных факторов, воздействующих на информацию в соответствии с ГОСТ Р 51275—99

1. Внутренние факторы

1.1. Передача сигналов по проводным линиям связи.

1.2. Передача сигналов по оптико-волоконным линиям связи.

1.3 Излучения сигналов, функционально присущих объекту информатизации (далее – объект).

1.3.1. Излучения акустических сигналов.

1.3.1.1. Излучения неречевых сигналов.

1.3.1.2. Излучения речевых сигналов.

1.3.2. Электромагнитные излучения и поля.

1.3.2.1. Излучения в радиодиапазоне.

1.3.2.2. Излучения в оптическом диапазоне.

1.4. Побочное электромагнитное излучение (ПЭМИ).

1.4.1. ПЭМИ сигналов (видеоимпульсов) от информационных цепей.

1.4.2. ПЭМИ сигналов (радиоимпульсов) от всех электрических цепей технических средств объекта информатизации.

1.4.2.1. Модуляция ПЭМИ электромагнитными сигналами от информационных цепей.

1.4.2.2. Модуляция ПЭМИ акустическими сигналами.

1.5. Паразитные электромагнитные излучения.

1.5.1. Модуляция паразитных электромагнитных излучений информационными сигналами.

1.5.2. Модуляция паразитных электромагнитных излучений акустическими сигналами.

1.6. Наводки на объект.

1.6.1. Наводки в электрических цепях технических средств, имеющих выход за пределы объекта.

1.6.1.1. Наводки в линиях связи.

1.6.1.1.1. Наводки, вызванные ПЭМИ и (или) паразитными электромагнитными излучениями, несущими информацию.

1.6.1.1.2. Наводки, вызванные внутренними емкостными и (или) индуктивными связями.

1.6.1.2. Наводки в цепях электропитания.

1.6.1.2.1. Наводки, вызванные ПЭМИ и (или) паразитными электромагнитными излучениями, несущими информацию.

1.6.1.2.2. Наводки, вызванные внутренними емкостными и (или) индуктивными связями.

1.6.1.2.3. Наводки через блоки питания технических средств объекта.

1.6.1.3. Наводки в цепях заземления.

1.6.1.3.1. Наводки, вызванные ПЭМИ и (или) паразитными электромагнитными излучениями, несущими информацию.

1.6.1.3.2. Наводки, вызванные внутренними емкостными и (или) индуктивными связями.

1.6.1.3.3. Наводки, обусловленные гальванической связью схемной (рабочей) «земли» узлов и блоков ТС объекта информатизации.

1.6.2. Наводки на технические средства, провода, кабели и иные токопроводящие коммуникации и конструкции, гальванически не связанные с техническими средствами объекта, вызванные побочными и (или) паразитными электромагнитными излучениями, несущими информацию.

1.7. Акустоэлектрические преобразования в элементах технических средств объекта.

1.8. Дефекты, сбои, отказы, аварии технических средств и систем объекта.

1.9. Дефекты, сбои и отказы программного обеспечения объекта.

2. Внешние факторы

2.1. Явления техногенного характера.

2.1.1. Непреднамеренные электромагнитные облучения объекта.

2.1.2. Радиационные облучения объекта.

2.1.3. Сбои, отказы и аварии систем обеспечения объекта.

2.2. Природные явления, стихийные бедствия.

2.2.1. Термические факторы (пожары и др.).

2.2.2. Климатические факторы (наводнения и др.).

2.2.3. Механические факторы (землетрясения и др.).

2.2.4. Электромагнитные факторы (грозовые разряды и др.).

2.2.5. Биологические факторы (микробы, грызуны и др.).

Перечень субъективных факторов, воздействующих на защищаемую информацию

1. Внутренние факторы

1.1. Разглашение защищаемой информации лицами, имеющими к ней право доступа.

1.1.1. Разглашение информации лицам, не имеющим права доступа к защищаемой информации.

1.1.2. Передача информации по открытым линиям связи.

1.1.3. Обработка информации на незащищенных технических средствах обработки информации.

1.1.4. Опубликование информации в открытой печати и других средствах массовой информации.

1.1.5. Копирование информации на незарегистрированный носитель информации.

1.1.6. Передача носителя информации лицу, не имеющему права доступа к ней.

1.1.7. Утрата носителя с информацией.

1.2. Неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации.

1.2.1. Несанкционированное изменение информации.

1.2.2. Несанкционированное копирование информации.

1.3. Несанкционированный доступ к защищаемой информации.

1.3.1. Подключение к техническим средствам и системам объекта.

1.3.2. Использование закладочных устройств.

1.3.3. Использование программного обеспечения технических средств объекта.

1.3.3.1. Маскировка под зарегистрированного пользователя.

1.3.3.2. Использование дефектов программного обеспечения объекта.

1.3.3.3. Использование программных закладок.

1.3.3.4. Применение программных вирусов.

1.3.4. Хищение носителя защищаемой информации.

1.3.5. Нарушение функционирования технических средств обработки информации.

1.4. Неправильное организационное обеспечение защиты информации.

1.4.1. Неправильное задание требований по защите информации.

1.4.2. Несоблюдение требований по защите информации.

1.4.3. Неправильная организация контроля эффективности защиты информации.

1.5. Ошибки обслуживающего персонала объекта.

1.5.1. Ошибки при эксплуатации технических средств.

1.5.2. Ошибки при эксплуатации программных средств.

1.5.3. Ошибки при эксплуатации средств и систем защиты информации.

2. Внешние факторы

2.1. Доступ к защищаемой информации с применением технических средств.

2.1.1. Доступ к защищаемой информации с применением технических средств разведки.

2.1.1.1. Доступ к защищаемой информации с применением средств радиоэлектронной разведки.

2.1.1.2. Доступ к защищаемой информации с применением средств оптико-электронной разведки.

2.1.1.3. Доступ к защищаемой информации с применением средств фотографической разведки.

2.1.1.4 Доступ к защищаемой информации с применением средств визуально-оптической разведки.

2.1.1.5. Доступ к защищаемой информации с применением средств акустической разведки.

2.1.1.6. Доступ к защищаемой информации с применением средств гидроакустической разведки

2.1.1.7. Доступ к защищаемой информации с применением средств компьютерной разведки.

2.1.2. Доступ к защищаемой информации с использованием эффекта «высокочастотного навязывания».

2.1.2.1. Доступ к защищаемой информации с применением генератора высокочастотных колебаний.

2.1.2.2. Доступ к защищаемой информации с применением генератора высокочастотного электромагнитного поля.

2.2. Несанкционированный доступ к защищаемой информации.

2.2.1. Подключение к техническим средствам и системам объекта.

2.2.2. Использование закладочных устройств.

2.2.3. Использование программного обеспечения технических средств объекта.

2.2.3.1. Маскировка под зарегистрированного пользователя.

2.2.3.2. Использование дефектов программного обеспечения объекта.

2.2.3.3. Использование программных закладок.

2.2.3.4. Применение программных вирусов.

2.2.4. Несанкционированный физический доступ на объект.

2.2.5. Хищение носителя с защищаемой информацией.

2.3. Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку.

2.4. Действия криминальных групп и отдельных преступных субъектов.

2.4.1. Диверсия в отношении объекта.

Приложение 4

Примерный классификатор конфиденциальной информации, содержащейся в автоматизированной информационной системе

Код	Наименование групп, подгрупп и видов конфиденциальной информации	Примечание
1	2	3
100	Сведения, относящиеся к служебной тайне	–
110	Общие вопросы управления	–
111	Информация, содержащаяся в организационно-распорядительных документах организации	В части сведений, касающихся конкретных работников и организации, а также других организаций
112	Информация, связанная с подготовкой организационно-распорядительных документов организации	В случае, если их преждевременное разглашение нанесет ущерб организации и работникам организации
113	Информация, связанная с подготовкой проектов организационно-распорядительных документов	В случае, если их преждевременное разглашение приведет к созданию односторонних преимуществ для лиц, получивших доступ к указанной информации
114	Информация о запланированных, готовящихся или проводимых проверках	Планы проверок, решения об их проведении, методы и приемы проведения, места особого внимания проверяющих, аналитические материалы
115	Информация о внутриведомственных и межведомственных обсуждениях и консультациях рабочего и подготовительного характера	–
120	Сведения, переданные гражданами и организациями	В части сведений, передаваемых в государственные органы на условиях сохранения их конфиденциальности (в т.ч. заявления, рапорты, запросы, доклады, видео- и аудиозаписи, телефонограммы и т.д.)

Продолжение

1	2	3
130	Сведения, связанные с безопасностью организации	–
131	Сведения о координации взаимодействия с правоохранительными органами	Договоры, соглашения о совместной деятельности, распоряжения, приказы, директивы, оперативные планы, материалы работы межведомственных комиссий
132	Сведения о порядке и состоянии охраны	В части деятельности организации, ее пропускного режима, системы сигнализации, средств связи и оповещения (планы и схемы организации, приказы и распоряжения об организации работы службы, должностные инструкции, устройство и параметры работы средств связи)
133	Информация о проведении комплексных обследований, разработке и реализации мероприятий по защите объектов организации	Если такая информация не скрывает информацию 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, санитарии, фактах нарушения прав и свобод человека и гражданина
134	Информация о дислокации, устройстве, системе технологического доступа к охраняемым объектам организации	Подстанции, вентиляционные шахты, трубопроводы и кабели, линии связи и передачи энергии и др.
140	Информация, связанная с защитой должностных лиц и работников	–
141	Информация о возможных угрозах в адрес должностных лиц и работников организации в связи с исполнением ими своих обязанностей	–

Продолжение

1	2	3
142	Информация о порядке физической защиты должностных лиц организации и иных работников	Приказы (распоряжения об организации физической защиты, штатная структура организации)
150	Информация, связанная с чрезвычайными ситуациями	–
151	Информация о разработках технических средств, технологий и мероприятий для контроля, предупреждения, ликвидации чрезвычайных ситуаций и защиты работников	–
160	Экономическая информация	–
161	Информация о маркетинговых исследованиях	Информация, содержащая оценки состояния и перспективы развития рыночной конъюнктуры, если это нарушит интересы организации в случае публикации
162	Информация о политике подразделений организации, отвечающих за закупки товаров, работ, услуг для нужд организации	В части информации, разглашение которой противоречит интересам организации и неблагоприятно повлияет на ценовую политику участников контрактов и договоров
163	Информация о заинтересованности в приобретении товара по конкретной минимальной цене, другие условия коммерческих контрактов	В частности, материалы (протоколы) обсуждений, содержащие соответствующую информацию, распоряжения и иные решения с указанной информацией
164	Информация о применяемых негласных методах изучения экономической обстановки на соответствующих рынках, угрожающей интересам организации	Рапорты, донесения, обзоры, исследования, анализы, справки, выводы
170	Сведения по обеспечению информационной безопасности	–
171	Информация, раскрывающая систему и средства защиты информации	Включая значения действующих кодов и паролей

Продолжение

1	2	3
172	Информация об особенностях информационного, компьютерного и программного обеспечения	Информация, влекущая возможность незаконного вмешательства (утечку информации, подлог документов, искажение баз данных, разрушение системы и т. д.) в указанную деятельность
173	Информация о разработке, использовании и совершенствовании программы защиты информации	В том числе методы контроля эффективности средств защиты, структуры защищенных телекоммуникационных систем организации, средств повышения надежности специального программного обеспечения
174	Информация о системах и средствах предотвращения несанкционированного доступа	В том числе специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи
175	Оперативная информация о выявлении технических устройств и программ	В части технических устройств и программ, представляющих угрозу для нормального функционирования телекоммуникационных систем
176	Информация о применении криптографических средств защиты информации	При хранении, обработке, передаче по каналам связи, о специальных требованиях по защите информации
177	Информация о порядке контроля действий персонала, имеющего доступ к защищенным АИС системам и информационным ресурсам	Контроль действий персонала может устанавливаться по согласию на это сотрудников либо по решению суда
200	Персональные данные	–
210	Персональные данные работников	–
211	Биографические данные	Личное дело (автобиография или биография), трудовая книжка
212	Опознавательные данные	Личное дело
213	Личные характеристики	Все документы в указанной части
214	Информация о семейном положении	(Авто)биография, документы (копии) о семейном положении

Продолжение

1	2	3
215	Информация о финансовом положении	Штатное расписание, приказы по личному составу, документы (справки, ведомости) о полученных доходах
216	Информация об образовании	(Авто)биография, документы (копии) документов об образовании
217	Информация о профессиональных навыках	Все виды документов (копии) о профессиональной аттестации работника
218	Информация о состоянии здоровья	Все виды документов, содержащие информацию о состоянии здоровья
219	Иная информация по заявлениям работников	Согласно полученным заявлениям
220	Иные персональные данные	–
221	Информация о гражданах (персональные данные)	Сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность
222	Персональные данные о гражданах в их заявлениях и жалобах	–
223	Сведения, содержащиеся в записях актов гражданского состояния	Сведения о рождении, смерти, заключении брака, расторжении брака, об установлении отцовства, о перемене имени, а также сведения о тайне усыновления (удочерения), за исключением сведений, разглашение которых осуществлено по воле усыновителя
300	Сведения, составляющие коммерческую тайну	–
310	Коммерческая информация, принадлежащая третьим лицам	Информация, полученная от партнеров при взаимодействии по заключенным с ними договорам (контрактам)
320	Экономическая и инвестиционная информация	–
321	Информация о претендентах и участниках программ и проектов	Документы, представленные заинтересованными лицами или полученные с их согласия

Продолжение

1	2	3
323	Информация о кодах электронного взаимодействия участников программ и проектов	Идентификаторы пароля и др.
324	Информация о переговорах с потенциальными партнерами	В части целей, задач, стратегии и тактики ведения переговоров, деловая переписка, инструкции, распоряжения, предварительные договоры и соглашения, материалы обсуждений
325	Предварительная информация о предлагаемых участниками аукциона (конкурса, тендера) условиях исполнения выставленного на аукцион контракта	–
327	Информация о состоянии дел и соблюдении интересов организации в других организациях и предприятиях, в капиталах которых имеется доля организации	–
330	Научно-техническая информация	–
331	Тайна научного опыта	Результаты фундаментальных, поисковых и прикладных научных исследований, содержащие сведения, утрата, которых может нанести ущерб национальным интересам и престижу России
332	Незапатентованные секреты	Сведения об организации производства (ноу-хау), торговые секреты, оригинальные идеи НИОКР, готовящиеся проекты, результаты которых могут быть незаконно использованы
333	Незапатентованные изобретения, промышленные образцы и полезные модели	В том числе конструкционные характеристики создаваемых изделий и параметры разрабатываемых технологических процессов (размеры, объемы, конфигурация, процентное содержание компонентов, температура, давление, время и т.д.)

Продолжение

1	2	3
334	Экспериментальные данные	Данные об условиях экспериментов и оборудовании, на котором они проводились
335	Информация о материалах, из которых изготовлены детали изделий	–
336	Информация об особенностях конструкторско-технологического и художественно-технического решения изделия (дизайна), не защищенных законом	–
337	Информация о методах защиты от подделок и от незаконного тиражирования результатов работ	–
400	Информация, составляющая профессиональную тайну	Информация, ставшая известной компетентным органам (налоговая инспекция и т. д.)
401	Врачебная тайна	Информация, содержащая сведения об обращении за медицинской помощью, о состоянии здоровья, диагнозе заболевания, иные сведения, полученные при обследовании и лечении гражданина
402	Тайна связи	Информация, полученная оператором связи и его работниками, составляющая тайну переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений
403	Нотариальная тайна	Информация, доверенная нотариусу либо ставшая ему известной иным образом при совершении нотариальных действий, в том числе тайна завещания
404	Адвокатская тайна	Информация, связанная с оказанием адвокатом юридической помощи своему доверителю

Окончание

1	2	3
405	Тайна страхования	Информация, полученная страховщиком в результате его профессиональной деятельности, сведения о страхователе, застрахованном лице, в том числе о состоянии их здоровья и имущественном положении
406	Налоговая тайна	Любая информация о лице – налогоплательщике, полученная органами, указанными в ст. 102 НК РФ
407	Банковская тайна	Информация о банковских и межбанковских операциях и сделках в интересах клиентов, счетах и вкладах своих клиентов и корреспондентов, а также иные сведения о самих клиентах и корреспондентах, разглашение которых может нарушить их право неприкосновенности частной жизни
408	Инсайдерская тайна	Любая нераскрытая информация, относящаяся к ценным бумагам и операциям с ними, а также к эмитенту этих ценных бумаг и осуществляемой им деятельности, раскрытие которой может оказать существенное влияние на рыночную цену указанных ценных бумаг
409	Информация личного характера, ставшая известной работникам учреждения социального обслуживания при оказании социальных услуг	–
500	Информация, содержащая тайну следствия и судопроизводства	–
501	Информация, содержащая тайну следствия	Сведения предварительного следствия в порядке, установленном УПК РФ
502	Информация, содержащая тайну судопроизводства	Сведения, раскрывающие порядок принятия конкретного судебного решения в совещательной комнате
503	Информация о защищаемых лицах и мерах государственной защиты	–

Приложение 5

Основные термины и определения по организации защиты конфиденциальной информации

Основные понятия

Блокирование персональных данных — временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

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.

Государственное регулирование в сфере применения информационных технологий:

• регулирование отношений, связанных с поиском, получением, передачей, производством и распространением информации с применением информационных технологий (информатизации);

• развитие информационных систем различного назначения для обеспечения граждан (физических лиц), организаций, государственных органов и органов местного самоуправления информацией, а также обеспечение взаимодействия таких систем;

• создание условий для эффективного использования в Российской Федерации информационно-телекоммуникационных сетей, в том числе Интернета и иных подобных информационно-телекоммуникационных сетей.

Государственные информационные системы — федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов и законов субъектов Российской Федерации, на основании правовых актов государственных органов.

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

Документированная информация – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или, в установленных законодательством Российской Федерации случаях, ее материальный носитель.

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 – возможность получения информации и ее использования.

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

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

Защита информации – принятие правовых, организационных и технических мер, направленных на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения и от иных неправомерных действий в отношении такой информации; а также соблюдение конфиденциальности информации ограниченного доступа и реализация права на доступ к информации.

Защита информации от агентурной разведки – деятельность по предотвращению получения защищаемой информации агентурной разведкой.

Защита информации от непреднамеренного воздействия – деятельность по предотвращению воздействия на защищаемую информацию, ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений или иных, ненаправленных на изменение информации воздействий, связанных с функционированием технических средств, систем или с деятельностью людей, приводящих к искажению, уни-

чтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Защита информации от несанкционированного воздействия (защита информации от НСВ) – деятельность по предотвращению воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Защита информации от несанкционированного доступа (защита информации от НСД) – деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации. Заинтересованным субъектом, осуществляющим несанкционированный доступ к защищаемой информации, может выступать: государство, юридическое лицо, группа физических лиц, в том числе общественная организация, отдельное физическое лицо.

Защита информации от (иностранной) разведки – деятельность по предотвращению получения защищаемой информации (иностранной) разведкой.

Защита информации от (иностранной) технической разведки – деятельность по предотвращению получения защищаемой информации (иностранной) разведкой с помощью технических средств.

Защита информации от разглашения – деятельность по предотвращению несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

Защита информации от утечки – деятельность по предотвращению неконтролируемого распространения защищаемой информации, ее разглашения, несанкционированного допуска к защищаемой информации и получения защищаемой информации (иностранными) разведками.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми обладателем, собственником информации.

Информационная безопасность – состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

Информационные продукты (продукция) – документированная информация, подготовленная в соответствии с потребностями пользователей и предназначенная или применяемая для удовлетворения потребностей пользователя.

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

Информационная система – совокупность содержащейся в базах данных информации и информационных технологий и технических средств, обеспечивающих ее обработку.

Информационная система персональных данных – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Информационная сфера (среда) – сфера деятельности субъектов, связанная с созданием, преобразованием и потреблением информации.

Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информация – сведения (сообщения, данные) независимо от формы их представления.

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

Использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

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

Категорирование защищаемой информации (объекта защиты) – установление градаций важности защиты защищаемой информации (объекта защиты).

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

Контроль организации защиты информации – проверка соответствия состояния организации, наличия и содержания документов требованиям правовых, организационно-распорядительных и нормативных документов по защите информации.

Контроль состояния защиты информации – проверка соответствия организации и эффективности защиты информации установленным требованиям и (или) нормам в области защиты информации.

Контроль эффективности защиты информации – проверка соответствия эффективности мероприятий по защите информации установленным требованиям или нормам эффективности защиты информации.

Конфиденциальная информация – документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

Массовая информация – предназначенные для неограниченного круга лиц печатные, аудиосообщения, аудиовизуальные и иные сообщения и материалы.

Метод (способ) контроля эффективности защиты информации – порядок и правила применения определенных принципов и средств контроля эффективности защиты информации.

Мероприятие по защите информации – совокупность действий по разработке и (или) практическому применению способов и средств защиты информации.

Мероприятие по контролю эффективности защиты информации – совокупность действий по разработке и (или) практическому применению методов (способов) и средств контроля эффективности защиты информации.

Муниципальные информационные системы – системы, созданные на основании решения органа местного самоуправления.

Нормы эффективности защиты информации – значения показателей эффективности защиты информации, установленные нормативными документами

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.

Обезличивание персональных данных – действия, в результате которых становится невозможным определение принадлежности персональных данных конкретному субъекту персональных данных.

Обладатель информации – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

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

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Объект защиты – информация, или носитель информации, или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации.

Оператор информационной системы – гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

Оператор персональных данных – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Организационный контроль эффективности защиты информации – проверка полноты и обоснованности мероприятий по защите информации требованиям нормативных документов по защите информации.

Организация защиты информации – содержание и порядок действий по обеспечению защиты информации.

Перечень информации, подлежащей защите, – совокупность категорий информации, в соответствии с которыми информация относится к защищаемой и становится недоступной для других лиц и иных организаций на основаниях и в порядке, установленных собственником, владельцем (обладателем) информации, в соответствии с законодательством о государственной тайне, коммерческой тайне и других видах тайны.

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.

Персональные данные (личная и семейная тайны) – любая информация, относящаяся к конкретному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Показатель эффективности защиты информации – мера или характеристика для оценки эффективности защиты информации.

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

Пользователь (потребитель) информации, средств международного информационного обмена – субъект, обращающийся к собственнику или владельцу за получением необходимых ему информационных продуктов или возможности использования средств международного информационного обмена и пользующийся ими.

Предоставление информации – действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

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

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

Распространение информации – действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

Распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

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

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 – совокупность органов и (или) исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации.

Способ защиты информации – порядок и правила применения определенных принципов и средств защиты информации.

Средство защиты информации – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

Средства защиты информации, составляющей государственную тайну, – 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 контроля эффективности защиты информации – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для контроля эффективности защиты информации.

Средства международного информационного обмена – информационные системы, сети и сети связи, используемые при международном информационном обмене.

Средства обеспечения автоматизированных информационных систем и их технологий – программные, технические, лингвистические, правовые, организационные средства (программы для электронных вычислительных машин; средства вычислительной техники и связи; словари, тезаурусы и классификаторы; инструкции и методики; положения, уставы, должностные инструкции; схемы и их описания, другая эксплуатационная и сопроводительная документация), используемые или создаваемые при проектировании информационных систем и обеспечивающие их эксплуатацию.

Техника защиты информации – средства защиты информации; средства контроля эффективности защиты информации; средства и системы управления, предназначенные для обеспечения защиты информации.

Технический контроль эффективности защиты информации – контроль эффективности защиты информации, проводимый с использованием средств контроля.

Трансграничная передача персональных данных – передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановление содержания персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Цель защиты информации – желаемый результат защиты информации. Целью защиты информации может быть предотвращение ущерба обладателю, собственнику, владельцу, пользователю информации

в результате возможной утечки информации и (или) несанкционированного и непреднамеренного воздействия на информацию.

Электронное сообщение – информация, переданная или полученная пользователем информационно-телекоммуникационной сети.

Эффективность защиты информации – степень соответствия результатов защиты информации поставленной цели.

Термины и определения, необходимые для понимания текста основных терминов

Владелец информации — субъект, осуществляющий владение и пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и (или) собственником информации.

Доступ к информации — получение субъектом возможности ознакомления с информацией, в том числе с помощью технических средств.

Носитель информации — физическое лицо или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов.

Орган защиты информации — административный орган, осуществляющий организацию защиты информации.

Пользователь (потребитель) информации — субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением.

Правило доступа к информации — совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям.

Право доступа к информации — право доступа: совокупность правил доступа к информации, установленных правовыми документами или обладателем, собственником, владельцем информации.

Собственник информации — субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами.

Субъект доступа к информации — участник правоотношений в информационных процессах.

Примечание: Информационные процессы — процессы создания, обработки, хранения, защиты от внутренних и внешних угроз, передачи, получения, использования и уничтожения информации.

Приложение 6

Примерный перечень преступлений и административных правонарушений в информационной сфере

1. Выписка из Уголовного кодекса Российской Федерации

Уголовный кодекс Российской Федерации включает в себя следующие статьи, касающиеся преступлений в информационной сфере:

Статья 137*. Нарушение неприкосновенности частной жизни*

1. Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации, —

наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо обязательными работами на срок от ста двадцати до ста восьмидесяти часов, либо исправительными работами на срок до одного года, либо арестом на срок до четырех месяцев, либо лишением свободы на срок до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

2. Те же деяния, совершенные лицом с использованием своего служебного положения, —

наказываются штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет, либо арестом на срок от четырех до шести месяцев, либо лишением свободы на срок от одного года до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет.

Статья 138. *Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений*

1. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан —

наказывается штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев, либо обязательными работами на срок от ста двадцати до ста восьмидесяти часов, либо исправительными работами на срок от одного года до четырех лет.

2. То же деяние, совершенное лицом с использованием своего служебного положения или специальных технических средств, предназначенных для негласного получения информации, —

наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо арестом на срок от двух до четырех месяцев.

3. Незаконные производство, сбыт или приобретение в целях сбыта специальных технических средств, предназначенных для негласного получения информации, —

наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо ограничением свободы на срок до трех лет, либо лишением свободы на срок до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

Статья 155*. Разглашение тайны усыновления*

Разглашение тайны усыновления вопреки воле усыновителя, совершенное лицом, обязанным хранить факт усыновления как служебную или профессиональную тайну, либо иным лицом из корыстных или иных низменных побуждений, —

наказывается штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев, либо исправительными работами на срок до одного года, либо арестом на срок до четырех месяцев с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

Статья 180. *Незаконное использование товарного знака*

1. Незаконное использование чужого товарного знака, знака обслуживания, наименования места происхождения товара или сходных с ними обозначений для однородных товаров, если это деяние совершено неоднократно или причинило крупный ущерб, —

наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо исправительными работами на срок до двух лет.

2. Незаконное использование предупредительной маркировки в отношении не зарегистрированного в Российской Федерации товарного знака или наименования места происхождения товара, если это деяние совершено неоднократно или причинило крупный ущерб, —

наказывается штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок от ста двадцати до ста восьмидесяти часов, либо исправительными работами на срок до одного года.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой, —

наказываются лишением свободы на срок до шести лет со штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет либо без такового.

Статья 183*. Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну*

1. Собирание сведений, составляющих коммерческую, налоговую или банковскую тайну, путем похищения документов, подкупа или угроз, а равно иным незаконным способом, —

наказывается штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного до шести месяцев либо лишением свободы на срок до двух лет.

2. Незаконные разглашение или использование сведений, составляющих коммерческую, налоговую или банковскую тайну, без согласия их владельца лицом, которому она была доверена или стала известна по службе или работе, —

наказываются штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет либо лишением свободы на срок до трех лет.

3. Те же деяния, причинившие крупный ущерб или совершенные из корыстной заинтересованности, —

наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет либо лишением свободы на срок до пяти лет.

4. Деяния, предусмотренные частями второй или третьей настоящей статьи, повлекшие тяжкие последствия, —

наказываются лишением свободы на срок до десяти лет.

***Статья 187**. Изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов*

1. Изготовление в целях сбыта или сбыт поддельных кредитных либо расчетных карт, а также иных платежных документов, не являющихся ценными бумагами, —

наказываются лишением свободы на срок от двух до шести лет со штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет.

2. Те же деяния, совершенные организованной группой, —

наказываются лишением свободы на срок от четырех до семи лет со штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до пяти лет либо без такового.

***Статья 189.** Незаконный экспорт или передача сырья, материалов, оборудования, технологий, научно-технической информации, незаконное выполнение работ (оказание услуг), которые могут быть использованы при создании оружия массового поражения, вооружения и военной техники*

1. Незаконные экспорт или передача лицом, наделенным правом осуществлять внешнеэкономическую деятельность, иностранной организации или ее представителю сырья, материалов, оборудования, технологий, научно-технической информации, незаконное выполнение этим лицом работ для иностранной организации или ее представителя либо незаконное оказание услуг иностранной организации

или ее представителю, которые заведомо для указанного лица могут быть использованы при создании вооружения и военной техники и в отношении которых установлен экспортный контроль, —

наказываются штрафом в размере от ста тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо лишением свободы на срок до трех лет.

2. Те же деяния, совершенные группой лиц по предварительному сговору, —

наказываются лишением свободы на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

3. Деяния, предусмотренные частью первой настоящей статьи, совершенные организованной группой либо в отношении сырья, материалов, оборудования, технологий, научно-технической информации, работ (услуг), которые заведомо для лица, наделенного правом осуществлять внешнеэкономическую деятельность, могут быть использованы при создании оружия массового поражения, средств его доставки и в отношении которых установлен экспортный контроль, —

наказываются лишением свободы на срок от трех до семи лет со штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до пяти лет либо без такового.

Статья 237. *Сокрытие информации об обстоятельствах, создающих опасность для жизни или здоровья людей*

1. Сокрытие или искажение информации о событиях, фактах или явлениях, создающих опасность для жизни или здоровья людей либо для окружающей среды, совершенные лицом, обязанным обеспечивать население и органы, уполномоченные на принятие мер по устранению такой опасности, указанной информацией, —

наказываются штрафом в размере до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до двух лет либо лишением свободы на срок до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

2. Те же деяния, если они совершены лицом, занимающим государственную должность Российской Федерации или государственную должность субъекта Российской Федерации, а равно главой ор-

гана местного самоуправления либо если в результате таких деяний причинен вред здоровью человека или наступили иные тяжкие последствия, —

наказываются штрафом в размере от ста тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет либо лишением свободы на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

Статья 272. *Неправомерный доступ к компьютерной информации*

1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, —

наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, —

наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

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

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами —

наказываются лишением свободы на срок до трех лет со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

2. Те же деяния, повлекшие по неосторожности тяжкие последствия, —

наказываются лишением свободы на срок от трех до семи лет.

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

1. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, —

наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет.

2. То же деяние, повлекшее по неосторожности тяжкие последствия, —

наказывается лишением свободы на срок до четырех лет.

Статья 283. *Разглашение государственной тайны*

1. Разглашение сведений, составляющих государственную тайну, лицом, которому она была доверена или стала известна по службе или работе, если эти сведения стали достоянием других лиц, при отсутствии признаков государственной измены —

наказывается арестом на срок от четырех до шести месяцев либо лишением свободы на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

2. То же деяние, повлекшее по неосторожности тяжкие последствия, —

наказывается лишением свободы на срок от трех до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

Статья 284. *Утрата документов, содержащих государственную тайну*

Нарушение лицом, имеющим допуск к государственной тайне, установленных правил обращения с содержащими государственную тайну документами, а равно с предметами, сведения о которых со-

ставляют государственную тайну, если это повлекло по неосторожности их утрату и наступление тяжких последствий, —

наказывается ограничением свободы на срок до трех лет, либо арестом на срок от четырех до шести месяцев, либо лишением свободы на срок до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

Статья 287. *Отказ в предоставлении информации Федеральному Собранию Российской Федерации или Счетной палате Российской Федерации*

1. Неправомерный отказ в предоставлении или уклонение от предоставления информации (документов, материалов), а также предоставление заведомо неполной либо ложной информации Совету Федерации Федерального Собрания Российской Федерации, Государственной Думе Федерального Собрания Российской Федерации или Счетной палате Российской Федерации, если эти деяния совершены должностным лицом, обязанным предоставлять такую информацию, —

наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет, либо арестом на срок от четырех до шести месяцев, либо лишением свободы на срок до трех лет.

2. Те же деяния, совершенные лицом, занимающим государственную должность Российской Федерации или государственную должность субъекта Российской Федерации, —

наказываются штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет либо лишением свободы на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, если они:

а) сопряжены с сокрытием правонарушений, совершенных должностными лицами органов государственной власти;

б) совершены группой лиц по предварительному сговору или организованной группой;

в) повлекли тяжкие последствия, —

наказываются лишением свободы на срок от четырех до восьми лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

Статья 292. *Служебный подлог*

1. Служебный подлог, то есть внесение должностным лицом, а также государственным служащим или служащим органа местного самоуправления, не являющимся должностным лицом, в официальные документы заведомо ложных сведений, а равно внесение в указанные документы исправлений, искажающих их действительное содержание, если эти деяния совершены из корыстной или иной личной заинтересованности (при отсутствии признаков преступления, предусмотренного частью 1 статьи 292.1 настоящего Кодекса), —

наказываются штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до двух лет.

2. Те же деяния, повлекшие существенное нарушение прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства, —

наказываются штрафом в размере от ста тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет либо лишением свободы на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

Статья 310*. Разглашение данных предварительного расследования*

Разглашение данных предварительного расследования лицом, предупрежденным в установленном законом порядке о недопустимости их разглашения, если оно совершено без согласия следователя или лица, производящего дознание, —

наказывается штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев, либо исправительными работами на срок до двух лет, либо арестом на срок до трех месяцев.

Статья 311. *Разглашение сведений о мерах безопасности, применяемых в отношении судьи и участников уголовного процесса*

1. Разглашение сведений о мерах безопасности, применяемых в отношении судьи, присяжного заседателя или иного лица, участвующего в отправлении правосудия, судебного пристава, судеб-

ного исполнителя, потерпевшего, свидетеля, других участников уголовного процесса, а равно в отношении их близких, если это деяние совершено лицом, которому эти сведения были доверены или стали известны в связи с его служебной деятельностью, —

наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо ограничением свободы на срок до двух лет, либо арестом на срок до четырех месяцев.

2. То же деяние, повлекшее тяжкие последствия, —

наказывается лишением свободы на срок до пяти лет.

Статья 320. *Разглашение сведений о мерах безопасности, применяемых в отношении должностного лица правоохранительного или контролирующего органа*

1. Разглашение сведений о мерах безопасности, применяемых в отношении должностного лица правоохранительного или контролирующего органа, а также его близких, если это деяние совершено в целях воспрепятствования его служебной деятельности, —

наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев либо арестом на срок до четырех месяцев.

2. То же деяние, повлекшее тяжкие последствия, —

наказывается лишением свободы на срок до пяти лет.

Статья 327. *Подделка, изготовление или сбыт поддельных документов, государственных наград, штампов, печатей, бланков*

1. Подделка удостоверения или иного официального документа, предоставляющего права или освобождающего от обязанностей, в целях его использования либо сбыт такого документа, а равно изготовление в тех же целях или сбыт поддельных государственных наград Российской Федерации, РСФСР, СССР, штампов, печатей, бланков, —

наказываются ограничением свободы на срок до трех лет, либо арестом на срок от четырех до шести месяцев, либо лишением свободы на срок до двух лет.

2. Те же деяния, совершенные с целью скрыть другое преступление или облегчить его совершение, —

наказываются лишением свободы на срок до четырех лет.

3. Использование заведомо подложного документа, —

наказывается штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо исправительными работами на срок до двух лет, либо арестом на срок от трех до шести месяцев.

2. Выписка из Кодекса Российской Федерации об административных правонарушениях

Кодекс Российской Федерации об административных правонарушениях включает в себя следующие статьи, касающиеся правонарушений в информационной сфере, организации пропускного и внутриобъектового режима предприятий и организаций.

Статья 5.53. *Незаконные действия по получению и (или) распространению информации, составляющей кредитную историю*

Незаконные действия по получению и (или) распространению информации, составляющей кредитную историю, если такие действия не содержат уголовно наказуемого деяния, —

влекут наложение административного штрафа на граждан в размере от одной тысячи до двух тысяч пятисот рублей; на должностных лиц – от двух тысяч пятисот до пяти тысяч рублей или дисквалификацию на срок до трех лет; на юридических лиц – от тридцати тысяч до пятидесяти тысяч рублей.

Статья 5.56. *Нарушение порядка и сроков представления и хранения документов, связанных с подготовкой и проведением выборов, референдума*

1. Непредставление председателем, заместителем председателя или секретарем избирательной комиссии, комиссии референдума в вышестоящую избирательную комиссию, комиссию референдума документов, связанных с подготовкой и проведением выборов, референдума, или их представление с нарушением установленных законом сроков —

влечет наложение административного штрафа в размере от двух тысяч до пяти тысяч рублей.

2. Уничтожение документов, связанных с подготовкой и проведением выборов, референдума, до истечения сроков их хранения, а также нарушение установленного порядка уничтожения таких документов —

влечет наложение административного штрафа на граждан в размере от одной тысячи пятисот до двух тысяч рублей; на должностных лиц – от двух тысяч до пяти тысяч рублей.

Статья 7.31. *Предоставление, опубликование или размещение недостоверной информации о размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных или муниципальных нужд, а также направление недостоверных сведений, внесение их в реестр государственных или муниципальных контрактов, заключенных по итогам размещения заказов, реестр недобросовестных поставщиков*

1. Предоставление, опубликование в официальном печатном издании или размещение на официальном сайте в сети Интернет должностным лицом государственного или муниципального заказчика, уполномоченного органа, специализированной организацией, должностным лицом органа, уполномоченного на ведение официального сайта в сети Интернет, оказывающей услуги по обслуживанию официального сайта в сети Интернет и обеспечению функционирования такого сайта организацией недостоверной информации о размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных или муниципальных нужд, а также направление должностным лицом государственного или муниципального заказчика недостоверных сведений в федеральный орган исполнительной власти, орган исполнительной власти субъекта Российской Федерации, орган местного самоуправления, уполномоченные на ведение реестров государственных или муниципальных контрактов, заключенных по итогам размещения заказов, и (или) в федеральный орган исполнительной власти, уполномоченный на осуществление контроля в сфере размещения заказов на поставки товаров, выполнение работ, оказание услуг для государственных или муниципальных нужд, либо внесение должностным лицом федерального органа исполнительной власти, органа исполнительной власти субъекта Российской Федерации или органа местного самоуправления, уполномоченных на ведение реестров государственных или муниципальных контрактов, заключенных по итогам размещения заказов, заведомо недостоверных сведений в указанные реестры государственных или муниципальных контрактов либо реестр недобросовестных поставщиков —

влечет наложение административного штрафа на должностных лиц в размере пятидесяти тысяч рублей; на юридических лиц – в размере трехсот тысяч рублей.

2. Внесение должностным лицом федерального органа исполнительной власти, уполномоченного на осуществление контроля в сфере размещения заказов на поставки товаров, выполнение работ, оказание услуг для государственных или муниципальных нужд, заведомо недостоверных сведений в реестр государственных или муниципальных контрактов, заключенных по итогам размещения заказов, или реестр недобросовестных поставщиков —

влечет наложение административного штрафа в размере пятидесяти тысяч рублей.

3. Нарушение должностным лицом федерального органа исполнительной власти, органа исполнительной власти субъекта Российской Федерации, органа местного самоуправления, уполномоченных на

ведение реестров государственных или муниципальных контрактов, заключенных по итогам размещения заказов, порядка ведения реестров государственных или муниципальных контрактов —

влечет наложение административного штрафа в размере десяти тысяч рублей.

Статья 7.31.1. *Нарушение сроков возврата денежных средств, порядка и (или) сроков блокирования операций по счету участника размещения заказа, порядка ведения реестра участников размещения заказа, правил документооборота при проведении открытого аукциона в электронной форме, разглашение оператором электронной площадки, должностным лицом оператора электронной площадки сведений об участнике размещения заказа до подведения результатов открытого аукциона в электронной форме*

1. Нарушение должностным лицом государственного или муниципального заказчика, должностным лицом уполномоченного органа, оператором электронной площадки срока возврата денежных средств, внесенных в качестве обеспечения заявки на участие в конкурсе, аукционе, открытом аукционе в электронной форме, установленного законодательством Российской Федерации о размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд, не более чем на три рабочих дня, —

влечет наложение административного штрафа на должностных лиц в размере пяти тысяч рублей; на юридических лиц – тридцати тысяч рублей.

2. Нарушение должностным лицом государственного или муниципального заказчика, должностным лицом уполномоченного органа, оператором электронной площадки срока возврата денежных средств, внесенных в качестве обеспечения заявки на участие в конкурсе, аукционе, открытом аукционе в электронной форме, установленного законодательством Российской Федерации о размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд, более чем на три рабочих дня, —

влечет наложение административного штрафа на должностных лиц в размере пятнадцати тысяч рублей; на юридических лиц – девяноста тысяч рублей.

3. Нарушение оператором электронной площадки порядка и (или) сроков блокирования, прекращения блокирования операций по счету участника размещения заказа для проведения операций по обеспечению участия в открытых аукционах в электронной форме —

влечет наложение административного штрафа в размере пятнадцати тысяч рублей.

4. Нарушение оператором электронной площадки порядка ведения реестра участников размещения заказа, получивших аккредитацию на электронной площадке, —

влечет наложение административного штрафа в размере пятнадцати тысяч рублей.

5. Нарушение оператором электронной площадки правил документооборота при проведении открытого аукциона в электронной форме, а также порядка и (или) сроков размещения, направления информации и (или) уведомлений, проектов государственных или муниципальных контрактов, установленных законодательством Российской Федерации о размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд, –

влечет наложение административного штрафа в размере тридцати тысяч рублей.

6. Разглашение оператором электронной площадки, должностным лицом оператора электронной площадки сведений об участнике размещения заказа до подведения результатов открытого аукциона в электронной форме, —

влечет наложение административного штрафа на должностных лиц в размере пятидесяти тысяч рублей; на юридических лиц — двухсот пятидесяти тысяч рублей.

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 трехсот до пятисот рублей; на должностных лиц — от пятисот до одной тысячи рублей; на юридических лиц – от пяти тысяч до десяти тысяч рублей.

Статья 13.12. *Нарушение правил защиты информации*

1. 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 трехсот до пятисот рублей; на должностных лиц – от пятисот до одной тысячи рублей; на юридических лиц — от пяти тысяч до десяти тысяч рублей.

2. 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 пятисот до одной тысячи рублей с конфискацией несертифицированных средств защиты информации или без таковой; на должностных лиц – от одной тысячи до двух тысяч рублей; на юридических лиц — от десяти тысяч до двадцати тысяч рублей с конфискацией несертифицированных средств защиты информации или без таковой.

3. 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 двух тысяч до трех тысяч рублей; на юридических лиц – от пятнадцати тысяч до двадцати тысяч рублей.

4. Использование несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну, —

влечет наложение административного штрафа на должностных лиц в размере от трех тысяч до четырех тысяч рублей; на юридических лиц — от двадцати тысяч до тридцати тысяч рублей с конфискацией несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну, или без таковой.

5. Грубое нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну), —

влечет наложение административного штрафа на лиц, осуществляющих предпринимательскую деятельность без образования юридического лица, в размере от одной тысячи до одной тысячи пятисот рублей или административное приостановление деятельности на срок до девяноста суток; на должностных лиц — от одной тысячи до одной тысячи пятисот рублей; на юридических лиц — от десяти тысяч до пятнадцати тысяч рублей или административное приостановление деятельности на срок до девяноста суток.

Статья 13.13. *Незаконная деятельность в области защиты информации*

1. 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 пятисот до одной тысячи рублей с конфискацией средств защиты информации или без таковой; на должностных лиц – от двух тысяч до трех тысяч рублей с конфискацией средств защиты информации или без таковой; на юридических лиц – от десяти тысяч до двадцати тысяч рублей с конфискацией средств защиты информации или без таковой.

2. 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 четырех тысяч до пяти тысяч рублей; на юридических лиц – от тридцати тысяч до сорока тысяч рублей 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, за исключением случаев, предусмотренных частью 1 статьи 14.33 настоящего Кодекса, —

влечет наложение административного штрафа на граждан в размере от пятисот до одной тысячи рублей; на должностных лиц — от четырех тысяч до пяти тысяч рублей.

Статья 13.15. *Злоупотребление свободой массовой информации*

Изготовление и (или) распространение теле-, видео-, кинопрограмм, документальных и художественных фильмов, а также относящихся к специальным средствам массовой информации информационных компьютерных файлов и программ обработки ин-

формационных текстов, содержащих скрытые вставки, воздействующие на подсознание людей и (или) оказывающие вредное влияние на их здоровье, а равно распространение информации об общественном объединении или иной организации, включенных в опубликованный перечень общественных и религиозных объединений, иных организаций, в отношении которых судом принято вступившее в законную силу решение о ликвидации или запрете деятельности по основаниям, предусмотренным Федеральным законом от 25 июля 2002 года № 114-ФЗ «О противодействии экстремистской деятельности», без указания на то, что соответствующее общественное объединение или иная организация ликвидированы или их деятельность запрещена, —

влечет наложение административного штрафа на граждан в размере от двух тысяч до двух тысяч пятисот рублей с конфискацией предмета административного правонарушения; на должностных лиц – от четырех тысяч до пяти тысяч рублей с конфискацией предмета административного правонарушения; на юридических лиц – от сорока тысяч до пятидесяти тысяч рублей с конфискацией предмета административного правонарушения.

Статья 13.17. *Нарушение правил распространения обязательных сообщений*

Нарушение правил распространения обязательных сообщений, —

влечет наложение административного штрафа на граждан в размере от ста до трехсот рублей; на должностных лиц — от трехсот до пятисот рублей; на юридических лиц — от трех тысяч до пяти тысяч рублей.

Статья 13.19. *Нарушение порядка представления статистической информации*

Нарушение должностным лицом, ответственным за представление статистической информации, необходимой для проведения государственных статистических наблюдений, порядка ее представления, а равно представление недостоверной статистической информации, —

влечет наложение административного штрафа в размере от трех тысяч до пяти тысяч рублей.

Статья 13.20. *Нарушение правил хранения, комплектования, учета или использования архивных документов*

Нарушение правил хранения, комплектования, учета или использования архивных документов, за исключением случаев, предусмотренных статьей 13.25 настоящего Кодекса, —

влечет предупреждение или наложение административного штрафа на граждан в размере от ста до трехсот рублей; на должностных лиц — от трехсот до пятисот рублей.

Статья 13.22. Нарушение порядка объявления выходных данных

Выпуск (изготовление) или распространение продукции средства массовой информации без указания в установленном порядке выходных данных, а равно с неполными или заведомо ложными выходными данными, —

влечет предупреждение или наложение административного штрафа на граждан в размере от трехсот до пятисот рублей с конфискацией продукции средства массовой информации или без таковой; на должностных лиц – от пятисот до одной тысячи рублей с конфискацией продукции средства массовой информации или без таковой; на юридических лиц – от пяти тысяч до десяти тысяч рублей с конфискацией продукции средства массовой информации или без таковой.

Статья 13.23. *Нарушение порядка представления обязательного экземпляра документов, письменных уведомлений, уставов и договоров*

Нарушение установленного законом порядка представления обязательного экземпляра документов, письменных уведомлений, уставов редакций или заменяющих их договоров, а равно порядка хранения материалов теле- и радиопередач, —

влечет наложение административного штрафа на граждан в размере от двухсот до пятисот рублей; на должностных лиц – от одной тысячи до двух тысяч рублей; на юридических лиц – от десяти тысяч до двадцати тысяч рублей.

Статья 13.25. *Нарушение требований законодательства о хранении документов*

1. Неисполнение акционерным обществом, профессиональным участником рынка ценных бумаг, управляющей компанией акционерного инвестиционного фонда, паевого инвестиционного фонда или негосударственного пенсионного фонда либо специализированным депозитарием акционерного инвестиционного фонда, паевого инвестиционного фонда или негосударственного пенсионного фонда обязанности по хранению документов, которые предусмотрены законодательством об акционерных обществах, о рынке ценных бумаг, об инвестиционных фондах и принятыми в соответствии с ним нормативными правовыми актами и хранение которых является обязательным, а также нарушение установленных порядка и сроков хранения таких документов, —

влечет наложение административного штрафа на должностных лиц в размере от двух тысяч пятисот до пяти тысяч рублей; на юридических лиц – от двухсот тысяч до трехсот тысяч рублей.

2. Неисполнение обществом с ограниченной (дополнительной) ответственностью или унитарным предприятием обязанности по хранению документов, которые предусмотрены законодательством об обществах с ограниченной ответственностью, о государственных и муниципальных унитарных предприятиях и принятыми в соответствии с ним нормативными правовыми актами и хранение которых является обязательным, а также нарушение установленных порядка и сроков хранения таких документов, —

влечет наложение административного штрафа на должностных лиц в размере от двух тысяч пятисот до пяти тысяч рублей; на юридических лиц – от двухсот тысяч до трехсот тысяч рублей.

Статья 13.26. *Нарушение сроков и (или) порядка доставки (вручения) адресату судебных извещений*

Нарушение оператором почтовой связи правил оказания услуг почтовой связи в отношении сроков и (или) порядка доставки (вручения) адресату судебных извещений, в том числе несвоевременное сообщение суду о доставке (вручении) судебного извещения или невозможности его доставки (вручения) адресату, —

влечет наложение административного штрафа на должностных лиц в размере от пятисот до одной тысячи рублей; на юридических лиц – от пяти тысяч до десяти тысяч рублей.

Статья 14.10*. Незаконное использование товарного знака*

Незаконное использование чужого товарного знака, знака обслуживания, наименования места происхождения товара или сходных с ними обозначений для однородных товаров, —

влечет наложение административного штрафа на граждан в размере от одной тысячи пятисот до двух тысяч рублей с конфискацией предметов, содержащих незаконное воспроизведение товарного знака, знака обслуживания, наименования места происхождения товара; на должностных лиц – от десяти тысяч до двадцати тысяч рублей с конфискацией предметов, содержащих незаконное воспроизведение товарного знака, знака обслуживания, наименования места происхождения товара; на юридических лиц – от тридцати тысяч до сорока тысяч рублей с конфискацией предметов, содержащих незаконное воспроизведение товарного знака, знака обслуживания, наименования места происхождения товара.

Статья 17.10. *Нарушение порядка официального использования государственных символов Российской Федерации*

Нарушение порядка официального использования Государственного флага Российской Федерации, Государственного герба Российской Федерации или Государственного гимна Российской Федерации, —

влечет наложение административного штрафа на граждан в размере от трехсот до пятисот рублей; на должностных лиц – от пятисот до одной тысячи рублей.

Статья 17.13. *Разглашение сведений о мерах безопасности*

Разглашение сведений о мерах безопасности, примененных в отношении должностного лица правоохранительного или контролирующего органа либо в отношении его близких, —

влечет наложение административного штрафа на граждан в размере от трехсот до пятисот рублей; на должностных лиц – от пятисот до одной тысячи рублей.

Статья 19.2. *Умышленное повреждение или срыв печати (пломбы)*

Умышленное повреждение или срыв печати (пломбы), наложенной правомочным должностным лицом, за исключением случаев, предусмотренных частью 2 статьи 11.15 и статьей 16.11 настоящего Кодекса, —

влечет предупреждение или наложение административного штрафа на граждан в размере от ста до трехсот рублей; на должностных лиц – от трехсот до пятисот рублей.

Статья 19.7. *Непредставление сведений (информации)*

Непредставление или несвоевременное представление в государственный орган (должностному лицу) сведений (информации), представление которых предусмотрено законом и необходимо для осуществления этим органом (должностным лицом) его законной деятельности, а равно представление в государственный орган (должностному лицу) таких сведений (информации) в неполном объеме или в искаженном виде, за исключением случаев, предусмотренных статьями 19.7.1, 19.7.2, 19.7.3, 19.7.4, 19.8, 19.19 настоящего Кодекса, —

влечет наложение административного штрафа на граждан в размере от ста до трехсот рублей; на должностных лиц – от трехсот до пятисот рублей; на юридических лиц – от трех тысяч до пяти тысяч рублей.

Статья 19.10. *Нарушение законодательства о наименованиях географических объектов*

Нарушение установленных правил присвоения или употребления наименований географических объектов, —

влечет наложение административного штрафа на должностных лиц в размере от двух тысяч до трех тысяч рублей.

Статья 19.11. *Нарушение порядка изготовления, использования, хранения или уничтожения бланков, печатей либо иных носителей воспроизведения Государственного герба Российской Федерации*

Нарушение порядка изготовления, использования, хранения или уничтожения бланков, печатей либо иных носителей изображения Государственного герба Российской Федерации, —

влечет наложение административного штрафа в размере от пятисот до одной тысячи рублей.

Статья 19.23. *Подделка документов, штампов, печатей или бланков, их использование, передача либо сбыт*

Подделка документа, удостоверяющего личность, подтверждающего наличие у лица права или освобождение его от обязанности, а равно подделка штампа, печати, бланка, их использование, передача либо сбыт, —

влечет наложение административного штрафа на юридических лиц в размере от тридцати тысяч до сорока тысяч рублей с конфискацией орудий совершения административного правонарушения.

Статья 20.17. *Нарушение пропускного режима охраняемого объекта*

Самовольное проникновение на охраняемый в установленном порядке объект, —

влечет наложение административного штрафа в размере от трехсот до пятисот рублей.

Статья 20.19. *Нарушение особого режима в закрытом административно-территориальном образовании (ЗАТО)*

Нарушение установленного законом особого режима в закрытом административно-территориальном образовании (ЗАТО) —

влечет наложение административного штрафа в размере от ста до одной тысячи рублей.

Статья 20.23. *Нарушение правил производства, хранения, продажи и приобретения специальных технических средств, предназначенных для негласного получения информации*

1. Нарушение правил производства, хранения, продажи и приобретения специальных технических средств, предназначенных для негласного получения информации, при наличии специального разрешения (лицензии), —

влечет наложение административного штрафа на должностных лиц в размере от четырех тысяч до пяти тысяч рублей.

2. Нарушение правил разработки, ввоза в Российскую Федерацию и вывоза из Российской Федерации, а также порядка сертификации, регистрации и учета специальных технических средств, предназначенных для негласного получения информации, —

влечет наложение административного штрафа на граждан в размере от двух тысяч до двух тысяч пятисот рублей с конфискацией специальных технических средств, предназначенных для негласного получения информации; на должностных лиц – от трех тысяч до пяти тысяч рублей с конфискацией специальных технических средств, предназначенных для негласного получения информации.

Статья 20.24. *Незаконное использование специальных технических средств, предназначенных для негласного получения информации, в частной детективной или охранной деятельности*

Использование в частной детективной или охранной деятельности специальных технических средств, предназначенных для негласного получения информации и не предусмотренных установленными перечнями, —

влечет наложение административного штрафа на частных детективов (охранников) в размере от одной тысячи до двух тысяч пятисот рублей с конфискацией незаконно используемых специальных технических средств; на руководителей частных охранных организаций (объединений, ассоциаций) – от одной тысячи до пяти тысяч рублей.

Приложение 7

Типовой порядок работы с электронными документами, подписанными электронной цифровой подписью

1. Общие положения

1.1. Настоящий документ устанавливает Порядок использования электронных документов, подписанных электронной цифровой подписью (ЭЦП), в работе государственных и негосударственных структур – учреждений, предприятий, организаций (далее — организация).

1.2. Действие настоящего Порядка распространяется на деятельность организации, а также на деятельность уполномоченных удостоверяющих центров (УУЦ) при применении внутреннего электронного документооборота (ВЭД) и между другими организациями – межведомственного (межсетевого) электронного документооборота (МЭД), с использованием электронных сообщений.

1.3. При рассмотрении и согласовании электронных документов в системе электронного документооборота могут использоваться способы подтверждения действий с электронными документами, при которых ЭЦП не используется.

1.4. Правовое регулирование отношений в области использования ЭЦП в системах ВЭД и МЭД осуществляется в соответствии с Гражданским кодексом Российской Федерации, часть 4, федеральными законами от 10.01.2002 № 1-ФЗ «Об электронной цифровой подписи», от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»; Постановлением Правительства Российской Федерации от 22.09.2009 № 754 «Об утверждении положения о системе межведомственного электронного документооборота»; Постановлением Правительства Российской Федерации от 15.06.2009 № 477 «Об утверждении Правил делопроизводства в федеральных органах исполнительной власти»; техническими требования к организации взаимодействия системы межведомственного электронного документооборота с системами электронного документооборота федеральных органов исполнительной власти, утвержденными Распоряжением Правительства

Российской Федерации от 02.10.2009 № 1403-р; Приказом Мининформсвязи Российской Федерации от 09.01.2008 № 1 «Об утверждении требований по защите сетей связи от несанкционированного доступа к ним и передаваемой посредством их информации» с иными нормативными правовыми документами и технической документации.

1.5. При определении условий и возможности замещения бумажных документов аналогичными по содержанию электронными документами следует исходить из следующего:

1.5.1. Существующий или ранее существовавший бумажный документ может быть временно замещен или вместо бумажного документа может быть использован электронный документ, если выполнены условия признания соответствующего электронного документа электронным дубликатом бумажного или электронной копией бумажного документа. Электронный дубликат или электронная копия не могут использоваться за пределами срока действия соответствующего бумажного документа, а также в том случае, если соответствующий бумажный документ отменен, признан утратившим силу, отозван или уничтожен.

1.5.2. Вместо составления бумажного документа и удостоверения его собственноручной подписью создавшего его лица может быть создан электронный документ (далее – ЭД) с использованием электронной цифровой подписи (далее – ЭЦП) соответствующего лица, если выполняются условия признания электронного документа электронным оригиналом документа.

1.6. При определении условий и возможности замещения ЭД по содержанию бумажными документами следует исходить из следующего. Бумажный документ, полученный в результате обработки соответствующего электронного документа (распечатки), может признаваться равнозначным соответствующему ЭД при выполнении условий признания бумажного документа бумажной копией или бумажным дубликатом соответствующего электронного документа.

1.7. Бумажная копия или бумажный дубликат ЭД не могут быть использованы, если соответствующий электронный документ не существует или если владельцем соответствующей автоматизированной информационной системы (далее – АИС) принято правомерное решение о его удалении (уничтожении).

1.8. Обмен электронными сообщениями, каждое из которых подписано ЭЦП или иным аналогом собственноручной подписи отправителя такого сообщения, в порядке, установленном федеральными законами, иными нормативными правовыми актами или соглашением сторон, рассматривается как обмен документами.

1.9. Электронные документы должны быть подготовлены, переданы и обработаны в соответствии с настоящими Порядком, который обязателен для исполнения должностными и иными лицами Сторон, участвующими в процессе обмена электронными документами.

1.10. Участники обмена электронными документами

1.10.1. Участниками обмена электронными документами являются уполномоченные должностные и иные лица Сторон, осуществляющие: формирование и подготовку ЭД, заверение электронных документов ЭЦП, отправку/получение ЭД, проверку подлинности ЭЦП, хранение и обработку электронных документов, их учет и регистрацию.

1.10.2. Состав должностных лиц Сторон, наделенных правом электронной цифровой подписи, утверждается приказом руководства организации.

1.10.3. Для указанных должностных лиц Сторон обеспечивается процедура формирования ключей ЭЦП, изготовления и регистрации сертификатов ключей подписи в соответствии с требованиями по защите информации и криптографической защиты.

2. Организационные и технические требования при использовании электронных документов

2.1.Электронные документы создаются, хранятся и используется с использованием средств вычислительной техники.

2.2. Информация, содержащаяся в электронных документах и предназначенная для обработки с использованием средств вычислительной техники, должна быть представлена в форме, пригодной для восприятия человеком.

2.3. Электронные документы содержат реквизиты, позволяющие их идентифицировать. Обязательные реквизиты электронного документа определяются действующим законодательством, нормативными правовыми актами и владельцем АИС, в которой данный документ создается, используется и хранится, а также в регламенте информационного взаимодействия сторон, участвующих в электронном документообороте с использованием данного документа.

В регламенте информационного взаимодействия определяются: тип документа, структура передаваемой информации, формат передачи данных, периодичность представления информации и способ передачи.

2.4. Требования к внутренней структуре и содержательной части электронных документов устанавливаются с точки зрения делопроизводства и предметной сферы, где данный электронный документ создается и используется.

2.5. При составлении, хранении, изменении и передаче электронных документов в качестве способа, позволяющего достоверно идентифицировать его составителя, отправителя электронного документа, автора изменений, внесенных в электронный документ, и получателя электронного документа, используется ЭЦП в соответствии с действующим законодательством.

2.6. Категории электронных документов по источнику их возникновения:

2.6.1. Документы, созданные на основании получаемых от физических и юридических лиц документов, представленных в окончательно оформленном и действительном виде (заявления, удостоверения личности, доверенности, документы о государственной регистрации актов гражданского состояния, учредительные документы, свидетельства о регистрации, лицензии, сертификаты и иные личные документы).

2.6.2. Официальные документы органов государственной власти — документы, содержащиеся в официальных информационных ресурсах (нормативные документы, распорядительные документы, иные ранее созданные официальные информационные ресурсы правового или административного характера).

2.6.3. Документы, создаваемые в результате деятельности органов государственной власти и государственных учреждений (поручения, заключения, справки, согласования, протоколы, решения, копии, уведомления и иные документы).

2.6.4. Документы, создаваемые в результате деятельности организации (распорядительные документы, иные ранее созданные информационные ресурсы правового или административного характера).

2.7. Категории электронных документов по их отношению к оригиналу:

2.7.1. Электронный оригинал — документ, изначально созданный в электронном виде, подписанный ЭЦП, для которого не существует бумажного исходного оригинала, подписанного тем же лицом.

Электронные оригиналы создаются и используются в случаях, когда решение об этом принято владельцем АИС или участвующими в электронном документообороте сторонами, а также если это предписано нормативными правовыми актами.

2.7.2. Электронный дубликат бумажного документа — документ, произведенный в электронной форме вместе с идентичным бумажным документом, имеющим те же реквизиты, структуру и содержание, и подписанный ЭЦП того же лица, которое подписало оригинал бумажного документа.

Электронные дубликаты бумажных документов создаются в случаях, когда одним пользователям документа требуются и бумажный, и электронный экземпляры.

2.7.3. Электронная копия бумажного документа — электронный документ, полностью воспроизводящий информацию подлинного бумажного документа и его графическое изображение, заверенный в установленном порядке ЭЦП лица, которое является автором (составителем) бумажного документа либо обладает полномочиями на заверение данного документа ЭЦП. Полномочия на заверение электронных копий бумажных документов в АИС предоставляются в порядке, определяемом владельцем этой системы, а при использовании в системах МЭД — соглашением сторон, участвующих в данном электронном взаимодействии.

Электронные копии бумажных документов создаются в случаях, когда работа с заверенными электронными копиями бумажных документов не противоречит действующему законодательству и обеспечивает удобную обработку и использование информации, содержащейся в бумажном документе.

2.8. Способы создания электронных документов:

2.8.1. Сканирование бумажного документа — создание электронного образа бумажного документа с помощью специальных средств, обеспечивающих преобразование изображения на бумажном или ином материальном носителе в цифровую форму.

2.8.1.1. Сканирование бумажного документа без распознавания. Результатом сканирования бумажного документа без распознавания является файл, содержащий растровое графическое изображение.

Растровое графическое изображение пригодно для просмотра образа документа с экрана, для распечатки графического образа документа с сохранением расположения графических элементов, а также для возможного копирования графических элементов в целях создания иных документов.

Растровое графическое изображение без этапа распознавания непригодно для какой-либо автоматизированной обработки содержательной части электронного документа.

2.8.1.2. Сканирование бумажного документа с распознаванием. Результатом распознавания растрового графического изображения является файл, содержащий текст с повторением разметки страниц и формата шрифта, а также с возможными представлениями графических объектов, не поддавшихся текстовому распознаванию (такими графическими объектами могут являться: печать, штамп, герб, рисунок, диаграмма или рукописный текст).

При автоматизированном распознавании возможны потеря данных, искажение формата шрифта, смещение расположения графических элементов, частичная потеря графических элементов (таких, как рукописные надписи, слабоконтрастные фрагменты).

Распознанный текстовый электронный документ пригоден для частичной автоматизированной обработки текста.

Распознанный текстовый электронный документ предоставляет возможность осуществлять копирование и редактирование фрагментов текста.

Результатом сканирования формализованного бумажного документа с распознаванием полей формы документа является структурированный файл, содержащий все сведения в виде пар «название поля – значение поля».

2.8.2. Ручной ввод текстовых данных — создание электронного документа с помощью текстового редактора или специализированной АИС при непосредственном участии оператора.

Результат ручного ввода данных — электронный текстовый документ.

2.8.2.1. Неформализованный ручной ввод данных — ручной ввод данных без применения шаблона электронного сообщения, без использования классификаторов, словарей, справочников, реестров и иных высокоструктурированных общих информационных ресурсов.

Результат неформализованного ручного ввода данных — текстовый документ без строгой внутренней структуры.

Электронный документ без строгой внутренней структуры пригоден для использования человеком для автоматизированного поиска ключевых слов по тексту документа.

2.8.2.2. Формализованный ручной ввод данных — ручной ввод данных с применением шаблона, с использованием общих классификаторов, словарей, справочников, реестров и иных высокоструктурированных общих информационных ресурсов.

Результат формализованного ввода данных — электронный документ со строгой внутренней структурой данных.

Электронный документ со строгой внутренней структурой данных пригоден для интеграции и полностью автоматизированного анализа данных.

2.8.3. Автоматическая генерация электронного документа — создание электронного документа с помощью специализированных АИС на базе существующих информационных ресурсов без участия оператора или с минимальным управляющим участием оператора. Результат автоматической генерации электронного документа подразделяется по уровню структурирования информации.

2.8.3.1. Автоматическая генерация электронного документа, предназначенного для использования только человеком.

Результатом является электронный документ, предназначенный для просмотра или распечатки.

2.8.3.2. Автоматическая генерация электронного документа, предназначенного для использования иной АИС. Результатом является электронный документ с сохранением уровня внутренней структурированности информации.

2.8.4. Формирование файлов в специализированном программном обеспечении.

Результатом работы является файл, пригодный для работы в специализированном программном обеспечении, что позволяет получателю использовать дополнительные возможности специализированного программного обеспечения по анализу и использованию данных (отображать файл как карту, чертеж, электронную таблицу или презентацию).

2.9. Рекомендуемые форматы файлов электронного документа.

Выбор формата файла электронных сообщений зависит от условий создания и использования информации и определяется участниками МЭД и ВЭД.

2.9.1. Визуальное воспроизводство графического образа.

2.9.1.1. Электронная копия бумажного документа, предназначенная для подробного воспроизведения графического образа, создается с использованием растровых графических форматов (BMP, JPEG, TIFF, GIF или PNG) или гибридных текстово-растровых форматов (PDF, DjVu).

2.9.1.2. Электронный оригинал, изготовленный полуавтоматизированным или автоматизированным образом, предполагающий сохранение графического оформления документа с возможностью форматирования текста и внедрения графических элементов, создается с использованием форматов PDF, DOC, RTF, HTML.

2.9.2. Возможность текстового поиска.

Если при работе с электронным сообщением требуется обеспечить поиск по содержательной части с использованием ключевых слов, то электронная копия бумажного документа, содержащая информацию, предназначенную для распознавания текста и сохранения в текстовом формате, создается в формате с разметкой текста (PDF, DjVu, DOC, RTF, HTML) или простом текстовом формате (TXT).

2.9.3. Возможность интеграции и автоматизированного анализа.

Электронный оригинал, изготовленный полуавтоматизированным или автоматизированным образом, предполагающий необходимость автоматизированной интеграции информации, создается в формате файла XML.

2.10. Бумажная копия электронного документа.

При необходимости использования информации электронного документа в бумажном документообороте могут быть сделаны бумажная копия электронного документа или бумажный дубликат электронного документа.

2.10.1. Бумажная копия электронного документа, используемая для внутреннего документооборота организации, должна содержать всю информацию из соответствующего электронного документа, а также:

• оттиск штампа с текстом (или собственноручную запись с текстом) «Копия электронного документа верна»;

• номер или идентификатор электронного документа и наименование АИС, из которой он получен;

• собственноручную подпись должностного лица, его фамилию и дату создания бумажного документа – копии электронного документа.

Указанная информация размещается на той же стороне листа документа, на которой началось размещение информации соответствующего электронного документа. Если документ продолжается на другой стороне листа или на других листах, то дополнительная заверяющая подпись без расшифровки фамилии и должности ставится на каждом листе, на одной или на обеих сторонах, на которых размещена информация.

2.10.2. Бумажная копия электронного документа, выдаваемая организацией по запросам граждан, государственных и негосударственных структур, должна содержать всю информацию из соответствующего электронного документа, а также:

• оттиск штампа с текстом (или собственноручную запись с текстом) «(наименование организации), (наименование АИС), копия электронного документа верна»;

• номер или идентификатор электронного документа;

• собственноручную подпись должностного лица, его фамилию и дату создания бумажного документа – копии электронного документа;

• печать организации – владельца АИС.

Указанная дополнительная информация размещается на той же стороне листа документа, на которой началось размещение информации соответствующего электронного документа. Если документ продолжается на другой стороне листа или на других листах, то дополнительная заверяющая подпись и печать без расшифровки фамилии и должности ставится на каждом листе, на одной или на обеих сторонах, на которых размещена информация.

Страницы многостраничных документов следует пронумеровать. Допускается брошюрование листов многостраничных документов и заверение первой и последней страниц.

2.10.3. Бумажный документ – дубликат электронного документа – может создаваться лицом, уполномоченным на создание соответствующего электронного документа.

Бумажный дубликат электронного документа, предназначенный для резервного хранения и архивирования внутри организации — владельца АИС, заверяется так же, как бумажная копия электронного документа для целей внутреннего электронного документооборота.

Бумажный дубликат электронного документа, предназначенный для выдачи гражданам, направления в иные организации и органы власти, должен быть заверен в порядке, указанном в п. 2.10.2 настоящего Порядка.

2.11. Способы оформления электронных документов:

2.11.1. Используемые Сторонами ЭД включают в себя содержательную и сопроводительную части. Содержательная часть оформляется исполнителем документа в соответствии с требованиями к форматам электронного документа.

2.11.2. Порядок подготовки и внутреннего согласования содержательной части документов регламентируется внутренними нормативными документами Сторон.

2.11.3. Электронный документ, содержательная часть которого оформлена с нарушением установленных требований, к исполнению не принимается. Сторона, которой на исполнение был направлен такой ЭД, сообщает об этом подготовившей электронный документ Стороне. Ответственность за неисполнение или нарушение сроков исполнения электронных документов несет Сторона, допустившая нарушения установленных требований.

2.11.4. Сопроводительная часть ЭД представляет собой одну или несколько ЭЦП, заверяющих содержательную часть электронного документа, вместе с ранее сформированными ЭЦП. При необходимости сопроводительная часть ЭД включает сертификаты соответствующих ключей подписей и другую служебную информацию (метки времени, замечания и т.д.). Сопроводительная часть является неотъемлемой составляющей электронного документа и обеспечивает подтверждение его подлинности (контроль авторства и целостности) и механизм признания юридической силы электронному документу.

2.11.5. Процедуры оформления и обмена электронными документами должны обеспечивать необходимые условия признания равнозначности ЭЦП собственноручной подписи в соответствии

с Федеральным законом от 10 января 2002 № 1-ФЗ «Об электронной цифровой подписи», ст. 4.

2.11.6. Электронные документы, являющиеся непосредственным основанием для совершения юридически значимых действий (например, поручение о перечислении денежных средств), заверяются ЭЦП соответствующими должностными лицами Сторон, наделенными правом собственноручной подписи аналогичных документов на бумажных носителях.

2.11.7. Электронные документы, не используемые непосредственно для совершения юридически значимых действий (например, информационно-справочные документы), могут заверяться ЭЦП лицами, ответственными за прием/отправку и/или исполнение таких документов, например операторами автоматизированного рабочего места обмена электронными документами.

2.11.8. Электронные документы, в которых проверка подлинности ЭЦП в сопроводительной части дала отрицательный результат, к исполнению не принимается. Сторона, которой на исполнение был направлен такой электронный документ, сообщает об этом подготовившей его Стороне.

2.11.9. Электронные документы, заверенные ЭЦП до момента ввода в обращение и регистрации соответствующего сертификата ключа подписи или в момент приостановки его действия, или после окончания срока его действия, к исполнению не принимаются. Сторона, которой на исполнение был направлен электронный документ, заверенный такой ЭЦП, сообщает об этом подготовившей его Стороне.

3. Документы, создаваемые и используемые в электронной форме в режиме «одного окна»

В работе служб «одного окна» и согласующих организаций при подготовке и согласовании документов для заявителей могут создаваться электронные документы:

3.1. Электронные копии документов, которые имеют непосредственное отношение к заявителям и на момент подачи заявления имеются у заявителей в окончательно оформленном и действительном виде: заявления, удостоверения личности, доверенности, документы о государственной регистрации актов гражданского состояния, учредительные документы, свидетельства о регистрации, лицензии, сертификаты и иные личные документы, составляющие персональные данные.

3.2. Электронные копии нормативно-распорядительных документов организации, держателя «одного окна» и согласующих организаций, а именно документы, имеющиеся у организации, держателя «одного окна» и согласующих организаций на момент обращения заявителей (нормативные документы, распорядительные документы, иные ранее созданные документы правового, административного или технического характера).

3.3. Электронные копии и/или электронные оригиналы документов, создаваемых в режиме «одного окна» в процессах подготовки и согласования документов: поручения, заключения, справки, согласования, протоколы, решения, распоряжения, копии, уведомления и иные промежуточные документы.

3.4. Электронные копии и/или электронные оригиналы документов, выдаваемых заявителю по его запросу (выдаваемые документы и приложения к ним, мотивированные отказы с рекомендациями необходимых действий для получения запрашиваемых документов).

4. Условия создания и использования электронных документов

4.1. Использование электронного документа вместо бумажного документа приводит к сокращению времени подготовки документа, выдаваемого заявителям.

4.2. Использование электронного документа вместо бумажного документа приводит к сокращению затрат на организацию бумажного делопроизводства.

4.3. Создаваемые электронные документы могут быть неоднократно использованы в процессе подготовки запрашиваемого заявителем документа или иных документов, выдаваемых в режиме «одного окна».

4.4. Использование электронной формы документа не противоречит законодательству Российской Федерации.

4.5. Между участниками межведомственного (межсетевого) электронного документооборота заключаются соглашения об электронном взаимодействии с использованием ЭЦП.

4.5.1. Соглашения о МЭД устанавливают права и обязанности участников электронного информационного взаимодействия по следующей схеме: отправитель электронного сообщения (документа) – оператор АИС, обеспечивающей электронное взаимодействие, – получатель электронного сообщения (документа).

4.5.2. Соглашения о МЭД устанавливают условия признания юридической силы электронных документов и условия (ограничения) по распространению электронных документов.

4.5.3. МЭД или электронное информационное взаимодействие между участниками осуществляется по согласованным протоколам, в которых устанавливаются:

- перечень типов передаваемых электронных документов;
- требования к структуре и содержательной части электронных документов;
- используемые (допустимые) форматы файлов электронных документов;
- условия признания документа переданным;
- условия признания документа полученным;
- условия распространения обязательных сообщений;
- условия обеспечения сохранности информации.

5. Порядок сканирования и размещения электронных копий документов

5.1. Сканированию подлежат документы, принимаемые от заявителя и промежуточные, создаваемые в процессе подготовки документа, выдаваемого для заявителя, и выдаваемые заявителю документы, если при дальнейшей работе с ними предусматривается:

5.1.1. Многократное создание копий (дубликатов).

5.1.2. Необходимость работы с документом одновременно несколькими исполнителями.

5.1.3. Передача в другие службы «одного окна» или согласующие организации.

5.1.4. Автоматизированная обработка смысловой части документа в информационной системе службы «одного окна» или производственной системе держателя «одного окна».

5.1.5. Долговременное либо кратковременное хранение копий документов.

5.2. Документы сканируются после их первичной проверки сотрудником службы «одного окна» и регистрации в АИС.

5.3. Параметры сканирования устанавливаются оператором АИС исходя из потребностей производственного процесса, связанного с обработкой содержащейся в документе информации.

5.4. Электронные копии бумажных документов, полученные методом сканирования, проходят визуальную проверку на соответствие заданным требованиям и размещаются в хранилище АИС «одного окна» или АИС держателя «одного окна», обеспечивающей производственную деятельность организации.

5.5. Отсканированные документы перед размещением в хранилище АИС подписываются ЭЦП сотрудником, ответственным за сканирование и размещение электронных копий в АИС.

6. Подготовка электронного документа к отправке

6.1. Порядок подготовки содержательной (текстовой) части электронного документа, в том числе сверки и внесения в нее изменений, определяется внутренними инструкциями Сторон и аналогичен порядку подготовки документов на бумажных носителях, за исключением того, что электронные документы на каждом этапе согласования (визирования) заверяются не собственноручной подписью, а ЭЦП соответствующим исполнителем.

6.2. Подготовленному электронному документу присваиваются реквизиты, однозначно определяющие сам электронный документ (дата и регистрационный номер ЭД) и Сторону, его подготовившую (например, кодифицированное обозначение Стороны и региона). Указанные реквизиты могут быть оформлены в виде имени файла содержательной части электронного документа.

6.3. Подготовленный электронный документ, заверенный ЭЦП соответствующими уполномоченными лицами Сторон, передается оператору автоматизированного рабочего места АИС обмена электронными документами.

6.4. Оператор АРМ ведет журнал учета отправки электронных документов и получения подтверждений об их доставке по форме, позволяющей отразить все необходимые реквизиты электронных документов и обстоятельства их отправки/получения.

6.5. Оператор АРМ обязан перед отправкой:

проверить подлинность ЭЦП электронных документов;

проверить статус соответствующих сертификатов ключей подписи;

сверить полномочия лиц, сформировавших ЭЦП;

заверить отправляемые электронные документы с ЭЦП, используя свой закрытый ключ ЭЦП;

сохранить отправляемые электронные документы с ЭЦП в архиве.

Затем в случае положительного результата произведенных проверок оператор АРМ производит отправку электронных документов.

6.6. Отправка электронных документов может осуществляться непосредственно исполнителем документа при условии выполнения им требований п. 4.4, 4.5.

6.7. Организация хранения архивов отправляемых (получаемых) электронных документов осуществляется Сторонами самостоятельно в установленном порядке.

7. Порядок передачи (отправки)/приема электронных документов

7.1. Передача (отправка) электронных документов осуществляется с использованием АИС, являющихся официальными системами организаций, введенными в эксплуатацию в установленном порядке.

7.2. Электронные документы, передаваемые в процессе их согласования, подписываются ЭЦП уполномоченного лица.

7.3. Факт передачи электронного документа регистрируется в АИС организации, передающей документ.

7.3.1. В АИС организации, передающей электронный документ, фиксируются дата и время его отправки, регистрационный номер и отправитель документа.

7.3.2. Копия электронного документа, переданного в процессе согласования, сохраняется в АИС организации, передавшей документ.

7.3.3. Датой и временем отправки документа считаются дата и время отправки из АИС организации, отправившей электронный документ, если иное не предусмотрено протоколом электронного информационного взаимодействия.

8. Обработка электронного документа при получении

8.1. Оператор автоматизированного рабочего места АИС Стороны-получателя выполняет процедуру получения направленных ей электронных документов.

8.2. Оператор АРМ ведет журнал учета полученных электронных документов и отправленных подтверждений об их доставке по форме, позволяющей отразить все необходимые реквизиты ЭД и обстоятельства их отправки/получения.

8.3. Перед направлением электронных документов исполнителю оператор обязан:

проверить подлинность ЭЦП электронных документов;

проверить статус соответствующих сертификатов ключей подписи;

сверить полномочия лиц, сформировавших ЭЦП;

заверить полученные электронные документы ЭЦП, используя свой закрытый ключ ЭЦП;

сохранить полученные электронные документы с ЭЦП в архиве.

8.4. Затем в случае положительного результата произведенных проверок оператор направляет электронные документы исполнителю. Электронные документы, не прошедшие проверку, сохраняются в оригинальном виде в отдельном архиве на случай разрешения относительно них конфликтных ситуаций. Обо всех случаях непро-

хождения проверки электронные документы оператор извещает администратора информационной безопасности и уполномоченное лицо Стороны-отправителя.

8.4.1. Возможно использование следующих типов уведомлений о доставке:

техническое уведомление о доставке электронных документов адресату, при этом техническое уведомление представляющее собой, автоматически (средствами системы электронной почты), без участия оператора, сформированное и заверенное ЭЦП, которой соответствует обезличенный сертификат ключа подписи, зарегистрированный за АРМ;

служебное уведомление о доставке электронных документов, при этом служебное уведомление представляет собой электронный документ, формируемый и заверенный ЭЦП соответствующим уполномоченным лицом Стороны-получателя. Доставка служебных уведомлений подтверждается техническим уведомлением.

8.4.2. Датой и временем приема электронного документа являются дата и время отправки уведомления, если иное не предусмотрено протоколом электронного информационного взаимодействия.

8.4.3. Режим доставки со служебными уведомлениями обязателен в случае отправки/получения электронных документов, являющихся непосредственным основанием для совершения юридически значимых действий. Для иных электронных документов режим доставки со служебным уведомлением не обязателен.

8.4.4. Служебные и технические уведомления хранятся в архивах вместе с соответствующими электронными документами. Срок хранения уведомлений определяется сроком хранения соответствующих электронных документов.

8.4.5. Отзыв электронного документа. Сторона-отправитель вправе отозвать направленный Стороне-исполнителю электронных документов до момента принятия их к исполнению. В случае необходимости отзыва Сторона-отправитель направляет электронный документ установленной формы с запросом об отзыве, заверенный ЭЦП соответствующим уполномоченным лицом Стороны-отправителя. В запросе указываются основания отзыва и реквизиты, идентифицирующие отзываемых электронных документов.

8.5. Получение электронных документов может осуществляться непосредственно исполнителем, при условии выполнения им требований п. 5.2, 5.3.

8.6. Исполнитель электронных документов проверяет подлинность ЭЦП, статус сертификатов ключей подписи и полномочия их владельцев и по результатам проверки принимает либо не принимает к исполнению.

8.7. В случаях непрохождения проверки электронных документов исполнитель обязан незамедлительно доложить об этом руководителю подразделения и Администратору информационной безопасности.

8.8. Факт приема электронного документа фиксируется в АИС организации, принимающей электронный документ, с формированием и передачей уведомления о приеме.

8.11. Электронный документ, полученный на согласование, хранится в АИС организации, получившей документ.

9. Учет электронных документов

9.1. Учет электронных документов ведется в соответствии с требованиями нормативных документов и обязательной регистрацией: даты и регистрационного номера ЭД; а также номеров сертификатов ключей подписи лиц, заверивших электронные документы ЭЦП, формирования ЭЦП, времени отправки/получения электронных документов, отправки/получения уведомления о доставке, результатов проверки электронных документов.

9.2. Учет ведется как оператором автоматизированного рабочего места АИС, так и исполнителями электронных документов.

9.3. Учет осуществляется путем автоматизированного ведения электронных или бумажных журналов учета установленной формы.

9.4. Стороны должны обеспечивать защиту учетной информации, содержащейся в электронных журналах учета, от несанкционированного доступа и воздействия, а также обеспечивать надежность ее хранения. Срок хранения учетных данных определяется сроком хранения учитываемых электронных документов.

9.5. Особенности учета электронных документов при обмене определяются соглашениями Сторон.

10. Порядок учета, хранения и уничтожения электронных документов

10.1. Документы, созданные в электронном виде и подписанные ЭЦП, учтенные электронные документы об обмене должны храниться в течение сроков, предусмотренных нормативными документами в АИС организации, – электронном архиве.

10.2. Хранение документов, ранее размещенных для хранения в АИС, продолжается до истечения сроков, определенных при их создании.

10.3. Срок хранения электронных документов устанавливается в соответствии с требованиями федерального законодательства об архивном деле и нормативных правовых документов, перечней документов и дел со сроками хранения, номенклатур дел для хранения документов в зависимости от содержащейся в них информации и вне зависимости от места хранения документов и формы документов (бумажная или электронная).

10.4. Для выполнения текущих работ по ведению электронных архивов и их контролю Стороны назначают ответственных лиц.

10.5. Если соглашениями Сторон и/или используемой Сторонами технологией не предусмотрено иное, электронные документы должны храниться в оригинальном виде, т.е. в том, в котором они были сформированы и/или отправлены/получены с сохранением всех реквизитов электронных документов, включая все заверяющие ЭЦП.

10.6. Срок хранения электронных документов соответствует сроку хранения их бумажных аналогов.

10.7. Хранение электронных документов должно сопровождаться хранением соответствующих журналов учета, сертификатов ключей подписи, уведомлений о доставке ЭД, а также средств, обеспечивающих возможность работы с электронными документами и ЭЦП.

10.8. Для сертификатов ключей подписи хранимых электронных документов должны быть оформлены и храниться в установленном порядке; документы, подтверждающие статус сертификатов ключей подписи (регистрационные карточки, справки об отзыве и приостановлении действия сертификатов ключей подписи и т.д.).

10.9. Электронные документы учитываются в составе архивного фонда фондообразователя по описям, единицам учета и единицам хранения. Информационный объем электронных документов указывается в мегабайтах (Мб). За единицу учета принимается единица хранения или комплект единиц хранения с записью файла или нескольких файлов, составляющих единый программно-информационный объект (текст, гипертекст, мультимедийный объект, базу данных, банк данных, базу знаний), а также сопроводительная документация.

За единицу хранения электронных документов принимается физически обособленный носитель (дискета, жесткий диск, компакт-диск и др.) с сопроводительной документацией.

10.10. Обязательными условиями архивного хранения электронных документов являются:

наличие в АИС – электронном архиве программно-аппаратных средств для хранения, копирования и воспроизведения электронных документов, их перезаписи в новые форматы, передачи информации по каналам связи и др.;

обеспечение доступа к информации установленных категорий пользователей, а также обеспечение защиты информации от несанкционированного доступа (путем применения соответствующих технических средств и правовых норм);

обеспечение режима хранения электронных документов, исключающего утрату, уничтожение или искажение информации.

Хранение электронных документов предусматривает также поддержание оптимальных режимов хранения их носителей. Технические параметры данных режимов определяются соответствующими государственными стандартами. По мере старения носителя должна производиться перезапись электронных документов на новые носители.

10.11. Уничтожение (удаление) электронных документов, используемых в АИС организаций, осуществляется по решению владельца АИС, если уничтожение (удаление) документа не противоречит действующему законодательству об архивном деле, нормативным правовым документам, утвержденным перечням документов и дел со сроками хранения, номенклатурам дел, являющихся одновременно классификаторами АИС.

10.12. Уничтожение (удаление) электронных документов, занесенных в электронный архив, осуществляется в соответствии с законодательством об архивном деле, если более длительный срок не установлен распорядительными документами.

10.13. Срок хранения сертификата ключа подписи в форме электронного документа определяется действующим законодательством и нормативными правовыми актами в области ЭЦП.

11. Обязательства и ответственность Сторон, использующих ЭЦП

11.1. Владелец АИС, в которой при создании электронных документов применяется ЭЦП, обязан обеспечить:

соответствие применяемого программного и аппаратного обеспечения требованиям, определенным производителем средств ЭЦП, и требованиям, содержащимся в регламентах удостоверяющих центров;

обеспечить соблюдение требований действующего законодательства об ЭЦП при выполнении в АИС действий с электронными документами, требующими использования ЭЦП.

11.2. Владелец сертификата ключа ЭЦП обязан выполнять требования действующего законодательства, нормативных правовых актов в области электронной цифровой подписи, нормативных актов организации – владельца АИС, в которой он применяет ЭЦП, регламент удостоверяющего центра, правомерные требования и распоряжения администраторов, взаимодействующих АИС, а также настоящий Порядок.

11.3. Владельцы АИС, удостоверяющие центры, участники электронного информационного обмена и иные лица несут предусмотренную действующим законодательством ответственность за причинение вреда их действиями или бездействием в случае несоблюдения ими требований настоящего Порядка.

11.4. Ответственность за правовые последствия, ставшие следствием исполнения электронных документов, заверенных подлинными ЭЦП, несет Сторона, уполномоченные лица которой заверили подготовленные электронные документы. Мера ответственности определяется в порядке, установленном законодательством Российской Федерации.

11.5. В случае наличия в электронных документах конфиденциальной информации Стороны обязаны соблюдать установленные требования по ее защите на всех этапах обработки, хранения и передачи этой информации. Сторона, допустившая нарушения требований по защите конфиденциальной информации, несет ответственность в соответствии с российским законодательством.

Приложение 8

Общее описание организации взаимодействия системы межведомственного (межсетевого) электронного документооборота с системой внутреннего электронного документооборота

В системе внутреннего электронного документооборота отправителя, – для адресата (адресатов) формируется электронное сообщение и в автоматическом режиме загружается в шлюз системы межведомственного (межсетевого) электронного документооборота.

Для загрузки электронного сообщения в шлюз МЭД используется автоматизированное рабочее место (АРМ) шлюза с установленным клиентским программным обеспечением для работы с базой данных шлюза.

Автоматизированное рабочее место шлюза через пользовательский интерфейс взаимодействует с базой данных шлюза. Взаимодействие заключается в загрузке или выгрузке данных, содержащихся в электронном сообщении, в базу данных шлюза. Прикладное программное обеспечение шлюза МЭД обеспечивает работу с хранящимися в базе данных документами в электронной форме (поиск, просмотр, распечатка, подготовка электронных сообщений к передаче адресатам и т.д.).

Передача электронных сообщений осуществляется в автоматическом режиме из соответствующей почтовой очереди клиентом комплекса программ «Почтовая служба», установленного на шлюзе МЭД.

Прием электронных сообщений выполняется также в автоматическом режиме. Прикладное программное обеспечение шлюза через клиента комплекса программ «Почтовая служба» получает из почтовой очереди электронные сообщения и помещает их в базу данных шлюза. Поступившие в составе электронного сообщения данные могут быть просмотрены с использованием АРМ шлюза.

Электронное сообщение содержит документ в электронной форме и следующий набор реквизитов в формате XML, приведенный в таблице.

Атрибут	Тип	Комментарий
Тип электронного сообщения	Число сообщения	Определяет тип электронного сообщения документооборота
Регистрационный номер исходящего документа	Строка	
Дата исходящего документа	Дата	Дата регистрации исходящего документа у отправителя
Данные о лице, подписавшем документ	Группа	Код, фамилия, имя, отчество, должность лица, подписавшего документ
Подразделение – ответственный исполнитель документа	Группа	Код и наименование подразделения
Краткое содержание (аннотация) документа	Строка	
Количество страниц основного документа и приложений	Число	
Адресат документа	Группа	Код адресата и наименование адресата документа
Связанные документы	Группа	Уникальный идентификатор документа, регистрационный номер и дата регистрации документа, тип связки («в ответ на», «в дополнение» и т.д.)
Файлы электронного документа	Группа	Количество и имена файлов электронного документа

При загрузке электронного сообщения в систему электронного документооборота реквизиты, содержащиеся в соответствующем XML-файле, могут использоваться для заполнения полей регистрационной (учетной) карточки поступившего в электронной форме документа. Для преобразования формата поступившего электронного сообщения в формат представления данных системы электронного документооборота используется программное обеспечение соответствующего адаптера.

Приложение 9

Квалификационная характеристика главного специалиста по защите информации

(Выписка из Квалификационного справочника должностей руководителей, специалистов и других служащих. Утверждено Постановлением Минтруда России от 21 августа 1998 г. № 37(в ред. от 18.10.2007 года))

Должностные обязанности. Руководит выполнением работ по комплексной защите информации в отрасли, на предприятии, в учреждении, организации, обеспечивая эффективное применение всех имеющихся организационных и инженерно-технических мер в целях защиты сведений, составляющих государственную тайну.

Участвует в разработке технической политики и определении перспектив развития технических средств контроля, организует разработку и внедрение новых технических и программно-математических средств защиты, исключающих или существенно затрудняющих несанкционированный доступ к служебной информации, составляющей государственную или коммерческую тайну.

Участвует в рассмотрении технических заданий на проекты изделий, научно-исследовательские и опытно-конструкторские работы, подлежащие защите, осуществляет контроль за включением в них требований нормативно-технических и методических документов по защите информации и выполнением этих требований. Готовит предложения для включения в планы и программы работ организационных и инженерно-технических мер по защите информационных систем.

Участвует в работе по созданию безопасных информационных технологий, отвечающих требованиям комплексной защиты информации.

Организует проведение научно-исследовательских работ в области совершенствования систем защиты информации и повышения их эффективности. Выполняет весь комплекс (в том числе особо сложных) работ, связанных с контролем и защитой информации, на основе разработанных программ и методик.

Организует сбор и анализ материалов о возможных каналах утечки информации, в том числе по техническим каналам, при проведении исследований и разработок, связанных с созданием и производством специальных изделий (продукции), необходимых для проведения работ по обеспечению защиты информации.

Обеспечивает координацию проводимых организационно-технических мероприятий, разработку методических и нормативных материалов и оказание необходимой методической помощи в проведении работ по защите информации, оценке технико-экономической эффективности предлагаемых и реализуемых организационно-технических решений.

Организует работу по сбору и систематизации необходимой информации об объектах, подлежащих защите, и охраняемых сведениях, осуществляет методическое руководство и контроль за работой по оценке технико-экономического уровня и эффективности разрабатываемых мер по защите информации.

Возглавляет работу по обобщению данных о потребности в технических и программно-математических средствах защиты информации, аппаратуре контроля, составлению заявок на изготовление этих средств, организует их получение и распределение между объектами защиты.

Содействует распространению передового опыта и внедрению современных организационно-технических мер, средств и способов защиты информации с целью повышения ее эффективности.

Обеспечивает контроль за выполнением требований нормативно-технической документации, за соблюдением установленного порядка выполнения работ, а также действующего законодательства при решении вопросов, касающихся защиты информации. Координирует деятельность подразделений и специалистов по защите информации в отрасли, на предприятии, в учреждении, организации.

Должен знать: законодательные и нормативные правовые акты о государственной тайне; документы, определяющие основные направления экономического и социального развития отрасли; нормативные и методические материалы по вопросам, связанным с обеспечением защиты информации; перспективы развития, специализацию и направления деятельности учреждения, организации, предприятия и их подразделений; характер взаимодействия подразделений в процессе исследований и разработок и порядок прохождения служебной информации; систему организации комплексной защиты информации, действующую в отрасли, учреждении, организации, на предприятии; перспективы и направления развития тех-

нических и программно-математических средств защиты информации; методы и средства контроля охраняемых сведений, выявления каналов утечки информации, организацию технической разведки; методы планирования и организации проведения научных исследований, разработок, выполнения работ по защите информации; порядок заключения договоров на проведение специальных исследований и проверок, работ по защите технических средств передачи, обработки, отображения и хранения информации; отечественный и зарубежный опыт в области технической разведки и защиты информации; основы экономики, организации производства, труда и управления; правила и нормы охраны труда.

Требования к квалификации. Высшее профессиональное (техническое) образование и стаж работы по защите информации не менее 5 лет.

Приложение 10

Методы и способы защиты информации в автоматизированных информационных системах персональных данных

(приказ Федеральной службы по техническому и экспортному контролю от 5 февраля 2010 г. N 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных»)

1. Общие положения

1.1. К методам и способам защиты информации в автоматизированных информационных системах относятся:

методы и способы защиты информации, обрабатываемой техническими средствами АИС, от несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий (далее – методы и способы защиты информации от несанкционированного доступа);

методы и способы защиты речевой информации, а также информации, представленной в виде информативных электрических сигналов, физических полей, от несанкционированного доступа к персональным данным, результатом которого может стать копирование, распространение персональных данных, а также иных несанкционированных действий (далее – методы и способы защиты информации от утечки по техническим каналам).

1.2. Для выбора и реализации методов и способов защиты информации в АИС оператором или уполномоченным лицом может назначаться структурное подразделение или должностное лицо (работник), ответственные за обеспечение безопасности персональных данных.

Для выбора и реализации методов и способов защиты информации в АИС может привлекаться организация, имеющая оформленную в установленном порядке лицензию на осуществление деятельности по технической защите конфиденциальной информации.

1.3. Выбранные и реализованные методы и способы защиты информации в АИС должны обеспечивать нейтрализацию предполагаемых угроз безопасности персональных данных при их обработке в составе создаваемой оператором (уполномоченным лицом) системы защиты персональных данных.

2. Методы и способы защиты информации от несанкционированного доступа

2.1. Методами и способами защиты информации от НСД являются:

реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам, в АИС и связанным с ее использованием работам, документам;

ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации;

разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;

регистрация действий пользователей и обслуживающего персонала, контроль НСД и действий пользователей, обслуживающего персонала и посторонних лиц;

учет и хранение съемных носителей информации, и их обращение, исключающее хищение, подмену и уничтожение;

резервирование технических средств, дублирование массивов и носителей информации;

использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;

использование защищенных каналов связи;

размещение технических средств, позволяющих осуществлять обработку персональных данных, в пределах охраняемой территории;

организация физической защиты помещений и собственно технических средств, позволяющих осуществлять обработку персональных данных;

предотвращение внедрения в АИС вредоносных программ (программ-вирусов) и программных закладок.

2.2. В системе защиты персональных данных АИС в зависимости от класса информационной системы и исходя из угроз безопасности персональных данных, структуры информационной системы, наличия межсетевого взаимодействия и режимов обработки персональных данных с использованием соответствующих методов и способов защиты информации от несанкционированного доступа реализуются функции управления доступом, регистрации и учета, обеспечения целостности, анализа защищенности, обеспечения безопасного межсетевого взаимодействия и обнаружения вторжений.

Методы и способы защиты информации от несанкционированного доступа, обеспечивающие функции управления доступом, регистрации и учета, обеспечения целостности, анализа защищенности,

обеспечения безопасного межсетевого взаимодействия в зависимости от класса АИС, определяются оператором (уполномоченным лицом) в соответствии с разд. 4.

2.3. В АИС, которые имеют подключение к информационно-телекоммуникационным сетям международного информационного обмена (сетям связи общего пользования) или при функционировании которых предусмотрено использование съемных носителей информации, используются средства антивирусной защиты.

2.4. При взаимодействии АИС с информационно-телекоммуникационными сетями международного информационного обмена (сетями связи общего пользования) наряду с методами и способами, указанными в п. 2.1, основными методами и способами защиты информации от несанкционированного доступа являются:

межсетевое экранирование с целью управления доступом, фильтрацей сетевых пакетов и трансляцей сетевых адресов для скрытия структуры информационной системы;

обнаружение вторжений в АИС, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности персональных данных;

анализ защищенности АИС, предполагающий применение специализированных программных средств (сканеров безопасности);

защита информации при ее передаче по каналам связи;

использование смарт-карт, электронных замков и других носителей информации для надежной идентификации и аутентификации пользователей;

использование средств антивирусной защиты;

централизованное управление системой защиты персональных данных АИС.

2.5. Подключение АИС, обрабатывающих государственные информационные ресурсы, к информационно-телекоммуникационным сетям международного информационного обмена осуществляется в соответствии с Указом Президента Российской Федерации от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»[59].

2.6. Для обеспечения безопасности персональных данных при подключении АИС к информационно-телекоммуникационным сетям международного информационного обмена (сетям связи общего пользования) с целью получения общедоступной информации помимо методов и способов, указанных в п. 2.1 и 2.4, применяются следующие основные методы и способы защиты информации от НСД:

фильтрация входящих (исходящих) сетевых пакетов по правилам, заданным оператором (уполномоченным лицом);

периодический анализ безопасности установленных межсетевых экранов на основе имитации внешних атак на АИС;

активный аудит безопасности АИС на предмет обнаружения в режиме реального времени несанкционированной сетевой активности;

анализ принимаемой по информационно-телекоммуникационным сетям международного информационного обмена (сетям связи общего пользования) информации, в том числе на наличие компьютерных вирусов.

Для реализации указанных методов и способов защиты информации могут применяться межсетевые экраны, системы обнаружения вторжений, средства анализа защищенности, специализированные комплексы защиты и анализа защищенности информации.

2.7. Для обеспечения безопасности персональных данных при удаленном доступе к АИС через информационно-телекоммуникационную сеть международного информационного обмена (сеть связи общего пользования) помимо методов и способов, указанных в п. 2.1 и 2.4, применяются следующие основные методы и способы защиты информации от НСД:

проверка подлинности отправителя (удаленного пользователя) и целостности передаваемых по информационно-телекоммуникационной сети международного информационного обмена (сети связи общего пользования) данных;

управление доступом к защищаемым персональным данным информационной сети;

использование атрибутов безопасности.

2.8. Для обеспечения безопасности персональных данных при межсетевом взаимодействии отдельных информационных систем через информационно-телекоммуникационную сеть международного информационного обмена (сеть связи общего пользования) помимо методов и способов, указанных в п. 2.1 и 2.4, применяются следующие основные методы и способы защиты информации от НСД:

создание канала связи, обеспечивающего защиту передаваемой информации;

осуществление аутентификации взаимодействующих АИС и проверка подлинности пользователей и целостности передаваемых данных.

2.9. Для обеспечения безопасности персональных данных при межсетевом взаимодействии отдельных АИС разных операторов через информационно-телекоммуникационную сеть международного

информационного обмена (сеть связи общего пользования) помимо методов и способов, указанных в п. 2.1 и 2.4, применяются следующие основные методы и способы защиты информации от НСД:

создание канала связи, обеспечивающего защиту передаваемой информации;

аутентификация взаимодействующих АИС и проверка подлинности пользователей и целостности передаваемых данных;

обеспечение предотвращения возможности отрицания пользователем факта отправки персональных данных другому пользователю;

обеспечение предотвращения возможности отрицания пользователем факта получения персональных данных от другого пользователя.

2.10. Обмен персональными данными при их обработке в АИС осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) применения технических средств.

2.11. Подключение АИС к АИС другого класса или к информационно-телекоммуникационной сети международного информационного обмена (сети связи общего пользования) осуществляется с использованием межсетевых экранов.

2.12. Программное обеспечение средств защиты информации, применяемых в информационных системах 1-го класса, проходит контроль на отсутствие недекларированных возможностей.

Необходимость проведения контроля на отсутствие недекларированных возможностей программного обеспечения средств защиты информации, применяемых в информационных системах 2- и 3-го классов, определяется оператором (уполномоченным лицом).

2.13. В зависимости от особенностей обработки персональных данных и структуры информационных систем могут разрабатываться и применяться другие методы защиты информации от несанкционированного доступа, обеспечивающие нейтрализацию угроз безопасности персональных данных.

3. Методы и способы защиты информации от утечки по техническим каналам

3.1. Защита речевой информации и информации, представленной в виде информативных электрических сигналов и физических полей, осуществляется в случаях, когда при определении угроз безопасно-

сти персональных данных и формировании модели угроз применительно к АИС являются актуальными угрозы утечки информации акустической (речевой), видовой и информации по каналам побочных электромагнитных излучений и наводок (ПЭМИН).

3.2. Для исключения утечки персональных данных за счет ПЭМИН в информационных системах 1-го класса могут применяться следующие методы и способы защиты информации:

использование технических средств в защищенном исполнении;

использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;

размещение объектов защиты в соответствии с предписанием на эксплуатацию;

размещение понижающих трансформаторных подстанций электропитания и контуров заземления технических средств в пределах охраняемой территории;

обеспечение развязки цепей электропитания технических средств с помощью защитных фильтров, блокирующих (подавляющих) информативный сигнал;

обеспечение электромагнитной развязки между линиями связи и другими цепями вспомогательных технических средств и систем, выходящими за пределы охраняемой территории, и информационными цепями, по которым циркулирует защищаемая информация.

3.3. В информационных системах 2-го класса для обработки информации используются средства вычислительной техники, удовлетворяющие требованиям национальных стандартов по электромагнитной совместимости, безопасности и эргономическим требованиям к средствам отображения информации, санитарным нормам, предъявляемым к видеодисплейным терминалам средств вычислительной техники.

3.4. При применении в АИС функции голосового ввода персональных данных в информационную систему или функции воспроизведения информации акустическими средствами информационных систем для информационной системы 1-го класса реализуются методы и способы защиты акустической (речевой) информации.

Методы и способы защиты акустической (речевой) информации заключаются в реализации организационных и технических мер для обеспечения звукоизоляции ограждающих конструкций помещений, в которых расположена АИС, их систем вентиляции и кондиционирования, не позволяющей вести прослушивание акустической (речевой) информации при голосовом вводе персональных данных в информационной системе или воспроизведении информации акустическими средствами.

Величина звукоизоляции определяется оператором исходя из характеристик помещения, его расположения и особенностей обработки персональных данных в АИС.

3.5. Размещение устройств вывода информации средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав информационной системы, в помещениях, осуществляется таким образом, чтобы была исключена возможность просмотра посторонними лицами текстовой и графической видовой информации, содержащей персональные данные.

4. Методы и способы защиты информации от несанкционированного доступа в зависимости от класса информационной системы

4.1. Методы и способы защиты информации от НСД для обеспечения безопасности персональных данных в информационных системах 4-го класса и целесообразность их применения определяются оператором (уполномоченным лицом).

4.2. Методы и способы защиты информации от НСД, обеспечивающие функции управления доступом, регистрации и учета, обеспечения целостности и безопасного межсетевого взаимодействия для информационных систем 3-го класса.

4.2.1. Для информационных систем 3-го класса при однопользовательском режиме обработки персональных данных применяются следующие основные методы и способы защиты информации:

а) управление доступом:

идентификация и проверка подлинности пользователя при входе в АИС по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов;

б) регистрация и учет:

регистрация входа (выхода) пользователя в систему (из системы) либо загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АИС. В параметрах регистрации указываются дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы;

учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета;

в) обеспечение целостности:

обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность программных средств проверяется при загрузке системы по наличию имен (идентификаторов) компонентов системы защиты персональных данных; а целостность программной среды обеспечивается отсутствием в АИС средств разработки и отладки программ;

физическая охрана АИС (технических средств и носителей информации), предусматривающая контроль доступа в помещения информационной системы посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АИС и хранилище носителей информации;

периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей информационной системы с помощью тест-программ, имитирующих попытки НСД;

наличие средств восстановления системы защиты персональных данных, предусматривающих ведение двух копий программных компонентов средств защиты информации, их периодическое обновление и контроль работоспособности.

4.2.2. Для информационных систем 3-го класса при многопользовательском режиме обработки персональных данных и равных правах доступа к ним пользователей применяются следующие основные методы и способы защиты информации:

а) управление доступом:

идентификация и проверка подлинности пользователя при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов;

б) регистрация и учет:

регистрация входа (выхода) пользователя в систему (из системы) либо загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения информационной системы. В параметрах регистрации указываются дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы, результат попытки входа (успешная или неуспешная);

учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета;

в) обеспечение целостности:

обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность программных

средств проверяется при загрузке системы по наличию имен (идентификаторов) компонентов системы защиты персональных данных, а целостность программной среды обеспечивается отсутствием в информационной системе средств разработки и отладки программ во время обработки и (или) хранения защищаемой информации;

физическая охрана АИС (устройств и носителей информации), предусматривающая контроль доступа в помещения информационной системы посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АИС и хранилище носителей информации;

периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей информационной системы с помощью тест-программ, имитирующих попытки НСД;

наличие средств восстановления системы защиты персональных данных, предусматривающих ведение двух копий программных компонентов средств защиты информации, их периодическое обновление и контроль работоспособности.

4.2.3. Для информационных систем 3-го класса при многопользовательском режиме обработки персональных данных и разных правах доступа к ним пользователей применяются следующие основные методы и способы защиты информации:

а) управление доступом:

идентификация и проверка подлинности пользователя при входе в систему по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов;

б) регистрация и учет:

регистрация входа (выхода) пользователя в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения информационной системы. В параметрах регистрации указываются дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы, результат попытки входа (успешная или неуспешная), идентификатор (код или фамилия) пользователя, предъявленный при попытке доступа;

учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета с отметкой об их выдаче (приеме);

в) обеспечение целостности:

обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность программных

средств проверяется при загрузке системы по контрольным суммам компонентов средств защиты информации, а целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации;

физическая охрана АИС (устройств и носителей информации), предусматривающая контроль доступа в помещения информационной системы посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АИС и хранилище носителей информации;

периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей АИС с помощью тест-программ, имитирующих попытки НСД;

наличие средств восстановления системы защиты персональных данных, предусматривающих ведение двух копий программных компонент средств защиты информации, их периодическое обновление и контроль работоспособности.

4.2.4. Безопасное межсетевое взаимодействие для информационных систем 3-го класса при их подключении к сетям международного информационного обмена, а также для распределенных информационных систем 3-го класса при их разделении на подсистемы достигается путем применения средств межсетевого экранирования (межсетевых экранов), которые обеспечивают:

фильтрацию на сетевом уровне для каждого сетевого пакета независимо (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов);

идентификацию и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия;

регистрацию входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова (регистрация выхода из системы не проводится в моменты аппаратурного отключения межсетевого экрана);

контроль целостности своей программной и информационной частей;

фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;

восстановление свойств межсетевого экрана после сбоев и отказов оборудования;

регламентное тестирование реализации правил фильтрации, процессов идентификации и аутентификации администратора межсетевого экрана, регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной частей, процедуры восстановления.

Межсетевые экраны, которые обеспечивают выполнение указанных выше функций, применяются в распределенных информационных системах 2-го и 1-го классов при их разделении на отдельные части.

При разделении информационной системы с помощью межсетевых экранов на отдельные части для последних может устанавливаться более низкий класс, чем для информационной системы в целом.

4.3. Методы и способы защиты информации от НСД, обеспечивающие функции управления доступом, регистрации и учета, обеспечения целостности и безопасного межсетевого взаимодействия для информационных систем 2-го класса.

4.3.1. Для информационных систем 2-го класса при однопользовательском режиме обработки персональных данных применяются все методы и способы защиты информации от НСД, соответствующие информационным системам 3-го класса при однопользовательском режиме обработки.

4.3.2. Для информационных систем 2-го класса при многопользовательском режиме обработки персональных данных и равных правах доступа к ним пользователей применяются все методы и способы защиты информации от НСД, соответствующие информационным системам 3-го класса при многопользовательском режиме обработки персональных данных и равных правах доступа к ним пользователей.

4.3.3. Для информационных систем 2-го класса при многопользовательском режиме обработки персональных данных и разных правах доступа к ним пользователей реализуются все методы и способы защиты информации от НСД, соответствующие информационным системам 3-го класса при многопользовательском режиме обработки персональных данных и разных правах доступа к ним пользователей.

4.3.4. Безопасное межсетевое взаимодействие для информационных систем 2-го класса при их подключении к сетям международного информационного обмена достигается путем применения средств межсетевого экранирования, которые обеспечивают:

фильтрацию на сетевом уровне независимо для каждого сетевого пакета (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов);

фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;

фильтрацию с учетом входного и выходного сетевого интерфейса как средства проверки подлинности сетевых адресов;

фильтрацию с учетом любых значимых полей сетевых пакетов;

регистрацию и учет фильтруемых пакетов (в параметры регистрации включаются адрес, время и результат фильтрации);

идентификацию и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия;

регистрацию входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова (регистрация выхода из системы не проводится в моменты аппаратурного отключения межсетевого экрана);

регистрацию запуска программ и процессов (заданий, задач);

контроль целостности своей программной и информационной частей;

восстановление свойств межсетевого экрана после сбоев и отказов оборудования;

регламентное тестирование реализации правил фильтрации, процессов регистрации, идентификации и аутентификации администратора межсетевого экрана, регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной частей, процедуры восстановления.

4.4. Методы и способы защиты информации от НСД, обеспечивающие функции управления доступом, регистрации и учета, обеспечения целостности и безопасного межсетевого взаимодействия для информационных систем 1-го класса.

4.4.1. Для информационных систем 1-го класса при однопользовательском режиме обработки персональных данных применяются следующие основные методы и способы защиты информации:

а) управление доступом:

идентификация и проверка подлинности пользователя при входе в систему по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов;

б) регистрация и учет:

регистрация входа (выхода) пользователя в систему (из системы) либо загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АИС. В параметрах регистрации указываются дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы, результат попытки входа (успешная или неуспешная);

регистрация выдачи печатных (графических) документов на бумажный носитель. В параметрах регистрации указываются дата и время выдачи (обращения к подсистеме вывода), краткое содержание документа (наименование, вид, код), спецификация устройства выдачи (логическое имя (номер) внешнего устройства);

учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета;

дублирующий учет защищаемых носителей информации;

очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти информационной системы и внешних носителей информации;

в) обеспечение целостности:

обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность программных средств проверяется при загрузке системы по наличию имен (идентификаторов) компонентов средств защиты информации, а целостность программной среды обеспечивается отсутствием в информационной системе средств разработки и отладки программ;

физическая охрана технических средств АИС (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания;

периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей АИС с помощью тест-программ, имитирующих попытки НСД;

наличие средств восстановления системы защиты персональных данных, предусматривающих ведение двух копий программных компонентов средств защиты информации, их периодическое обновление и контроль работоспособности.

4.4.2. Для информационных систем 1-го класса при многопользовательском режиме обработки персональных данных и равных правах доступа к ним пользователей применяются следующие основные методы и способы защиты информации:

а) управление доступом:

идентификация и проверка подлинности пользователя при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов;

идентификация технических средств АИС и каналов связи, внешних устройств информационных систем по их логическим адресам (номерам);

идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;

б) регистрация и учет:

регистрация входа (выхода) пользователя в систему (из системы) либо загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения информационной системы. В параметрах регистрации указываются дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы, результат попытки входа (успешная или неуспешная), идентификатор (код или фамилия) пользователя, предъявленный при попытке доступа;

регистрация выдачи печатных (графических) документов на бумажный носитель. В параметрах регистрации указываются дата и время выдачи (обращения к подсистеме вывода), спецификация устройства выдачи (логическое имя (номер) внешнего устройства), краткое содержание документа (наименование, вид, шифр, код), идентификатор пользователя, запросившего документ;

регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки персональных данных. В параметрах регистрации указываются дата и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор пользователя, запросившего программу (процесс, задание), результат запуска (успешный, неуспешный);

регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются дата и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор пользователя, спецификация защищаемого файла;

регистрация попыток доступа программных средств к дополнительным защищаемым объектам доступа (терминалам, техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей). В параметрах регистрации указываются дата и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная), идентификатор пользователя, спецификация защищаемого объекта (логическое имя (номер));

учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета с отметкой об их выдаче (приеме);

дублирующий учет защищаемых носителей информации;

очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти АИС и внешних носителей информации;

в) обеспечение целостности:

обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность системы защиты персональных данных проверяется при загрузке системы по наличию имен (идентификаторов) ее компонент, а целостность программной среды обеспечивается отсутствием в АИС средств разработки и отладки программ;

физическая охрана технических средств АИС (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания;

периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей АИС с помощью тест-программ, имитирующих попытки НСД;

наличие средств восстановления системы защиты персональных данных, предусматривающих ведение двух копий программных компонентов средств защиты информации, их периодическое обновление и контроль работоспособности.

4.4.3. Для информационных систем 1-го класса при многопользовательском режиме обработки персональных данных и разных правах доступа к ним пользователей применяются следующие основные методы и способы защиты информации:

а) управление доступом:

идентификация и проверка подлинности пользователя при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов;

идентификация терминалов, технических средств, узлов сети, каналов связи, внешних устройств по логическим именам;

идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;

контроль доступа пользователей к защищаемым ресурсам в соответствии с матрицей доступа;

б) регистрация и учет:

регистрация входа (выхода) пользователей в систему (из системы) либо загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения информационной системы. В параметрах регистрации указываются дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы, результат попытки входа (успешная или неу-

спешная), идентификатор (код или фамилия) пользователя, предъявленный при попытке доступа, код или пароль, предъявленный при неуспешной попытке;

регистрация выдачи печатных (графических) документов на бумажный носитель. В параметрах регистрации указываются дата и время выдачи (обращения к подсистеме вывода), спецификация устройства выдачи (логическое имя (номер) внешнего устройства), краткое содержание документа (наименование, вид, шифр, код), идентификатор пользователя, запросившего документ;

регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки персональных данных. В параметрах регистрации указываются дата и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор пользователя, запросившего программу (процесс, задание), результат запуска (успешный, неуспешный);

регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются дата и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор пользователя, спецификация защищаемого файла;

регистрация попыток доступа программных средств к дополнительным защищаемым объектам доступа (терминалам, техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей). В параметрах регистрации указываются дата и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная), идентификатор пользователя, спецификация защищаемого объекта (логическое имя (номер));

учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета с отметкой об их выдаче (приеме);

очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти информационной системы и внешних накопителей;

в) обеспечение целостности:

обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность системы защиты персональных данных проверяется при загрузке системы по контрольным суммам компонентов системы защиты, а целостность программной среды обеспечивается использованием трансляторов

с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения персональных данных;

физическая охрана технических средств информационной системы (устройств и носителей информации), предусматривающая контроль доступа в помещения посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения и хранилище носителей информации;

периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей АИС с помощью тест-программ, имитирующих попытки НСД;

наличие средств восстановления системы защиты персональных данных, предусматривающих ведение двух копий программных компонентов средств защиты информации, их периодическое обновление и контроль работоспособности.

4.4.4. Безопасное межсетевое взаимодействие для информационных систем 1-го класса при их подключении к сетям международного информационного обмена достигается путем применения средств межсетевого экранирования, которые обеспечивают выполнение следующих функций:

фильтрацию на сетевом уровне для каждого сетевого пакета независимо (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов);

фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;

фильтрацию с учетом входного и выходного сетевого интерфейса как средства проверки подлинности сетевых адресов;

фильтрацию с учетом любых значимых полей сетевых пакетов;

фильтрацию на транспортном уровне запросов на установление виртуальных соединений с учетом транспортных адресов отправителя и получателя;

фильтрацию на прикладном уровне запросов к прикладным сервисам с учетом прикладных адресов отправителя и получателя;

фильтрацию с учетом даты и времени;

аутентификацию входящих и исходящих запросов методами, устойчивыми к пассивному и (или) активному прослушиванию сети;

регистрацию и учет фильтруемых пакетов (в параметры регистрации включаются адрес, время и результат фильтрации);

регистрацию и учет запросов на установление виртуальных соединений;

локальную сигнализацию попыток нарушения правил фильтрации;

идентификацию и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия;

предотвращение доступа неидентифицированного пользователя или пользователя, подлинность идентификации которого при аутентификации не подтвердилась;

идентификацию и аутентификацию администратора межсетевого экрана при его удаленных запросах методами, устойчивыми к пассивному и активному перехвату информации;

регистрацию входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова (регистрация выхода из системы не проводится в моменты аппаратурного отключения межсетевого экрана);

регистрацию запуска программ и процессов (заданий, задач);

регистрацию действия администратора межсетевого экрана по изменению правил фильтрации;

возможность дистанционного управления своими компонентами, в том числе возможность конфигурирования фильтров, проверки взаимной согласованности всех фильтров, анализа регистрационной информации;

контроль целостности своей программной и информационной частей;

контроль целостности программной и информационной частей межсетевого экрана по контрольным суммам;

восстановление свойств межсетевого экрана после сбоев и отказов оборудования;

регламентное тестирование реализации правил фильтрации, процессов регистрации, идентификации и аутентификации запросов, идентификации и аутентификации администратора межсетевого экрана, регистрации действий администратора межсетевого экрана, контроля за целостностью программной и информационной части, процедуры восстановления.

4.5. Анализ защищенности проводится для распределенных АИС и информационных систем, подключенных к сетям международного информационного обмена, путем использования в составе АИС программных или программно-аппаратных средств (систем) анализа защищенности.

Средства (системы) анализа защищенности должны обеспечивать возможность выявления уязвимостей, связанных с ошибками в конфигурации программного обеспечения АИС, которые могут быть использованы нарушителем для реализации атаки на систему.

4.6. Обнаружение вторжений проводится для информационных систем, подключенных к сетям международного информационного обмена, путем использования в составе АИС программных или программно-аппаратных средств (систем) обнаружения вторжений.

4.7. Для информационных систем 1-го класса применяется программное обеспечение средств защиты информации, соответствующее четвертому уровню контроля отсутствия недекларированных возможностей.

СПИСОК ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

Нормативные правовые акты Российской Федерации

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) // Российская газета. 1993. № 237. 25 декабря.

2. Федеральный конституционный закон от 28.06.2004 № 5-ФКЗ «О референдуме Российской Федерации» // Парламентская газета. № 117. 30.06.2004.

3. Федеральный конституционный закон от 25.12.2000 № 2-ФКЗ «О Государственном гербе Российской Федерации» // Собрание законодательства Российской Федерации. 2000. № 52 (Ч. 1). Ст. 5021.

4. Федеральный конституционный закон от 17.12.1997 № 2-ФКЗ «О Правительстве Российской Федерации // Собрание законодательства Российской Федерации. 1997. № 51. Ст. 5712.

5. Гражданский кодекс Российской Федерации (Ч. 4) от 18.12.2006 № 230-ФЗ // Собрание законодательства Российской Федерации. 2006. № 52 (Ч. 1). Ст. 5496.

6. Гражданский процессуальный кодекс Российской Федерации от 14.11.2002 № 138-ФЗ // Собрание законодательства Российской Федерации. 2002. № 46. Ст. 4532.

7. Арбитражный процессуальный кодекс Российской Федерации от 24.07.2002 № 95-ФЗ // Собрание законодательства Российской Федерации. 2002. № 30. Ст. 3012.

8. Трудовой кодекс Российской Федерации от 30.12.2001 г. № 197-ФЗ // Собрание законодательства Российской Федерации. 2002, № 1 (Ч. 1), Ст. 3.

9. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ // Собрание законодательства Российской Федерации. 2002. № 1 (Ч. 1). Ст. 1.

10. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ // Собрание законодательства Российской Федерации. 2001. № 52 (Ч. 1). Ст. 4921.

11. Гражданский кодекс Российской Федерации (Ч. 3) от 26.11.2001 № 146-ФЗ // Собрание законодательства Российской Федерации. 2001. № 49. Ст. 4552.

12. Налоговый кодекс Российской Федерации от 31.07.1998 № 146-ФЗ // Российская газета. 1998. № 148–149.

13. Уголовно-исполнительный кодекс Российской Федерации от 08.01.1997 № 1-ФЗ // Собрание законодательства Российской Федерации. 1997. № 2. Ст. 198.

14. Уголовный кодекс Российской Федерации от 13.07.1996 № 63-ФЗ // Собрание законодательства Российской Федерации. 1996. № 25. Ст. 2954.

15. Гражданский кодекс Российской Федерации (Ч. 2) от 26.01.1996 № 14-ФЗ // Собрание законодательства Российской Федерации. 1996. № 5. Ст. 410.

16. Семейный кодекс Российской Федерации от 29.12.1995 № 223-ФЗ // Собрание законодательства Российской Федерации. 1996. № 1. Ст. 16.

17. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ // Собрание законодательства Российской Федерации. 1994. № 32. Ст. 3301.

18. Основы законодательства Российской Федерации о культуре // Российская газета. № 248. 17.11.1992.

19. Основы законодательства Российской Федерации об охране здоровья граждан от 22.07.1993 № 5487-1 // Ведомости Съезда народных депутатов РСФСР и Верховного Совета РСФСР. 1993. № 33. Ст. 1318.

20. Основы законодательства Российской Федерации о нотариате от 11.02.1993 № 4462-1 // Ведомости Съезда народных депутатов РСФСР и Верховного Совета РСФСР.1993. № 10. Ст. 357.

21. Федеральный закон от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» // Собрание законодательства Российской Федерации. 2009. № 7. Ст. 776.

22. Федеральный закон 27.07.2006 № 152-ФЗ «О персональных данных» // Российская газета. 2006. № 165.

23. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Российская газета. 2006. № 165.

24. Федеральный закон от 06.03.2006 № 35-ФЗ «О противодействии терроризму» // Российская газета. 2001. № 151–152.

25. Федеральный закон от 21.07.2005 № 94-ФЗ «О размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд» // Собрание законодательства Российской Федерации. 2005. № 30 (Ч. 1). Ст. 3105.

26. Федеральный закон от 02.12.2004 № 218-ФЗ «О кредитных историях» // Собрание законодательства Российской Федерации. 2005. № 1 (Ч. 1). Ст. 44.

27. Федеральный закон от 22.10.2004 № 125-ФЗ «Об архивном деле в Российской Федерации» (ред. 13.05.2008) // Парламентская газета. 2004. № 201.

28. Федеральный закон от 20.08.2004 № 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства» // Собрание законодательства Российской Федерации. 2004. № 34. Ст. 3534.

29. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» (ред. 24.07.2007) // Парламентская газета. 2004. № 144.

30. Федеральный закон от 27.06.2004 № 79-ФЗ «О государственной гражданской службе Российской Федерации» // Парламентская газета. 2004. № 140–141.

31. Федеральный закон от 23.12.2003 № 177-ФЗ «О страховании вкладов физических лиц в банках Российской Федерации» // Российская газета. 2003. № 261.

32. Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» // Российская газета. 2003. № 135.

33. Федеральный закон 27.12.2002 № 184-ФЗ «О техническом регулировании» // Собрание законодательства Российской Федерации. 2002. № 52 (Ч. 1). Ст. 5140.

34. Федеральный закон от 25.07.2002 № 114-ФЗ «О противодействии экстремистской деятельности» // Собрание законодательства Российской Федерации. 2002. № 30. Ст. 3031.

35. Федеральный закон от 12.09.2002 № 67-ФЗ «Об основных гарантиях избирательных прав и прав на участие в референдуме граждан Российской Федерации» // Парламентская газета. 2002. № 110-111.

36. Федеральный закон от 31.05.2002 № 63-ФЗ «Об адвокатской деятельности и адвокатуре Российской Федерации» // Парламентская газета. 2002. № 104.

37. Федеральный закон от 10.01.2002 № 1-ФЗ «Об электронной цифровой подписи» // Российская газета. 2002. № 6.

38. Федеральный закон от 08.08.2001 № 128-ФЗ «О лицензировании отдельных видов деятельности» // Российская газета. 2001. № 153-154.

39. Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем» // Российская газета. 2001. № 151-152.

40. Федеральный закон от 07.08.2001 № 119-ФЗ (ред. от 01.07.2010) «Об аудиторской деятельности» // Российская газета. 2008. № 267.

41. Федеральный закон от 11.07.2001 № 95-ФЗ «О политических партиях» // Российская газета. 2001. № 133.

42. Федеральный закон от 17.07.1999 № 176-ФЗ «О почтовой связи» // Собрание законодательства Российской Федерации. 1999. № 29. Ст. 3697.

43. Федеральный закон от 15.11.1997 № 143-ФЗ «Об актах гражданского состояния» // Российская газета. 1997. № 224.

44. Федеральный закон от 26.09.1997 № 125-ФЗ «О свободе совести и о религиозных объединениях» // Собрание законодательства Российской Федерации. 1997. № 39. Ст. 4465.

45. Федеральный закон от 15.08.1996 № 114-ФЗ «О порядке выезда из Российской Федерации и въезда в Российскую Федерацию» // Собрание законодательства Российской Федерации. 1996. № 34. Ст. 4029.

46. Федеральный закон от 27.05.1996 № 57-ФЗ «О государственной охране» // Собрание законодательства Российской Федерации. 1996. № 22. Ст. 2594.

47. Федеральный закон от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности» // Собрание законодательства Российской Федерации. 1995. № 33. Ст. 3349.

48. Федеральный закон от 03.04.1995 № 40-ФЗ «О федеральной службе безопасности» // Собрание законодательства Российской Федерации. 1995. № 15. Ст. 1269.

49. Федеральный закон от 21.12.1994 № 68-ФЗ «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера» // Российская газета. 1994. № 250.

50. Закон Российской Федерации от 21.07.1993 № 5485-1 «О государственной тайне» // Собрание законодательства Российской Федерации. 1997. № 41. С. 8220–8235.

51. Закон Российской Федерации от 11.03.1992 № 2487-1 «О частной детективной и охранной деятельности в Российской Федерации» // Ведомости Съезда народных депутатов РСФСР и Верховного Совета РСФСР. 1992. № 17. Ст. 888.

52. Закон Российской Федерации от 05.03.1992 № 2446-1 «О безопасности» // Ведомости Съезда народных депутатов РСФСР и Верховного Совета РСФСР. 1992. № 15. Ст. 769.

53. Закон Российской Федерации от 27.12.1991 № 2124-I «О средствах массовой информации» // Российская газета. 1992. № 32.

54. Закон РСФСР 25.12.1990 № 445-1 «О предприятиях и предпринимательской деятельности» // Ведомости Съезда народных депутатов РСФСР и Верховного Совета РСФСР. 1990. № 30. Ст. 418 (утратил силу).

55. Закон РСФСР от 02.12.1990 № 395-1 «О банках и банковской деятельности в РСФСР» // Собрание законодательства Российской Федерации. 1996. № 6. Ст. 492.

56. Закон СССР от 04.06.1990 № 1529-1 «О предприятиях в СССР» // Справочная правовая система «Консультант Плюс» (утратил силу).

57. Указ Президента Российской Федерации от 12.05.2009 № 537 «О стратегии национальной безопасности до 2020 года» // Собрание законодательства Российской Федерации. 2009. № 20. Ст. 2444.

58. Указ Президента Российской Федерации от 19.05.2008 № 815 «О мерах по противодействию коррупции» // Справочная правовая система «Консультант Плюс».

59. Указ Президента Российской Федерации 17.03.2008 № 611 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» // Собрание законодательства Российской Федерации. 2008. № 12. Ст. 1110.

60. Указ Президента Российской Федерации от 15.02.2006 № 116 «О мерах по противодействию терроризму» // Российская газета. 2006. № 34.

61. Указ Президента Российской Федерации от 30.05.2005 № 609 «Об утверждении Положения о персональных данных государственного гражданского служащего и ведение его личного дела» // Собрание законодательства Российской Федерации. 2005. № 23. Ст. 2242.

62. Указ Президента Российской Федерации от 22.03.2005 № 330 «О внесении изменения в Указ Президента Российской Федерации от 16.08.2004 № 1085» // Справочная правовая система «Консультант Плюс».

63. Указ Президента Российской Федерации от 16.08.2004 № 1085 «Вопросы Федеральной службы по техническому и экспертному

контролю» // Собрание законодательства Российской Федерации. 2004. № 34. Ст. 3541.

64. Указ Президента Российской Федерации от 07.08.2004 № 1013 «Вопросы Федеральной службы охраны Российской Федерации» // Собрание законодательства Российской Федерации. 2004. № 32. Ст. 3314.

65. Указ Президента Российской Федерации от 11.08.2004 № 960 «Вопросы Федеральной службы безопасности Российской Федерации» // Российская газета. 2003. № 161.

66. Указ Президента Российской Федерации от 15.03.2000 № 511 «О классификаторе правовых актов» // Собрание законодательства Российской Федерации. 2000. № 12. Ст. 1260.

67. Указ Президента Российской Федерации от 10.01.2000 № 24 «О Концепции национальной безопасности» // Собрание законодательства Российской Федерации. 2008. № 5. Ст. 434 (утратил силу).

68. Указ Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера» // Собрание законодательства Российской Федерации. 1997. № 10. Ст. 1127.

69. Указ Президента Российской Федерации от 09.01.1996 № 21 «О мерах по упорядочению разработки, производства, реализации, приобретения в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы, а также использования специальных технических средств, предназначенных для негласного получения информации» // Собрание законодательства Российской Федерации. 1996. № 3. Ст. 153.

70. Указ Президента Российской Федерации от 03.04.1995 № 334 «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставление услуг в области шифрования информации» // Российская газета. 1995. № 68.

71. Доктрина информационной безопасности России // Российская газета. 2000. № 187.

72. Постановление Правительства Российской Федерации от 06.02.2010 № 63 «Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне» // Собрание законодательства Российской Федерации. 2010. № 7. Ст. 762.

73. Постановление Правительства Российской Федерации от 24.11.2009 № 953 «Об обеспечении доступа к информации о деятельности Правительства Российской Федерации и федеральных органов

исполнительной власти» // Собрание законодательства Российской Федерации. 2009. № 48. Ст. 5832.

74. Постановление Правительства Российской Федерации от 22.09.2009 № 754 «Об утверждении положения о системе межведомственного электронного документооборота» // Собрание законодательства Российской Федерации. 2009. № 39. Ст. 4614.

75. Постановление Правительства Российской Федерации от 10.09.2009 № 723 «О порядке ввода в эксплуатацию отдельных государственных информационных систем» // Собрание законодательства Российской Федерации. 2009. № 37. Ст. 4416.

76. Постановление Правительства Российской Федерации от 15.07.2009 № 477 «Об утверждении Правил делопроизводства в федеральных органах исполнительной власти» // Собрание законодательства Российской Федерации. 2009. № 25. Ст. 3060.

77. Постановление Правительства Российской Федерации № 697 от 08.09.2010 «О Единой системе межведомственного электронного взаимодействия» // Собрание законодательства Российской Федерации. 20.09.2010. № 38. Ст. 483.

78. Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» // Собрание законодательства Российской Федерации. 2008. № 38. Ст. 4320.

79. Постановление Правительства Российской Федерации от 06.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных вне информационных систем» // Российская газета. 2008. № 148.

80. Постановление Правительства Российской Федерации от 29.12.2007 № 957 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами» // Собрание законодательства Российской Федерации. 2008. № 2. Ст. 86.

81. Постановление Правительства Российской Федерации от 25.12.2007 № 931 «О некоторых мерах по обеспечению информационного взаимодействия государственных органов и органов местного самоуправления при оказании государственных услуг гражданам и организациям» // Справочная правовая система «Консультант Плюс».

82. Постановление Правительства Российской Федерации от 17.11.2007 № 781 «Об утверждении Положения об обеспечении без-

опасности персональных данных при их обработке в информационных системах персональных данных» // Российская газета. 2007. № 260.

83. Постановление Правительства Российской Федерации от 22.10.2007 № 689 «Об утверждении Положения о лицензировании деятельности по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)» // Собрание законодательства Российской Федерации. 2007. № 44. Ст. 5363.

84. Постановление Правительства Российской Федерации от 10.09.2007 № 575 «Об утверждении Правил оказания телематических услуг связи» // Собрание законодательства Российской Федерации. 2007. № 38. Ст. 4552.

85. Постановление Правительства Российской Федерации от 16.01.2007 № 15 «О лицензировании деятельности по изготовлению защищенной от подделок полиграфической продукции, в том числе бланков ценных бумаг, а также торговли указанной продукцией» // Собрание законодательства Российской Федерации. 2007. № 4. Ст. 520.

86. Постановление Правительства Российской Федерации от 31.08.2006 № 532 «О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации» // Собрание законодательства Российской Федерации. 2006. № 36. Ст. 3837.

87. Постановление Правительства Российской Федерации от 15.08.2006 № 504. «О лицензировании деятельности по технической защите конфиденциальной информации» // Собрание законодательства Российской Федерации. 2006. № 34. Ст. 3691.

88. Постановление Правительства Российской Федерации от 23.01.2006 № 32 «Об утверждении правил оказания услуг связи по передаче данных» // Собрание законодательства Российской Федерации». 2006. № 5. Ст. 553.

89. Постановление Правительства Российской Федерации от 08.12.2005 № 24 «О стандартизации оборонной продукции (работ, услуг), продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации информации ограниченного доступа, и продукции (работ, услуг) сведения о которой составляют государственную тайну» // Собрание законодательства Российской Федерации. 2009. № 43. Ст. 5072.

90. Постановление Правительства Российской Федерации от 28.07.2005 № 452 «О Типовом регламенте внутренней организации федеральных органов исполнительной власти». // Собрание законодательства Российской Федерации. 2005. № 31. Ст. 3233.

91. Постановление Правительства Российской Федерации от 15.04.2005 № 221 «Об утверждении Правил оказания услуг почтовой связи» // Собрание законодательства Российской Федерации. 2005. № 17. Ст. 1556.

92. Постановление Правительства Российской Федерации от 21.01.2004 № 24 «Об утверждении стандартов раскрытия информации субъектами оптового и розничных рынков электрической энергии» // Собрание законодательства Российской Федерации. 2004. № 4. Ст. 282.

93. Постановление Правительства Российской Федерации от 10.11.2003 № 677 «Об общероссийских классификаторах технико-экономической и социальной информации в социально-экономической области» // Собрание законодательства Российской Федерации. 2003. № 46 (Ч. 2). Ст. 4472.

94. Постановление Правительства Российской Федерации от 25.09.2003 № 594 «Об опубликовании национальных стандартов и общероссийских классификаторов технико-экономической и социальной информации» // Собрание законодательства Российской Федерации. 2003. № 39. Ст. 3773.

95. Постановление Правительства Российской Федерации от 12.02.2003 № 98 «Об обеспечении доступа к информации о деятельности Правительства Российской Федерации и федеральных органов исполнительной власти» // Собрание законодательства Российской Федерации. 2009. № 48. Ст. 5832.

96. Постановление Правительства Российской Федерации от 15.07.2002 № 526 «Об утверждении Положения о лицензировании деятельности по разработке, производству, реализации и приобретению в целях продажи специальных технических средств, предназначенных для негласного получения информации, индивидуальными предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность» // Собрание законодательства Российской Федерации. 2002. № 29. Ст. 2965.

97. Постановление Правительства Российской Федерации от 08.09.1999 № 1016 «О подписании Соглашения между Правительством Российской Федерации и Правительством Итальянской Республики о взаимном обеспечении сохранности засекреченных сведений» // Собрание законодательства Российской Федерации. 1999. № 37. Ст. 4520.

98. Постановление Правительства Российской Федерации от 22.08.1998 № 1003 «Об утверждении Положения о порядке допуска лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов к государственной тайне» // Собрание законодательства Российской Федерации. 1998. № 35. Ст. 4407.

99. Постановление Правительства Российской Федерации от 29.07.1998 № 854 «О внесении дополнения в Положение о лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны» // Российская газета. 1998. № 148–149.

100. Постановление Правительства Российской Федерации от 02.08.1997 № 973 «Об утверждении Положения о подготовке к передаче сведений, составляющих государственную тайну, другим государствам» // Собрание законодательства Российской Федерации. 1997. № 32. Ст. 3786.

101. Постановление Правительства Российской Федерации от 03.03.1997 № 242 «О назначении российского органа по защите информации, которой обмениваются Российская Федерация и Организация Североатлантического договора, и создании Центральной службы регистрации и контроля документов, которыми обмениваются Российская Федерация и Организация Североатлантического договора» // Собрание законодательства Российской Федерации. 1997. № 10. Ст. 1182.

102. Постановление Правительства Российской Федерации от 28.02.1996 № 226 «Об утверждении временного положения о государственном учете и регистрации баз и банков данных» // Справочная правовая система «Консультант Плюс» (утратил силу).

103. Постановление Правительства Российской Федерации от 27.12.1995 № 1268 «Об упорядочении изготовления, использования, хранения и уничтожения печатей и бланков с воспроизведением Государственного герба Российской Федерации» // Собрание законодательства Российской Федерации. 1996. № 2. Ст. 123.

104. Постановление Правительства Российской Федерации от 23.07.2005 № 443 «Об утверждении Правил разработки перечня сведений, отнесенных к государственной тайне» // Собрание законодательства Российской Федерации. 2005. № 31.

105. Постановление Правительства Российской Федерации от 28.10.1995 № 1050 «Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне» // Собрание законодательства Российской Федерации. 2010. № 7. Ст. 762.

106. Постановление Правительства Российской Федерации от 04.09.1995 № 879 «Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности» // Собрание законодательства Российской Федерации. 1995. № 37. Ст. 3619.

107. Постановление Правительства Российской Федерации от 26.06.1995 № 608 «О сертификации средств защиты информации» // Российская газета. 1995. № 145.

108. Постановление Правительства Российской Федерации от 20.02.1995 № 170 «Об установлении порядка рассекречивания и продления засекречивания архивных документов Правительства СССР» // Собрание законодательства Российской Федерации. 1995. № 9. Ст. 762.

109. Постановление Правительства Российской Федерации от 15.04.1995 № 333 «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» // Собрание законодательства Российской Федерации. 1995. № 17. Ст. 1540.

110. Постановление Правительства Российской Федерации от 03.11.1994 № 1233 «Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти» // Собрание законодательства Российской Федерации. 2005. № 30 (Ч. 2). Ст. 3165.

111. Постановление Правительства Российской Федерации от 12.02.1994 № 100 «Об организации работ по стандартизации, обеспечению единства измерений, сертификации продукции и услуг» // Собрание актов Президента и Правительства Российской Федерации. 1994. № 8. Ст. 598.

112. Постановление Правительства Российской Федерации от 14.08.1992 № 587 «Вопросы частной детективной и охранной деятельности» // Собрание законодательства Российской Федерации. 1994. № 9. Ст. 1013.

113. Распоряжение Правительства Российской Федерации от 25.08.2008 № 1243-р «Об утверждении перечня технологий, имеющих важное социально-экономическое значение или важное значение для обороны страны и безопасности государства (критические технологии)» // Собрание законодательства Российской Федерации. 2008 № 35. Ст. 4068.

114. Распоряжение Правительства Российской Федерации от 28.02.1996 № 286-р «О разработке развернутых перечней сведений, подлежащих засекречиванию» // Справочная правовая система «Консультант Плюс».

115. Распоряжение Правительства Российской Федерации от 21.03.1994 № 358-р «О включении в учредительные документы юридических лиц положения, касающегося обеспечения учета и сохранности документов по личному составу» // Справочная правовая система «Консультант Плюс».

116. Концепция формирования в Российской Федерации электронного правительства до 2010 года / Одобрена Распоряжением Правительства Российской Федерации от 06.05.2008 № 632-р // Собрание законодательства Российской Федерации. 2008. № 20. Ст. 2372.

117. Технические требования к организации взаимодействия системы межведомственного электронного документооборота с системами электронного документооборота федеральных органов исполнительной власти / Утверждены Распоряжением Правительства Российской Федерации от 02.10.2009 № 1403-р // Справочная правовая система «Консультант Плюс».

118. Приказ Федеральной службы по техническому и экспортному контролю от 05.02.2010 № 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных» // Российская газета. 2010. № 46.

119. Приказ Федеральной службы безопасности Российской Федерации от 01.04.2009 № 123 «Об утверждении Административного регламента Федеральной службы безопасности Российской Федерации по исполнению государственной функции по лицензированию деятельности по разработке и (или) производству средств защиты конфиденциальной информации» // Справочная правовая система «Консультант Плюс».

120. Приказ Федеральной службы безопасности Российской Федерации от 18.09.2008 № 464 «Об утверждении Регламента Федеральной службы безопасности Российской Федерации» // Справочная правовая система «Консультант Плюс».

121. Приказ Роскомсвязьнадзора от 17.07.2008 № 08 «Об утверждении образца формы уведомления об обработке персональных данных» // Справочная правовая система «Консультант Плюс».

122. Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России), Федеральной службы безопасности Российской Федерации (ФСБ России), Министерства информационных технологий и связи Российской Федерации (Мининформсвязи России) от 13.02.2008 № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных» // Российская газета. 2008. № 80.

123. Приказ Министерства информационных технологий и связи Российской Федерации от 09.01.2008 № 1 «Об утверждении требований по защите сетей связи от несанкционированного доступа к ним и передаваемой посредством их информации» // Бюллетень нормативных актов федеральных органов исполнительной власти. 2008. № 9.

124. Приказ Федеральной службы по техническому и экспортному контролю от 28.08.2007 № 182 «Об утверждении административного регламента федеральной службы по техническому и экспортному контролю по исполнению государственной функции по лицензированию деятельности по разработке и (или) производству средств защиты конфиденциальной информации» // Бюллетень нормативных актов федеральных органов исполнительной власти. 2007. № 45.

125. Приказ Федеральной службы по техническому и экспортному контролю от 28.08.2007 № 181 «Об утверждении административного регламента федеральной службы по техническому и экспортному контролю по исполнению государственной функции по лицензированию деятельности по технической защите конфиденциальной информации» // Бюллетень нормативных актов федеральных органов исполнительной власти. 2007. № 45.

126. Приказ Министерства культуры и массовых коммуникаций Российской Федерации от 31.07.2007 № 1182 «Об утверждении Перечня типовых архивных документов, образующихся в научно-технической и производственной деятельности организаций, со сроками хранения» // Справочная правовая система «Консультант Плюс».

127. Приказ Министерства информационных технологий и связи Российской Федерации от 19.03.2007 № 36 «Об утверждении перечня представляемых сведений об использовании информационных технологий в деятельности федеральных органов государственной вла-

сти и порядка представления их в электронном виде» // Бюллетень нормативных актов федеральных органов исполнительной власти. 2007. № 20.

128. Приказ Министерства культуры и массовых коммуникаций Российской Федерации от 18.01.2007 № 19 «Об утверждении правил организации хранения, комплектования, учета и использования документов Архивного фонда Российской Федерации и других архивных документов в государственных и муниципальных архивах, музеях и библиотеках, организациях Российской академии наук» // Бюллетень нормативных актов федеральных органов исполнительной власти. 2007. № 20.

129. Приказ Федеральной службы безопасности Российской Федерации от 09.02.2005 № 66 «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (положение ПКЗ-2005)» // Бюллетень нормативных актов федеральных органов исполнительной власти. 2005. № 11.

130. Приказ Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 № 152 «Об утверждении инструкции 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» // «Бюллетень нормативных актов федеральных органов исполнительной власти». 2001. № 34.

131. Положение о правилах обмена электронными документами между Банком России, кредитными организациями (филиалами) и другими клиентами Банка России при осуществлении расчетов через расчетную сеть Банка России // Вестник Банка России. 2000. № 22.

132. Приказ Федеральной службы безопасности Российской Федерации от 04.07.1998 № 282 «Об утверждении Инструкции о порядке оформления допуска к особой важности, совершенно секретным и секретным сведениям и доступа к государственной тайне в органах Федеральной» службы безопасности // Справочная правовая система «Консультант Плюс».

133. Квалификационный справочник должностей руководителей, специалистов и других служащих / Утвержден Постановлением Минтруда России от 21.08.1998. № 37.

134. Решение Гостехкомиссии России и Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 27.04.1994 № 10 «Об утверждении Положения о государственном лицензировании деятельности в области защиты информации» // Справочная правовая система «Консультант Плюс».

135. Положение по аттестации объектов информатизации по требованиям безопасности информации / Утверждено председателем Гостехкомиссии России от 25.11.1994 // Справочная правовая система «Консультант Плюс».

136. Положение об аккредитации испытательных лабораторий и органов по сертификации средств защиты информации по требованиям безопасности информации / Решение председателя Гостехкомиссии России от 25.11.1994 // Справочная правовая система «Консультант Плюс».

137. Постановление Правительства Москвы от 10.04.2007 № 249-ПП «Об утверждении порядка работы органов исполнительной власти города Москвы, государственных учреждений и государственных унитарных предприятий города Москвы с электронными документами, подписанными электронной цифровой подписью» // Справочная правовая система «Консультант Плюс».

138. Постановление Правительства Москвы от 19.12.2006 № 997-ПП «Об утверждении порядка использования электронной цифровой подписи органами исполнительной власти города Москвы и государственными заказчиками при размещении государственного заказа города Москвы» // Справочная правовая система «Консультант Плюс».

139. Постановление Правительства Москвы от 30.05.2006 № 352-ПП «Об утверждении Регламента организации работы органов исполнительной власти, государственных учреждений и государственных унитарных предприятий города Москвы в режиме «одного окна» // Справочная правовая система «Консультант Плюс».

140. Постановление Правительства Москвы от 21.02.2006 № 112-ПП «Регламент Правительства Москвы» // Справочная правовая система «Консультант Плюс».

141. Постановление Правительства Москвы от 11.05.2004 № 299-ПП «Об утверждении Положения о порядке организации выдачи и отзыва сертификатов ключей электронных цифровых подписей уполномоченных лиц органов исполнительной власти города Москвы» // Справочная правовая система «Консультант Плюс».

Стандарты и иные нормативные и методические документы

142. ГОСТ Р ИСО 15489-1–2007. Система стандартов по информации, библиотечному и издательскому делу. Управление документами. Общие требования.

143. ГОСТ 2.601–2006. Единая система конструкторской документации. Эксплутационные документы.

144. ГОСТ 2.610–2006. Единая система конструкторской документации. Правила выполнения эксплуатационных документов.

145. ГОСТ 2.051–2006. Единая система конструкторской документации. Электронные документы. Общие положения.

146. ГОСТ Р 52551–2006. Системы охраны и безопасности. Термины и определения.

147. ГОСТ Р ИСО/МЭК 17799–2005. Информационная технология. Практические правила управления информационной безопасностью.

148. ГОСТ Р 52294–2004. Информационная технология. Управление организацией. Электронный регламент административной и служебной деятельности. Основные положения.

149. ГОСТ Р 52292–2004. Информационная технология. Электронный обмен информацией. Термины и определения.

150. ГОСТ Р 52069.0–2003. Защита информации. Система стандартов. Основные положения.

151. ГОСТ Р 6.30–2003. Унифицированные системы документации. Унифицированная система организационно-распорядительной документации. Требования к оформлению документов.

152. ГОСТ Р ИСО/МЭК 15408-1–2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 1. Введение и общая модель; Ч. 2. Функциональные требования безопасности; Ч. 3. Требования доверия к безопасности.

153. ГОСТ Р ИСО 9000–2001. Системы менеджмента качества. Основные положения и словарь.

154. ГОСТ Р 51511–2001. Печати с воспроизведением Государственного герба Российской Федерации. Форма, размеры и технические требования.

155. ГОСТ Р ИСО/МЭК 12119–2000. Информационная технология. Пакеты программ. Требования к качеству и тестирование.

156. ГОСТ Р 51583–2000. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения.

157. ГОСТ Р ИСО/МЭК 12207–99. Информационная технология. Процессы жизненного цикла программных средств.

158. ГОСТ Р ИСО 7498–2–99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Ч. 2. Архитектура защиты информации.

159. ГОСТ Р ИСО 7498–1–99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Ч. 1. Базовая модель.

160. ГОСТ Р 51275–99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

161. ГОСТ Р 51320–99. Совместимость технических средств электромагнитная. Приборы для измерения радиопомех. Технические требования и методы испытаний.

162. ГОСТ Р 51319–99. Совместимость технических средств электромагнитная. Радиопомехи индустриальные. Методы испытаний технических средств – источников индустриальных радиопомех.

163. ГОСТ Р 51141–98. Делопроизводство и архивное дело. Термины и определения.

164. ГОСТ Р 51170–98. Качество служебной информации. Термины и определения.

165. ГОСТ Р 51188–98. Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство.

166. ГОСТ Р 51241–98. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний.

167. ГОСТ 34.320–96. Международный стандарт. Информационные технологии. Система стандартов по базам данных. Концепции и терминология для концептуальной схемы и информационной базы.

168. ГОСТ Р 50923–96. Рабочее место оператора. Общие эргономические требования и требования к производственной среде. Методы измерения.

169. ГОСТ Р 50949–96. Средства отображения информации индивидуального пользования. Методы измерений и оценки эргономических параметров и параметров безопасности.

170. ГОСТ Р 50948–96. Средства отображения информации индивидуального пользования. Общие эргономические требования и требования безопасности.

171. ГОСТ 34.321–96. Информационные технологии. Система стандартов по базам данных. Эталонная модель управления данными.

172. ГОСТ Р 50922–96. Защита информации. Основные термины и определения.

173. ГОСТ 2.601–95. Единая система конструкторской документации. Эксплуатационные документы.

174. ГОСТ 2.114–95. Единая система конструкторской документации. Технические условия.

175. ГОСТ Р 50739–95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.

176. ГОСТ Р 34.10–94. Информационная технология. Криптографическая защита информации. процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма.

177. ГОСТ Р 50628–93. Совместимость электромагнитная машин электронных вычислительных персональных. Устойчивость к электромагнитным помехам. Технические требования и методы испытаний.

178. ГОСТ 13661–92. Совместимость технических средств электромагнитная. Пассивные помехоподавляющие фильтры и элементы. Методы измерения вносимого затухания.

179. ГОСТ 29216–91. Совместимость технических средств электромагнитная. Радиопомехи индустриальные от оборудования информационной техники. Нормы и методы испытаний.

180. ГОСТ 34.601–90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадия создания.

181. ГОСТ 34.003–90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения.

182. ГОСТ Р ИСО/МЭК 9126–90. Информационная технология. Оценка программной продукции. Характеристика качества и руководства по их применению.

183. ГОСТ 15971–90. Системы обработки информации. Термины и определения.

184. РД Гостехкомиссии России. Безопасность информационных технологий. Руководство по формированию семейств профилей защиты.

185. РД Гостехкомиссии России. Безопасность информационных технологий. Руководство по регистрации профилей защиты.

186. РД Гостехкомиссии России. Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности.

187. РД Гостехкомиссии России. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий.

188. Временная методика оценки защищенности речевой конфиденциальной информации от утечки по акустическому и виброакустическому каналам. Гостехкомиссия России. 2001.

189. 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. Гостехкомиссия России. 2001.

190. Временная методика оценки защищенности основных технических средств и систем, предназначенных для обработки, хранения и (или) передачи по линиям связи конфиденциальной информации. Гостехкомиссия России. 2001.

191. РД Гостехкомиссии России. Специальные требования и рекомендации по технической защите конфиденциальной информации.

192. РД Гостехкомиссии России. Средства защиты информации. Специальные общие технические требования, предъявляемые к сетевым помехоподавляющим фильтрам.

193. РД Гостехкомиссии России. Защита от несанкционированного доступа к информации. Ч. 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей.

194. РД Гостехкомиссии России. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники.

195. РД Гостехкомиссии России. Защита от несанкционированного доступа к информации. Ч. 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей.

196. РД Гостехкомиссии России. Средства антивирусной защиты. Показатели защищенности и требования по защите от вирусов.

197. РД Гостехкомиссии России. Защита информации. Специальные защитные знаки. Классификация и общие требования.

198. РД Гостехкомиссии России. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации.

199. РД Гостехкомиссии России. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники.

200. РД Гостехкомиссии России. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.

201. РД Гостехкомиссии России. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации.

202. РД Гостехкомиссии России. Защита от несанкционированного доступа к информации. Термины и определения.

203. РД Госстандарта 50-34.698–90. Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов.

204. РД Госстандарта 50-680–89. Методические указания. Автоматизированные системы. Основные положения.

205. РД Госстандарта 50-682–89. Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Общие положения.

206. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Федеральная служба по техническому и экспортному контролю. 2008 / Пометка «для служебного пользования» снята Решением ФСТЭК России от 16.11.2009.

207. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Литература

208. *Алексеенко В.Н., Древс Ю.Г.* Основы построения систем защиты производственных предприятий и банков / В.Н. Алексеенко, Ю.Г. Древс. – М.: МИФИ, 1996.

209. *Алексенцев А.И.* Конфиденциальное делопроизводство / А.И. Алексенцев. – М.: Бизнес-школа «Интел-Синтез», 2001.

210. *Бачило И.Л.* Информационное право: учебник для вузов / И.Л. Бачило. – М.: Высшее образование, Юрайт, 2009.

211. *Бачило И.Л.* Информационное право: учебник / Бачило И.Л., Лопатин В.Н., Федотов М.А.; под ред. акад. РАН Б.Н. Топорнина. – СПб.: Изд-во «Юридический центр Пресс», 2001.

212. *Бачило И.Л., Семилетов С.И.* Комментарий к Федеральному закону от 10.01.2002 № 1–ФЗ «Об электронной цифровой подписи» // Справочная правовая система «Консультант Плюс».

213. *Белопушкин В.И., Кириллычев А.Н.* Правовые аспекты обеспечения информационной безопасности / В.И. Белопушкин, А.Н. Кириллычев. – М.: Изд-во МГТУ, 2003.

214. *Гиляревский Р.С.* Рубрикатор как инструмент информационной навигации / Р.С. Гиляревский, А.В. Шапкин, В.Н. Белозеров. – СПб.: Профессия, 2008.

215. *Глушков В.М.* Основы безбумажной информатики. – 2-е изд. испр. – М.: Наука, 1987.

216. *Говорухин О.Э.* Правовые основы информационной безопасности и системы защиты информации коммерческого банка // Документация в информационном обществе: законодательство и стандарт: докл. и сообщ. на XXII Междунар. науч.-практ. конф., 22–23 ноября 2005 г. / Росархив. ВНИИДАД. М., 2006.

217. *Говорухин О.Э.* Служебная тайна // Служба кадров и персонал. – М.: ВНИИДАТ, 2006. № 4.

218. *Говорухин О.Э.* Когда персональные данные – коммерческая тайна // Служба кадров и персонал. 2006. № 7.

219. *Говорухин О.Э.* Служебная и профессиональная тайна // Делопроизводство. 2006. № 3.

220. *Говорухин О.Э.* Наименования ведомств: полное и сокращенное // Служба кадров и персонал. 2006. № 10.

221. *Говорухин О.Э.* Персональные данные: сбор, обработка, защита // Служба кадров и персонал. 2007. № 2.

222. *Говорухин О.Э.* Что такое служебная тайна? // Служба кадров и персонал. 2008. № 5.

223. *Говорухин О.Э.* Конфиденциальная информация: оформление доступа // Служба кадров и персонал. 2010. № 1.

224. *Головин С.Н.* Правовые основы электронного народовластия в России. – М.: IPmedia, 2004.

225. *Головистикова А.Н., Грудцына Л.Ю.* Права человека: учебник / А.Н. Головистикова, Л.Ю. Грудцына. – М.: Эксмо, 2008.

226. *Грушо А.А., Тимонина Е.Е.* Теоретические основы защиты информации / А.А. Грушо, Е.Е. Тимонина. – М.: Яхтсмен, 1996.

227. *Дашян М.С.* Право информационных магистралей (Law of information highways): вопросы правового регулирования в сфере Интернет / М.С. Дашян. – М.: Волтерс Клувер, 2007.

228. *Демушкин А.С.* Документы и тайна / А.С. Демушкин. – М.: Городец-издат, 2003.

229. *Демушкин А.С.* Организация работы с документированной информацией ограниченного доступа // Делопроизводство. 1999. № 1.

230. *Демушкин А.С.* Организация работы с документами ограниченного доступа // Отечественные архивы, 1999.

231. *Демушкин А.С.* Развитие системы кодирования информации // Делопроизводство. 2000. № 2.

232. *Демушкин А.С.* Секреты подлинные и мнимые. Нормативные акты по работе с документами ограниченного доступа // Законность. 2000. № 12.

233. *Демушкин А.С.* Организация работы по рассекречиванию документов // Делопроизводство. 2002. № 4.

234. *Демушкин А.С.* Кодирование кадровой информации // Служба кадров. 2002. № 12.

235. *Демушкин А.С.* Оформление допуска к закрытой информации // Служба кадров. 2003. № 2.

236. *Демушкин А.С.* Правовое регулирование организации работы с документированной информацией ограниченного доступа // Документация в информационном обществе: проблемы государственного регулирования документационного обеспечения управления при переходе на электронные технологии: докл. и сообщ. на VIII Междунар. науч.-практ. конф. 21–22 ноября 2001 г. / Росархив. – М.: ВНИИДАД, 2003.

237. *Демушкин А.С.* Принципиальные изменения в развитии понятия «информация» // Делопроизводство. 2004. № 3.

238. *Демушкин А.С.* Федеральный закон «О коммерческой тайне» с позиций ДОУ // Документация в информационном обществе: административная реформа и управление документацией: докл. и сообщ. на XI Междунар. науч.-практ. конф. 23–25 ноября 2004 г. / Росархив. – М.ВНИИДАД, 2005.

239. *Демушкин А.С.* Классификация тайн // Секретарское дело. 2004. № 12.

240. *Демушкин А.С.* Документы и коммерческая тайна // Служба кадров и персонал. 2004. № 12.

241. *Демушкин А.С.* Защита коммерческой тайны: опыт США // Служба кадров и персонал. 2005. № 7.

242. *Демушкин А.С.* «Электронный чиновник» // Делопроизводство. 2005. № 4.

243. *Демушкин А.С.* Комплексная система защиты информации на предприятии: учеб.-методич. пособие / А.С. Демушкин. – М.: МФЮА, 2006.

244. *Демушкин А.С.* Электронный документооборот: термины и определения // Служба кадров и персонал. 2008. № 5.

245. *Демушкин А.С., Говорухин О.Э.* Документирование конфиденциальной информации // Служба кадров и персонал. 2008. № 9.

246. *Демушкин А.С., Говорухин О.Э.* Составление перечня конфиденциальной информации // Служба кадров и персонал. 2008. № 10.

247. *Демушкин А.С., Говорухин О.Э.* Конфиденциальная информация: учет бумажных носителей // Служба кадров и персонал. 2008. № 11.

248. *Демушкин А.С.* Служебная тайна как секрет производства // Служба кадров и персонал. 2009. № 9.

249. *Демушкин А.С.* Правовые проблемы служебной тайны межведомственного электронного документооборота // Актуальные социально-экономические и правовые проблемы развития России: докл. на VIII Всерос. межвуз. науч.-практ. конф., 24–25 декабря 2009 г. – М., 2009.

250. *Демушкин А.С.* Межведомственный электронный документооборот // Служба кадров и персонал. 2010. № 4.

251. *Доронин А.И.* Бизнес-разведка / А.И. Доронин. – М.: Ось-89, 2002.

252. *Дурманов Н.Д.* Государственная тайна. – М., 1942.

253. *Жихарев А.П.* Программная система ведения и использования единого реестра информационных ресурсов и систем города Москвы // Программные продукты и системы. 2007. № 2.

254. *Завгородний В.И.* Комплексная защита в компьютерных системах: учеб. пособие / В.И. Завгородний. – М.: Логос; ПБОЮЛ Н.А. Егоров, 2001.

255. *Зорькин В.Д.* Конституция и права человека в XXI веке. К 15-летию Конституции Российской Федерации и 60-летию Всеобщей декларации прав человека. – М.: Норма, 2008.

256. Информационное право. Актуальные проблемы теории и практики / под общ. ред. И.Л. Бачило. – М., 2009.

257. Информационно-безопасные системы. Анализ проблемы: учеб. пособие / под ред. В. Н. Козлова. СПб.: Изд-во СПГТУ, 1996.

258. *Копылов В.А.* Информационное право. Вопросы теории и практики / В.А. Копылов. – М.., 2002.

259. *Красавин А.С.* Документационное обеспечение управления кадрами: Аналитический обзор нормативно-правовой базы и практики применения / ВНИИДАД. – М., 1996.

260. *Куняев Н.Н.* История развития системы документационного обеспечения управления в налоговых органах Российской Федерации на основе информационно-коммуникационных технологий (1990 – начало 2000-х гг.) / Н.Н. Куняев. – М.: МФА, 2009.

261. *Куняев Н.Н.* Документоведение: учебник для вузов / Н.Н. Куняев, Д.Н. Уралов, А.Г. Фабричнов; под ред. проф. Н.Н. Куняева. – М.: Логос, 2008.

262. *Куняев Н.Н.* Современная организация государственных учреждений России: учеб. пособие / Н.Н. Куняев. – М.: Юридическая литература, 2007.

263. *Куняев Н.Н.* Национальные интересы Российской Федерации в информационной сфере на современном этапе развития Российского государства // Российская юстиция. 2010. № 5.

264. *Куняев Н.Н.* Основные направления и условия развития информационного общества в Российской Федерации // Российская юстиция. 2009. № 8.

265. *Куняев Н.Н.* Проблема обеспечения защиты прав и свобод человека и гражданина в информационной сфере // Юридический мир. 2008. № 9 (141).

266. *Куняев Н.Н.* Информационная безопасность как объект правового регулирования в Российской Федерации // Юридический мир. 2008. № 2 (134).

267. *Куняев Н.Н.* Электронный архив – объективная необходимость при реализации Федеральной целевой программы «Электронная Россия» // Вестник архивиста. 2002. № 6 (72).

268. *Куняев Н.Н.* Информация как объект права // Актуальные проблемы гуманитарных наук: Мат. IX Междунар. науч.-практ. конф. – М., 2010.

269. *Куняев Н.Н.* О некоторых вопросах правового регулирования информационной безопасности в условиях формирования в Российской Федерации электронного правительства // Документация

в информационном обществе. Электронное правительство: управление документами: докл. и сообщ. на XVI Междунар. науч.-практ. конф. 2009 г. / Росархив. – М.: ВНИИДАД, 2010.

270. *Куняев Н.Н.* Электронное правительство – основа развития информационного общества в Российской Федерации // Документация в информационном обществе: корпоративный документооборот: доклады и сообщения на XV Междунар. науч.-практ. конф. 2008 г. / Росархив. – М.: ВНИИДАД, 2009.

271. *Куняев Н.Н.* Развитие правового регулирования применения информационно-коммуникационных технологий в процессе совершения сделок на основе современных теоретических исследований // Мат. VII Всерос. межвуз. науч.-практ. конф., 18 декабря 2008 г. – М., 2008.

272. *Куняев Н.Н.* О задачах совершенствования электронного документооборота в органах государственной власти // Документация в информационном обществе: современные технологии документооборота: доклады и сообщения на XIII Междунар. науч.-практ. конф., 22–23 ноября 2006 г. / Росархив. – М.: ВНИИДАД, 2007.

273. *Куняев Н.Н.* О некоторых вопросах правового регулирования электронного документооборота // Документация в информационном обществе: законодательство и стандарты: доклады и сообщения на XII Междунар. науч.-практ. конф., 22–23 ноября 2005 г. / Росархив. – М.: ВНИИДАД, 2006.

274. *Куняев Н.Н.* Опыт внедрения СЭД и ЭЦП в МНС России // CIO (Chief Information Officer). 2003. № 7 (17).

275. *Куняев Н.Н.* Система электронного документооборота МНС России // Российский налоговый курьер. 2001. № 9.

276. *Ларин М.В.* Информационный менеджмент и управление документацией // Документ в административных структурах: тез. докл. и выступлений на Междунар. конф. «Документ в административных структурах», 27–28 октября 1994 г. / – М.: ВНИИДАД, 1995.

277. *Ларин М.В.* Документационное обеспечение и информационный менеджмент // Делопроизводство. 1997. № 2/1.

278. *Ларин М.В.* Управление документацией и новые информационные технологии / М.В. Ларин. – М.: ВНИИДАД, 1998.

279. *Ларин М.В.* К вопросу о разработке концепции Федерального закона «О документационном обеспечении управления» // Делопроизводство. 2001. № 2.

280. *Ларин М.В.* Управление документацией в организациях / М.В. Ларин. – М.: Научная книга, 2002.

281. *Ларин М.В.* Электронный документооборот: что мешает его внедрению // Справочник секретаря и офис-менеджера. 2003. № 12.

282. *Ларин М.В.* Управление документами на основе международного стандарта ИСО 15489–2001: метод. пособие / М.В. Ларин, О.И. Рысков. – М.: ВНИИДАД, 2005.

283. *Ларин М.В.* Электронные документы в управлении: науч.-метод. пособие / М.В. Ларин, О.И. Рысков. – М.: ВНИИДАД, 2005.

284. *Мазуров В.А.* Тайна государственная, коммерческая, банковская, частной жизни. Уголовно-правовая защита: учеб. пособие / В.А. Мазуров. – М.: Дашков и К, 2003.

285. Методические рекомендации по внедрению ГОСТ Р 6.30–2003 «Организационно-распорядительная документация. Требования к оформлению документов». – М.: ВНИИДАД, 2008.

286. *Минаев В.А.* Основы информационной безопасности / В.А. Минаев, С.В. Скрыль, А..П. Фисун, В.Е. Потанин, С.В. Дворянкин. – Воронеж: Воронежский институт МВД России, 2000.

287. Основные правила работы архивов организаций. – М.: ВНИИДАД, 2007.

288. Отбор на государственное хранение документов, образующихся в деятельности организаций и предприятий нового типа: аналит. обзор. – М.: ВНИИДАД, 1994.

289. Очерки истории российской внешней разведки / под общ. ред. Е.М. Примакова в 6 т. – М.: Ин-т междунар. отношений, 1999.

290. Перечень типовых архивных документов, образующихся в научно-технической и производственной деятельности организаций с указанием сроков хранения. – М.: ВНИИДАД, 2009.

291. Перечень типовых управленческих документов, образующихся в деятельности организаций, с указанием сроков хранения. – М.: ВНИИДАД, 2007.

292. *Петрухин И.Л.* Личные тайны (человек и власть) / И.Л. Петрухин. – М.: Ин-т государства и права РАН, 1998.

293. *Погуляев В.В., Моргунова Е.А.* Комментарий к Федеральному закону «Об информации, информатизации и защите информации» / В.В. Погуляев, Е.А. Моргунова. – М.: Юстицинформ, 2004.

294. Примерный перечень документов, образующихся в деятельности кредитных организаций, с указанием сроков хранения. – М.: ВНИИДАД, 2000.

295. Разработка нормативных документов по документационному обеспечению управления организации. Рекомендации. – М.: ВНИИДАД, 2007.

296. Рекомендации о порядке учета, оперативного хранения и отбора на постоянное хранение электронных документов. – М.: ВНИИДАД, 2005.

297. Российское законодательство X–XX веков: в 9 т. – М., 1989.

298. *Северин В.А.* Правовое обеспечение информационной безопасности предприятия: учеб.-практ. пособие / В.А. Северин. – М.: Городец, 2000.

299. Своя разведка: способы вербовки агентуры, способы проникновения в психику, форсированное воздействие на личность, технические средства скрытого наблюдения и съема информации. Практическое пособие. – Мн.: Харвест. М.: АСТ, 2000.

300. *Смолькова И. В.* Тайна: понятие, виды, правовая защита. Юридический терминологический словарь-комментарий / И.В. Смолькова. – М.: Луч, 1998.

301. *Снытников А.А., Туманова Л.В.* Обеспечение и защита права на информацию / А.А. Снытников, Л.В. Туманова. – М.: Городец-издат, 2001.

302. *Соловьев Э.Я.* Коммерческая тайна и ее защита. – 2-е изд., перераб. и доп. / Э.Я. Соловьев. – М.: Ось-89, 2002.

303. *Солянов В.М., Черняев В.В.* Частная охранная деятельность в вопросах и ответах: учеб. пособие / В.М. Солянов, В.В. Черняев. – М.: Объедин. ред. МВД России, 2001.

304. Специальная техника и информационная безопасность / под ред. В.И. Кирина. – М.: Московская типография № 12, 2000.

305. *Степанов Е.А., Корнеев И.К.* Информационная безопасность и защита информации: учеб. пособие / Е.А. Степанов, И.К. Корнеев. – М.: ИНФРА-М., 2001.

306. Сборник руководящих документов по защите информации от несанкционированного доступа. Государственная техническая комиссия при Президенте Российской Федерации. – М., 1998.

307. *Фабричнов А.Г.* Проблемы использования электронных средств связи в отношениях, возникающих из договора банковского вклада // Изв. РГПУ им. А.И. Герцена. Аспирантские тетради. 2008. № 26 (60).

308. *Фабричнов А.Г.* Особенности использования электронных средств связи при совершении банковских сделок // Вестник РУДН. Сер. Юридические науки. 2008. № 1.

309. *Фабричнов А.Г.* «Традиционные» и «электронные» документы: гражданско-правовой аспект // Хозяйство и право. 2008. № 10.

310. *Фабричнов А.Г.* О некоторых вопросах использования электронных средств связи в отношениях, возникающих из договора банковского счета // ЭПОС. 2008. № 2 (34).

311. *Фатьянов А.А.* Тайна и право. – М., 1999.

312. *Черняк В.З.* Тайны промышленного шпионажа. – М.: Вече, 2002.

313. *Чуковенков А.Ю., Янковая В.Ф.* Правила оформления документов. Комментарий к ГОСТ 6.30–2003. Унифицированные системы документации. Унифицированная система организационно-распорядительной документации. Требования к оформлению документов / А.Ю. Чуковенков, В.Ф. Янковая. – М.: Проспект, 2005.

314. Экспертиза ценности и отбор на государственное хранение заявок на открытия и изобретения, промышленные образцы и товарные знаки: метод. рекомендации. – М.: ВНИИДАД, 1991.

315. Экспертиза ценности управленческих документов и комплектование ими государственных архивов на современном этапе (теория и методика): науч. доклад. – М.: ВНИИДАД, 1995.

316. *Янковая В.Ф.* Деловая переписка: учеб.-практ. пособие / В.Ф. Янковая. – М., 2007.

317. *Ярочкин В.И.* Безопасность информационных систем / В.И. Ярочкин. – М.: Ось-89, 1996.

Электронные ресурсы

318. Организация Объединенных Наций (Целевая группа по информационно-коммуникационным технологиям) – http://www.un.org

319. ФСБ России – http//www.fsb.ru

320. ФСТЭК России – http://www.fstec.ru

321. Совет Безопасности Российской Федерации – http://www.scrf.gov.ru

322. Ассоциация документальной электросвязи – http://www.rans.ru

323. Международный союз электросвязи – http://www.itu.int

324. Институт развития информационного общества – http://www.iis.ru

325. Лаборатория Касперского – http://www.kaspersky.ru

326. Сайт Jet Info информационный бюллетень – http://www.jetinfo.ru

327. Сайт Свирского – http//www.corbina.net/kis/index.htm

328. Википедия – свободная энциклопедия – http://www.ru.wikipedia.org

329. Рубрикон. Энциклопедии, словари, справочники – http://www.rubricon.com

330. Энциклопедия «Кругосвет» – http://www.krugosvet.ru

331. Glossary Commander: служба тематических электронных словарей – http://www.glossary.ru

332. Справочная правовая система «Консультант Плюс».

333. ВНИИДАД – http://www.vniidad.ru

Учебное издание

Куняев Николай Николаевич
Дёмушкин Александр Сергеевич
Фабричнов Александр Геннадьевич

КОНФИДЕНЦИАЛЬНОЕ ДЕЛОПРОИЗВОДСТВО И ЗАЩИЩЕННЫЙ ЭЛЕКТРОННЫЙ ДОКУМЕНТООБОРОТ

Учебник

Редактор *Е.В. Комарова*
Корректоры *Л.П. Коротич, С.В. Зубина*
Компьютерная верстка *А.М. Моисеева*
Оформление *И.В. Кравченко*

Подписано в печать 20.01.11. Формат 60x90/16
Печать офсетная. Бумага офсетная. Печ. л. 28.25
Тираж 1000 экз. Заказ

Издательская группа «Логос»
123104, Москва, Б. Палашевский пер., д. 9, стр. 1

По вопросам приобретения литературы обращаться по адресу:
111024, г. Москва, ул. Авиамоторная, д. 55, корп. 31, офис 305
Тел. (495) 645-89-24
Электронная почта: universitas@mail.ru
Дополнительная информация на сайте www.logosbook.ru