Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Заполярный государственный университет им. Н.М. Федоровского»
Политехнический колледж

МЕТОДИЧЕСКИЕ УКАЗАНИЯ И КОНТРОЛЬНЫЕ ЗАДАНИЯ

для студентов заочной формы обучения
по дисциплине
«Организация защиты конфиденциальной информации»
для специальности
40.02.01 Право и организация социального обеспечения

2022

Методические указания и контрольные задания для студентов заочной формы обучения учебной дисциплины «Организация защиты конфиденциальной информации» разработаны на основе Федерального государственного образовательного стандарта (ФГОС) по специальности среднего профессионального образования 40.02.01 Право и организация социального обеспечения

Организация-разработчик: Политехнический колледж ФГБОУ ВО «Заполярный государственный университет им. Н.М. Федоровского»

Разработчик: Ирина Михайловна Проценко, преподаватель

Рассмотрена на заседании комиссии правовых дисциплин

Председатель комиссии _____ Ю.А. Кудрань

Утверждена методическим советом политехнического колледжа ФГБОУ ВО «Заполярный государственный университет им. Н.М. Федоровского»

Протокол заседания методического совета №_____от «____»_____20___г.

Зам. директора по УР _____ С.П. Блинова

1 Пояснительная записка

Дисциплина «Организация защиты конфиденциальной информации» входит в цикл общепрофессиональных дисциплин.

В результате освоения учебной дисциплины обучающийся должен:

иметь представление:

- о взаимосвязи курса «Организация защиты конфиденциальной информации» с другими общепрофессиональными и специальными дисциплинами;

знать:

- принципы организации защищенного конфиденциального документооборота;
- установленные нормы и требования для обеспечения сохранности документов;
- виды, формы, технологию процедур учета и контроля документов

уметь:

- работать с документами в соответствии с требованиями конфиденциальности.

2 Требования, предъявляемые к написанию контрольных работ

Методические указания и контрольные задания разработаны для студентов заочной формы обучения для специальности Право и организация социального обеспечения.

В рамках изучение данной дисциплины предусматривается:

- чтение лекций, в которых определяются базовые положения темы, освещается степень разработанности и существующие проблемы их изучения, раскрываются способы научного анализа исследуемых феноменов;

- самостоятельное изучение тем, которые предполагают конкретизацию и углубленную проработку лекционного материала, акцентирование практической направленности полученных знаний, освоение и закрепление изучаемых вопросов посредством решения как теоретических, так и практических задач. А также проведения контрольных работ для оценки качества освоения дисциплины.

Данное методическое руководство к написанию контрольных работ ставит своей задачей - помочь студентам овладеть базовыми знаниями, умениями и навыками в рамках изучаемого междисциплинарного курса Организация защиты конфиденциальной информации. Основной целью изучения данного междисциплинарного курса является - ознакомление студентов видами тайн и организацией работы с конфиденциальной информацией с использованием современных автоматизированных технологий. Задачи курса – формирование у них умений и навыков в области создания конфиденциальных документов, обладающих юридической силой и способных служить эффективным механизмом реализации управленческих решений, а также получение знаний о принципах рациональной организации работы с документами ограниченного доступа и требования к хранению документального фонда предприятия (организации).

Тематика контрольных работ в настоящем руководстве составлена таким образом, что охватывает главные аспекты, изучаемой дисциплины.

При подготовке и выполнению контрольных работ первым и наиболее важным шагом является внимательное изучение тех вопросов, которые затрагиваются в рассматриваемой теме. Поэтому для успешного выполнения контрольного и домашнего задания необходимо, прежде всего, хорошо понять формулировку темы, а затем обратиться к рекомендуемой основной и дополнительной литературе для последующего изучения в рамках самостоятельной работы студента.

Методические указания по выполнению контрольных работ по междисциплинарному курсу Организация защиты конфиденциальной информации разработаны в соответствии с требованиями Федерального государственного образовательного стандарта среднего профессионального образования в Российской Федерации к обязательному минимуму содержания и уровню подготовки специалиста.

Контрольная работа оценивается в соответствии с полнотой систематизации важного теоретического материала, проверке определенных теоретических концепций и гипотез. Поверхностное изложение вопроса, рассматривается как недостаток работы.

Полученный материал, может быть, использован в учебном процессе, а также в научно-исследовательской работе.

Завершается подготовка контрольной работы или реферата защитой, которая производится в присутствии учебной группы. Ему могут быть заданы вопросы, связанные с его работой, на которые требуется дать аргументированные ответы.

Требования к оформлению контрольного задания

1 Объем контрольного задания должен содержать 10-14 листов текста.

2 Контрольное задание должно быть выполнено на белой бумаге формата А4 по ГОСТ 2.301 (210х297 мм) с одной стороны листа.

3 Поля: левое – не менее 20 мм, правое – не менее 10 мм, верхнее – не менее 20 мм, нижнее – не менее 20 мм.

4 Отступ красной строки: 1,25 см (5 знаков).

5 Междустрочный интервал: 1 см (одинарный).

6 Шрифт TimesNewRoman.

7 Размер шрифта – 14.

8 Выравнивание по ширине, цвет - черный.

9 Нумерация страниц: правый нижний край, начиная со 3-й страницы. Все страницы должны иметь сквозную нумерацию. Номер страницы проставляется арабскими цифрами.

10 Произвольное сокращение слов не допускается. Прямое цитирование «берется» в кавычки, далее в квадратных скобках идет ссылка на источник (номер источника в списке использованных источников) и указывается номер страницы. Ссылки на исследователей и авторов литературы отмечаются указанием в квадратных скобках номера источника, в которых раскрывается содержание материала.

Пример - [7, с. 25].

11 Внутри пунктов или подпунктов могут быть приведены перечисления. Перед каждой позицией перечисления следует ставить дефис. Для дальнейшей детализации перечислений необходимо использовать арабские цифры, после которых точка не ставится, а запись производиться с абзацного отступа, как показано на примере.

Пример –

1 _____.

2 _____.

- _____;

- _____;

3 _____.

12 Каждый пункт, подпункт и перечисления записывают с абзацного отступа.

13 Содержание, заголовки, подзаголовки, список использованных источников выделяют полужирным начертанием.

14 Заголовки и подзаголовки выполняются с абзацного отступа с прописной буквы без точки в конце, не подчеркивая. В начале заголовка помещают номер соответствующего раздела, подраздела, пункта.

15 Содержание и Список использованных источников центруют относительно основного текста.

16 Переносы слов в заголовках не допускаются. Если заголовок состоит из двух предложений, их разделяют точкой.

17 Расстояние между заголовком и текстом должно быть равно удвоенному межстрочному расстоянию; между заголовками раздела и подраздела – одному межстрочному расстоянию.

18 При составлении списка использованных источников необходимо следовать общим правилам. Все источники располагаются в списке в алфавитном порядке по первой букве фамилии автора, при отсутствии автора – по первой букве названия книги, статьи.

19 Контрольная работа оценивается по следующим показателям:

- полнота и систематизация изложенного теоретического материала;
- эрудированности в рассматриваемой области;
- использование известных результатов и научных фактов в работе;
- полнота цитируемой литературы;
- владение научным и специальным аппаратом;
- грамотность и логичность изложения материала;
- структура работы (введение, основная часть, вывод, приложения, список использованных источников).

Структура работы

1 Титульный лист.

2 Содержание с указанием нумерации начальных страниц каждого раздела работы. Название раздела печатается заглавными буквами с указанием порядкового номера и названия рубрики (1 Название).

3 Введение (актуальность выбранной темы, анализ использованных источников, структура и цель работы).

4 Основная часть (делится на разделы, разделы - на подразделы).

5 Заключение (выводы, обобщающие результаты).

6 Список использованных источников должен включать не менее 4 источников.

7 Приложения (если есть).

На титульном листе должна содержаться следующая информация:

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Норильский государственный индустриальный институт»
Политехнический колледж

КОНТРОЛЬНАЯ РАБОТА

по дисциплине
«Организация защиты конфиденциальной информации»

Специальность

40.02.01 Право и организация социального обеспечения

Выполнил:
студент заочного отделения
группы _____
_____
(фамилия, инициалы)
Дата сдачи _____

Проверил преподаватель
_____
(фамилия, инициалы)
Дата проверки _____
Оценка _____

2020

3 Тематический план

Номера тем	Наименование тем
	Введение
Тема 1	Понятие и особенности конфиденциальной информации. Общая характеристика нормативной правовой базы
Тема 2	Документирование конфиденциальной информации
Тема 3	Организация конфиденциального документооборота
Тема 4	Разрешительная система доступа к конфиденциальной информации
Тема 5	Составление номенклатуры дел, формирование и оформление конфиденциальных дел
Тема 6	Подготовка конфиденциальных документов для архивного хранения или уничтожения
Тема 7	Режим конфиденциальности документированной информации

4 Содержание теоретического раздела дисциплины

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 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. Документированная информация представляет собой различные виды документов.

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, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя».

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).

По уровню доступности документы подразделяются на две категории: **общедоступные** и с **ограниченным доступом**. Общедоступными являются открытые документы. К документам с ограниченным доступом относятся документы, работа с которыми может производиться по специальному разрешению уполномоченных на то лиц.

Документирование открытой информации и организация работы с открытыми документами входят в сферу действия открытого делопроизводства. Документы с ограниченным доступом относятся к сфере деятельности не одного, а нескольких типов делопроизводства, в зависимости от того, к какому виду тайны относится содержащаяся в документах информация.

При этом **под доступом** к конфиденциальной информации понимается санкционированное полномочным должностным лицом ознакомление конкретного лица с данной информацией. 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.

Документы, содержащие информацию, составляющие коммерческую и служебную тайну, принято называть конфиденциальными, а процесс их изготовления и организацию работы с ними –**конфиденциальным делопроизводством.**

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.

Особенность конфиденциального делопроизводства - защита содержащейся в конфиденциальных документах информации - вообще не предусмотрена в определении открытого делопроизводства, хотя определяемая собственником часть открытой информации должна защищаться от утраты. Конфиденциальная информация должна защищаться и от утраты, и от утечки.

Утечка конфиденциальной информации представляет собой неправомерный, т.е. неразрешенный выход такой информации за пределы защищаемой зоны ее функционирования или установленного круга лиц, имеющих право работать с ней. Если этот выход привел к получению информации (ознакомлению с ней) лицами, не имеющими к ней санкционированного доступа, независимо от того, работают или не работают такие лица на данном предприятии, значит имеет место **уязвимость** информации.

Уязвимость информации следует понимать, как ее доступность для воздействий, которые нарушают установленный статус информации.

Нарушение статуса любой документированной информации заключается в нарушении ее физической сохранности (вообще либо у данного собственника в полном или частичном объеме), логической структуры и содержания, а также доступности для неправомочных пользователей. Нарушение статуса конфиденциальной документированной информации дополнительно включает нарушение ее конфиденциальности (закрытости для посторонних лиц).

Уязвимость документированной информации – понятие собирательное. Она не существует вообще, а проявляется в различных формах:

• хищение носителя информации или отображенной в нем информации (кража);

• потеря носителя информации (утеря);

• несанкционированное уничтожение носителя информации или отображенной в нем информации (разрушение);

• искажение информации (несанкционированное изменение, несанкционированная модификация, подделка, фальсификация);

• блокирование информации;

• разглашение информации (распространение, раскрытие).

Термин "**разрушение**" употребляется, главным образом, применительно к информации на машинных носителях.

Существующие варианты названий: модификация, подделка, фальсификация – не совсем адекватны термину "искажение", они имеют нюансы, однако суть их одна и та же – **несанкционированное частичное и полное изменение состава первоначальной информации.**

Блокирование информации означает блокирование доступа к ней правомочных пользователей, а не злоумышленников. **Разглашение информации** является формой проявления уязвимости только конфиденциальной информации.

Та или иная форма уязвимости документированной информации может реализоваться в результате преднамеренного или случайного дестабилизирующего воздействия на носитель информации или на саму информацию.

Источниками дестабилизирующего воздействия могут быть люди, технические средства обработки передачи информации, средства связи, стихийные бедствия и др.

Способами дестабилизирующего воздействия на информацию являются копирование (фотографирование), записывание, передача, съем, заражение программ обработки информации вирусом, нарушение технологии обработки и хранения информации, вывод (или выход) из строя и нарушение режима работы технических средств обработки и передачи информации, физическое воздействие на информацию и др.

Реализация форм проявления уязвимости документированной информации приводит или может привести к двум видам уязвимости – **утрате** или **утечке** информации.

К **утрате** документированной информации приводят хищение и потеря носителей информации, несанкционированное уничтожение носителей информации или

только отображенной в них информации, искажение и блокирование информации. Утрата может быть полной или частичной, безвозвратной или временной (при блокировании информации), но в любом случае она наносит ущерб собственнику информации.

К **утечке** конфиденциальной документированной информации приводит ее разглашение. Разглашение или распространение конфиденциальной информации означают несанкционированное доведение ее до потребителей, не имеющих права доступа к ней. При этом такое доведение должно осуществляться кем-то, исходить от кого-то.

Защита конфиденциальной документированной информации от утраты и утечки осуществляется в определенной мере в рамках конфиденциального делопроизводства.

Вопросы для самоконтроля

1 Что такое «конфиденциальная информация»?

2 Назовите категории по уровню доступности документов? Их характеристика.

3 Что понимается под технологиями конфиденциального делопроизводства?

4 Отличительные особенности конфиденциального делопроизводства от открытого?

5 Какие требования предъявляются к конфиденциальному делопроизводству?

6 Охарактеризуйте понятия: «утечка», «уязвимость», «утеря».

Литература: [15, с.68-73], [16, с. 8-17], [9, с.19-22].

Тема 1 Понятие и особенности конфиденциальной информации. Общая характеристика нормативной правовой базы

1.1. Общие положения. Характеристика понятий

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:

- 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.

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. Обладателями информации могут быть гражданин (физическое лицо), юридическое лицо, государственные органы и органы местного самоуправления (далее - государственные и негосударственные структуры) в пределах их полномочий.

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.

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.

Распространение информации– действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц. Следовательно, ограничение распространения информации – действия, направленные на получение информации определенным кругом лиц или передачу ее определенному кругу лиц.

Понятие «тайна» имеет два смысловых значения: нечто абсолютно неизвестное всем и нечто относительно неизвестное для каких-либо лиц. Иными словами, ин-

формация 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.

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.

Виды информационных ресурсов по категории доступа показаны на рисунке 1.

Рисунок 1 – Виды информационных ресурсов по категориям доступа

Вопросы для самоконтроля

1 Основные принципы Федерального закона «Об информации, информационных технологиях и защите информации»?

2 Кто является обладателем информации?

3 В каком документе утвержден Перечень сведений конфиденциального характера?

4 Какие ограничения введены законодательством на отнесение информации к конфиденциальной?

5 Перечислите виды информационных ресурсов по категории доступа.

Литература: [15, с.68-73], [16, с. 8-17], [9, с.19-22].

1.2 Понятие государственной тайны. Нормативные основы организации работы с документами, содержащими государственную тайну

Понятие государственной тайны. Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне» устанавливает правовые основы охраны государственной тайны, определяет требования к допуску и порядку документооборота.

Государственная тайна – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-разыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

Государственную тайну составляют:

1)сведения в военной области;

2)сведения в области экономики, науки и техники;

3)сведения в области внешней политики и экономики;

4)сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности, а также в области противодействия терроризму и в области обеспечения безопасности лиц, в отношении которых принято решение о применении мер государственной защиты.

Не подлежат отнесению к государственной тайне и засекречиванию сведения:

- о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях;
- о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;
- о привилегиях, компенсациях и социальных гарантиях, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям;
- о фактах нарушения прав и свобод человека и гражданина;
- о размерах золотого запаса и государственных валютных резервах Российской Федерации;
- о состоянии здоровья высших должностных лиц Российской Федерации;
- о фактах нарушения законности органами государственной власти и их должностными лицами.

Формы допуска к государственной тайне

В соответствии со степенями секретности сведений, составляющих государственную тайну, устанавливаются следующие формы допуска граждан к государственной тайне:

- первая форма – для граждан, допускаемых к сведениям особой важности;
- вторая форма – для граждан, допускаемых к совершенно секретным сведениям;
- третья форма – для граждан, допускаемых к секретным сведениям.

Допуск должностных лиц и граждан к государственной тайне предусматривает:

- принятие на себя обязательств перед государством по нераспространению доверенных им сведений, составляющих государственную тайну;
- согласие на частичные, временные ограничения их прав;
- письменное согласие на проведение в отношении их полномочными органами проверочных мероприятий;
- определение видов, размеров и порядка предоставления социальных гарантий;

- ознакомление с нормами законодательства РФ о государственной тайне, предусматривающими ответственность за их нарушение;

- принятие решения руководителем органа государственной власти, предприятия, учреждения или организации о допуске оформляемого лица к сведениям, составляющим государственную тайну.

При допуске к сведениям особой важности или совершенно секретным сведениям, отнесенным к государственной тайне в соответствии с законом РФ о государственной тайне, заключил трудовой договор (контракт), предполагающий временное ограничение права на выезд из РФ, при условии, что срок ограничения не может превышать пять лет со дня последнего ознакомления лица со сведениями особой важности или совершенно секретными сведениями. Таким образом, ограничение прав на выезд зависит от формы допуска.

Ответственность за нарушение законодательства о государственной тайне установлена Уголовным и Трудовым кодексом.

Государственная тайна – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ.

Установлено три степени секретности сведений, составляющих государственную тайну:

- «Особой важности»;
- «Совершенно секретно»;
- «Секретно».

Использование данных грифов для засекречивания сведений, не отнесенных к государственной тайне, не разрешается.

Организацией работы, в том числе и выполнением делопроизводственных операций, с документами, имеющими грифы секретности, занимаются специализированные подразделения организаций, учреждений (Пятый отдел).

Вопросы для самоконтроля

1 Что такое государственная тайна?

2 Какие сведения составляют государственную тайну?

3 Какие сведения не подлежат отнесению к государственной тайне и засекречиванию?

4 Охарактеризуйте формы допуска к государственной тайне?

5 В чем заключается механизм допуска должностных лиц и граждан к государственной тайне?

6 В чем состоят особенности оформления документов, содержащих государственную тайну?

Литература: [55, с.68-73], [16, с. 10-17], [9, с.19-22].

1.3 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».*

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.

Обработка персональных данных должна осуществляться при следующих **двух условиях.**

Первое условие: оператор может выполнять ее только с согласия субъектов персональных данных.

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.

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).

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.

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.

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.

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). В Уголовном кодексе Российской Федерации (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).

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.

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, – сведения, составляющие тайну следствия и судопроизводства, а также сведения о защищаемых лицах и мерах государственной защиты.

Вопросы для самоконтроля

1 Основной федеральный закон, который регулирует организацию работы с персональными данными?

2 В чем заключаются технологии обработки персональных данных?

3 В чем заключается организация обработки персональных данных?

4 Какие условия должны осуществляться при обработке персональных данных?

5 Охарактеризуйте правила работы (обработки) с документированными персональными данными.

6 Дайте характеристику понятия «конфиденциальность персональных данных»?

7 Кто является правообладателем информации?

Литература: [15, с.68-73],[16, с. 17-25], [9, с.19-22].

1.4 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 (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.

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

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.

Федеральным законом «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства» 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.

Вопросы для самоконтроля

1 Существует ли в законодательстве перечень сведений, составляющих следственную тайну?

2 Какой нормативно-правовой акт определяет, какие обстоятельства исследуются на закрытом судебном заседании?

Литература: [15, с.68-73],[16, с. 25-38], [9, с.19-22].

1.5 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 радом 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.

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.

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.

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.

Вопросы для самоконтроля

1 Существует ли нормативно-правовой документ, регулирующий служебную тайну?

2Что такое служебная тайна? Разница между служебной и коммерческой тайнами?

3 Кто является носителем или субъектом служебной тайны?

4 Охарактеризуйте требования, по которым информация может являться служебной тайной.

Литература: [15, с.68-73],[16, с. 25-38], [9, с.19-22].

1.6 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».

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.

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», «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».

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 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.

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».

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 сведении и учебном процессе и в иных целях.

Лица, которым в установленном законом порядке переданы сведения, составляющие врачебную тайну, наравне с медицинскими, 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.

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.

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.

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.

Вопросы для самоконтроля

1 Что такое профессиональная тайна?

2Что такое служебная тайна? Разница между служебной и коммерческой тайнами?

3Виды профессиональных тайн.

4 Охарактеризуйте нормативно-правовую базу, регулирующую профессиональную тайну.

Литература: [15, с.68-73],[16, с. 39-48], [9, с.19-22].

1.7 Коммерческая тайна

Точно назвать дату появления в 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». Дополнением к указанному определению понятия явилось принятие Закона РСФСР «О предприятиях и предпринимательской деятельности», 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).

Федеральный закон «О коммерческой тайне» определил понятие «коммерческая тайна». 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.

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».

Вопросы для самоконтроля

1 В какое время было первое официальное нормативно-правовое закрепление понятия «коммерческая тайна»?

2Укажите признаки, характеризующие коммерческую тайну?

Литература: [15, с.68-73],[16, с. 48-52], [9, с.19-22].

1.8 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.*

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

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.

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.

Вопросы для самоконтроля

1 Какие сведения могут признаваться информацией, относящейся к секрету производства (ноу-хау) и служебному секрету производства?

2 Кто имеет право на секрет производства?

3В чем заключается порядок для выполнения целей, функций и задач конкретной организации в области секрета производства?

4 Кем составляется перечень данной информации?

5 Назовите виды договоров, регулирующих конфиденциальность секрета производства.

Литература: [15, с.68-73],[16, с. 58-61], [9, с.19-22].

1.9 Ответственность за нарушение правил работы с конфиденциальными документами

Дисциплинарная ответственность за разглашение охраняемой законом тайны. В ТК РФ предусмотрено специальное основание расторжения трудового договора с работниками, работающими со сведениями, составляющими тайну: увольнение за разглашение охраняемой законом тайны – государственной, коммерческой, служебной, иной, ставшей известной работнику в связи с исполнением им трудовых обязанностей (пункт 6 первой части ст.81 ТК РФ).

Работодателю необходимо соблюдать порядок, установленный ст.193 ТК РФ, и помнить, что дисциплинарное взыскание в виде увольнения может быть применено не позднее одного месяца со дня обнаружения проступка и не позднее шести месяцев с момента совершения. В этот срок не включаются периоды болезни работника, пребывания его в отпуске, а также время, необходимое для учета мнения представительного органа работников.

Если работодатель обнаружил факт разглашения охраняемых сведений, *нужно составить акт.*

По итогам расследования и до оформления приказа о применении дисциплинарного взыскания за разглашение охраняемой законом тайны от работника следует потребовать письменное объяснение (ст. 193 ТК РФ). Если он готов представить объяснительную записку, письменное требование можно не оформлять. Если же ситуация носит явно конфликтный характер, то данное требование лучше оформить письменно и вручить работнику под роспись.

Уголовная ответственность в сфере конфиденциального делопроизводства. Ответственность за разглашение сведений, составляющих государственную тайну, предусмотрена ст.283 УК РФ.

Появление данной нормы в уголовном законодательстве обусловлено необходимостью реального противодействия преступным деяниям, совершаемым лицами, не являющимися специальными субъектами, указанными в ст. 283 УК и преступным путем завладевшими сведениями, составляющими государственную тайну.

Статья 284 УК устанавливает ответственность за утрату документов, содержащих государственную тайну.

Наконец, **наиболее тяжкими преступлениями являются шпионаж и государственная измена**. Ответственность за государственную измену предусмотрена ст.275 УК РФ.

Статья 276 УК РФ устанавливает ответственность за шпионаж. Передача, собирание, похищение или хранение в целях передачи иностранному государству, международной либо иностранной организации или их представителям сведений, составля-

ющих государственную тайну, а также передача или собирание по заданию иностранной разведки или лица, действующего в ее интересах, иных сведений для использования их против безопасности РФ, то есть шпионаж, если эти деяния совершены иностранным гражданином или лицом без гражданства, наказываются лишением свободы на срок от десяти до 20 лет.

Ответственность за разглашение коммерческой и иных видов тайн. Ответственность за незаконное разглашение коммерческой, банковской или налоговой тайны установлена ст. 183 УК РФ.

Вопросы для самоконтроля

1 Виды ответственности за разглашение охраняемой законом тайны?

2 В чем заключается дисциплинарная ответственность?

3Какой порядок должен соблюдаться при вынесении дисциплинарного взыскания?

4 За разглашение каких сведений предусмотрена уголовная ответственность в сфере конфиденциального делопроизводства?

5 Ответственность за разглашение коммерческой и иных видов тайн?

Литература: [5, с.68-73],[10, с. 10-12], [9, с.19-22].

Тема 2 Документирование конфиденциальной информации

2.1 Особенности документирования конфиденциальной информации

Документирование информации – одно из обязательных условий включения информации и документов в информационные ресурсы тобой 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.

В федеральных органах исполнительной власти документирование информации осуществляется в порядке, установленном Правительством Российской Федерации в Правилах делопроизводства и документооборота (далее – Правила делопроизводства). 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 государ-

ственным органом, органом местного самоуправления, юридическим или физическим лицом, оформленный в установленном порядке и включенный в документооборот федерального органа исполнительной власти.

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. Электронное сообщение, подписанное электронной 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.

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.

Конфиденциальная информация – документированная информация, доступ к которой также ограничен в соответствии с законодательством РФ.

На документах, содержащих такую информацию, могут быть проставлены следующие грифы ограничения доступа:

1 «Для служебного пользования» («ДСП»).

2 «Конфиденциально» - с подразделением на несколько уровней:

- «Конфиденциально»;
- «Строго конфиденциально»»;
- «Конфиденциально – особый контроль».

3 «Коммерческая тайна».

Вопросы для самоконтроля

1 В каком документе определены требования и особенности документирования информации ограниченного доступа?

2Объем и содержание создаваемых конфиденциальных документов?

3Специфика оформления реквизитов документов, носящих конфиденциальную информацию?

4 Какие грифы конфиденциальности используются?

Литература: [15, с.68-73],[16, с. 58-61], [9, с.19-22].

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

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).

Изменение отметки конфиденциальности документа производится при изменении степени конфиденциальности содержащихся в нем сведений.

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

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».

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

Например:

Строго конфиденциально
Экз. № 1

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 передаете 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.

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.

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».

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

• определение перечня информации, составляющей коммерческую тайну;

. 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;

•регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;

– 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).

Решение этой проблемы состоит в разделении информации по степеням конфиденциальности – на создаваемую и отправляемую документированную информацию.

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**.** 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».

Вопросы для самоконтроля

1 Назовите степень конфиденциальности, которая может быть присвоена документу?

2 Кто может установить степень конфиденциальности и внести изменения?

3Охарактеризуйте порядок оформления отметки о конфиденциальности на документах?

4 Какие грифы конфиденциальности используются?

Литература: [15, с.68-73],[16, с. 61-63], [9, с.19-22].

2.3 Перечни конфиденциальной информации и документов. Разработка Перечня конфиденциальной документированной информации

Одним из первоочередных и обязательных моментов в организации обращения конфиденциальных документов является определение перечня информации, составляющей коммерческую или служебную тайну. Только определившись с тем, к какой информации надлежит ограничить доступ, можно выстраивать (регламентировать) порядок ее обращения и защиты.

Разработкой перечня информации, составляющего коммерческую тайну, должна заниматься экспертная комиссия совместно со службой безопасности.

На первом этапе работы на основе анализа задач, функции и направлений деятельности организации (предприятия) необходимо установить весь состав циркулирующей информации, отображенной на любом носителе, любым способом и в любом виде.

На втором этапе определяется, какая из установленной информации должна быть конфиденциальной и отнесена к коммерческой тайне.

После установления состава конфиденциальной информации может определяться и дополнительное ограничение доступа к ней. Действительно, довольно часто бывает необходимо выделить наиболее значимую информацию (из всей конфиденциальной информации) с целью установления для нее более жесткого режима защиты. Чем больше предполагаемый ущерб от ее разглашения, тем ограниченнее должен быть круг лиц, к ней допущенных.

Дополнительное ограничение доступа целесообразно указывать для конкретного документа, например, введением, при его адресовании, дополнительной надписи «Только:». Порядок использования этого ограничения, перечень должностных лиц, имеющих право его устанавливать, а также указание о запрещении дальнейшего расширительного адресования документа с такой надписью следует изложить в положении, регламентирующем общую систему доступа.

Следующий этап– определение конкретных сроков конфиденциальности информации либо обстоятельств и событий, при наступлении которых конфиденциальность снимается. Продолжительность конфиденциальности информации должна соответствовать срокам действия условий, необходимых и достаточных для признания данной информации конфиденциальной в соответствии с законодательством.

Результаты работы оформляются документально – перечнем информации, составляющей коммерческую тайну, который может иметь следующую форму (таблица 1.1).

Таблица 1.1 – Перечень информации, составляющей коммерческую тайну

(наименование организации)

№ п/п	Наименование сведений, относящихся к конфиденциальным	Должностные лица (подразделения), имеющие право распоряжения сведениями	Срок конфиденциальности
1	2	3	4

При значительном объеме конфиденциальных сведений они классифицируются в перечне по разделам, соответствующим сферам деятельности.

Перечень рассматривается экспертной комиссией с оформлением соответствующего протокола, подписывается ее председателем (или на основании протокола – начальником службы безопасности, заместителем руководителя по безопасности) и утверждается (вводится в действие) приказом или распоряжением руководителя организации (предприятия).

В приказе должны быть определены мероприятия по обеспечению функционирования перечня и контролю его выполнения. С приказом и перечнем необходимо ознакомить **под роспись всех сотрудников**, работающих с конфиденциальной информацией. Копии перечня или выписки из него должны быть направлены конфидентам данной коммерческой тайны. Ими являются физические или юридические лица, которым в силу служебного положения, договора либо на ином законном основании известна коммерческая тайна ее обладателя.

Дополнения и изменения состава, включенных в перечень сведений осуществляются таким же порядком. При существенном изменении состава сведений перечень должен составляться заново. Об изменениях в составе коммерческой тайны обладатель информации обязан в письменной форме известить конфидентов данной информации.

Документирование конфиденциальной информации является важнейшей составной частью конфиденциального делопроизводства, поскольку от количества, состава и правильности оформления документов зависят качество и эффективность управленческой и производственной деятельности, достоверность и юридическая сила документов, трудоемкость их обработки. *Объем и характер документов влияют и на организацию работы по их защите.*

Определение состава документируемой информации должно увязываться с решением конкретных задач. В зависимости от назначения документируемой информации определяются конкретные виды документов, в которых эта информация должна быть зафиксирована.

После установления состава постоянно разрабатываемых (типовых) документов определяется круг лиц, имеющих право составлять, согласовывать и подписывать(утверждать) тот ИЛИ ИНОЙ ВИД документа, а также адресаты, которым данный документ должен направляться.

Перечень издаваемых конфиденциальных документов может иметь следующую форму (таблица 1.2).

Таблица 1.2 - Перечень издаваемых конфиденциальных документов

(наименование организации)

Порядковый номер	Наименование документа	Основание для конфиденциальности	Срок конфиденциальности	Подразделения или должностные лица, ответственные за подготовку	Подразделения или должностные лица, согласующие документ	Должностные лица, утверждающие (подписывающие документ	Количество экземпляров	Адресаты
1	2	3	4	5	6	7	8	9

С перечнями под роспись должны быть ознакомлены все лица, наделенные правом составлять, визировать, подписывать и утверждать соответствующие конфиденциальные документы.

Внесение возможных последующих уточнений или изменений в перечни оформляется тем же порядком.

При изменении перечня информации, составляющей коммерческую и служебную тайну, соответствующие изменения вносятся и в перечни издаваемых конфиденциальных документов. О снятии грифа конфиденциальности с отправленных документов должны быть письменно оповещены все адресаты.

При необходимости издания разовых документов, не включенных в перечни, или дополнительных экземпляров документов, их изготовление может производиться по решению соответствующего руководителя, наделенного правом распоряжаться теми или иными конфиденциальными сведениями (указанной в перечне информации, составляющей коммерческую или служебную тайну). Одновременно определяется целесообразность последующего включения таких документов (дополнительных экземпляров) в перечень издаваемых конфиденциальных документов.

В необходимых случаях рассмотренные перечни сами могут иметь гриф конфиденциальности. Гриф конфиденциальности должен соответствовать совокупной степени конфиденциальности сведений, содержащихся в графах этих перечней. При наличии грифа конфиденциальности перечни регистрируются по журналу учета изданных документов.

Общие положения

Одной из особенностей документирования конфиденциальной информации является регламентирование состава создаваемых конфиденциальных документов. Конфиденциальная документированная информация должна создаваться только при действительной необходимости в письменном удостоверении наличия и содержания управленческих, коммерческих, производственных и иных действий, передаче ин-

формации, 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.

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.

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 включенияв них избыточных данных.

Аналогичные перечни в качестве разделов, входящих в общий Перечень конфиденциальной документированной информации, могут иметь структурные подразделения организации.

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 информации. Затем этот Перечень можно будет наполнить конкретной информацией при изменении внешних и внутренних условий работы организации.

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;

– 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.

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

Таблица 1 – Форма перечня конфиденциальной информации

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

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.

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).

Таблица 2 – Форма Перечня создаваемой КДИ

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

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

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.

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.

Вопросы для самоконтроля

1 Технология разработки перечня конфиденциальных документов.

2 Кто занимается составлением перечня конфиденциальной информации?

3Кто вводит дополнительные ограничения доступа к документу?

4 Каким органом рассматривается перечень конфиденциальных документов?

Литература: [15, с.68-73],[16, с. 69-78], [9, с.19-22].

2.4 Учет бумажных носителей конфиденциальной информации

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 лист 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.

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

Таблица 1 – Форма учета бумажных носителей

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.

Вопросы для самоконтроля

1 Перечислите виды бумажных носителей.

2Укажите назначение бумажных носителей.

3Особенности оформления бумажных носителей.

4 Где учитывается носители конфиденциальной информации?

5 Какая информация проставляется на самих носителях?

Литература: [15, с.144-160],[16, с. 78-82], [9, с.29-33].

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. 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 но-

сителе 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.

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).

Таблица 1 – Форма учета проектов созданных конфиденциальных документов

Учетный номер и отметка конфиденциальности	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, сопроводительного документа	Отметка о возврате	Индекс (номер) дела, номер листов дела	Номер по учету документов выделенного хранения, количество экземпляров	
10	11	12	13	14	15	16	17	

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

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.

РАСПИСКА

Дана _____*в том, что мною* _____
(инициалы, фамилия) (инициалы, фамилия)

получены во временное пользование документы, носители информации
за № _____*,*
всего на _____*л.*
Подпись
Дата

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.

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.

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

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.

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

Форма акта

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».

Вопросы для самоконтроля

1 Каким способом могут изготавливаться проекты конфиденциальных документов?

2Каким нормам должны отвечать черновики и проекты текстовых документов?

3Какие требования должны учитываться при изготовлении дополнительных экземпляров проекта документа?

4 Что должен учитывать исполнитель после отработки проекта текстового документа?

5 Назначение Службы делопроизводства при работе с проектами конфиденциальных документов.

Литература: [15, с.144-160],[16, с. 82-89], [9, с.29-33].

2.6-2.7 Особенности создания и изготовления конфиденциальных документов с помощью средств электронно-вычислительной техники, их печатания, тиражирования, размножения

Размножение конфиденциальных документов должно производиться только при действительной служебной необходимости в их дополнительных экземплярах.

Конфиденциальные документы могут размножаться в подразделении конфиденциального делопроизводства или в специальном множительном подразделении предприятия. Размножение (тиражирование) конфиденциальных документов в типографиях методом набора и печатания текста, как правило, не осуществляется главным образом из-за отсутствия потребности в большом тираже.

Размножение конфиденциальных документов не должно производиться вперемежку с размножением открытых документов. Во время размножения конфиденциальных документов все, что не имеет отношения к их размножению, должно быть

убрано с рабочих мест, используемых при размножении, доступ посторонних лиц в помещение, в котором производится размножение, не разрешается.

При возникновении в процессе размножения листов брака они помещаются в специальную папку.

Разрешение на размножение документов могут давать по усмотрению руководителя предприятия руководители соответствующих структурных подразделений самостоятельно либо совместно с руководителем службы безопасности (подразделения конфиденциального делопроизводства) предприятия. *Подписанный руководителем предприятия список лиц, имеющих право давать разрешение на размножение конфиденциальных документов, должен находиться в множительном подразделении.*

Документы, поступившие из других предприятий, могут размножаться только с письменного разрешения издавших их предприятий.

Размножение документов производится в форме изготовлении дополнительных экземпляров, снятия копий с документов и производства выписок из документов.

Разрешение на изготовление дополнительных экземпляров документов оформляется на обороте последнего листа экземпляра, с которого должно производиться размножение. Этот экземпляр не должен в последующем направляться на другие предприятия, он подшивается в дело или переводится на учет документов выделенного хранения.

При размножении поступившего документа дополнительно делается ссылка на номер и дату разрешения.

При невозможности оформления разрешения на размножение на самом документе оно оформляется в форме учета данного документа.

При размножении документов в специальном множительном подразделении их передача на размножение производится специально назначенному для размножения конфиденциальных документов лицу под его подпись в форме учета или карточке выдачи документа.

Подлежащие размножению документы регистрируются в подразделении конфиденциального делопроизводства или в специальном множительном подразделении (по месту размножения) в ***журнале учета размножения конфиденциальных документов.***

Учетный номер, присвоенный документу, сохраняется на размноженных экземплярах.

На размноженных экземплярах работник подразделения конфиденциального делопроизводства проставляет их номера. При этом если документ был издан данным предприятием, то номера размноженных экземпляров продолжают номера ранее изготовленных экземпляров, если документ был издан другим предприятием, то на размноженных экземплярах их номера проставляются дробно: в числителе на всех экземплярах остается номер, присвоенный предприятием, издавшим документ, а в знаменателе на каждом экземпляре проставляется присвоенный ему порядковый номер, начиная с № 1.

На каждом размноженном экземпляре в реквизите "Отметка об исполнителе" проставляется только учетный номер, присвоенный документу при его издании,

независимо от места издания, фамилия, имя, отчество исполнителя и его рабочий телефон (если проставлен на размножаемом экземпляре).

Если размноженные экземпляры не воспроизводят подпись, то они удостоверяются **печатью** предприятия или подразделения конфиденциального делопроизводства, которая проставляется с захватом части слова, обозначающего должность лица, подписавшего документ.

Технология производства выписок из конфиденциальных документов имеет следующие особенности.

Выписки могут производиться с документов, как не подшитых, так и подшитых в дела, а также с документов выделенного хранения.

Разрешение на изготовление выписки оформляется записью: "Размножить л.л. (п.п.) _____ в _____ экз.".

Выпискам присваивается отдельный учетный номер – очередной порядковый номер по журналу учета изданных документов, независимо от того, по какому виду учета зарегистрирован документ, из которого производится выписка. Проставление учетного номера на выписке осуществляется аналогично проставлению его на копии.

Особенности создания и изготовления конфиденциальных документов с помощью средств электронно-вычислительной техники, их печатания, тиражирования, размножения

Конфиденциальные документы, создаваемые в организации, оформляются на бланках, на стандартных листах бумаги формата А4 (210 х 297 мм) или А5 (148 х 210 мм) либо в виде электронных документов, или в виде электронных сообщений – информации, переданной или полученной пользователем информационно-телекоммуникационной сети. Они должны иметь установленный состав реквизитов.

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.

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.

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.

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

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.

Вопросы для самоконтроля

1 Размножение конфиденциальных документов.

2 Технология изготовления копий документов.

3 Технология производства выписок из конфиденциальных документов.

4 Особенности создания и изготовления конфиденциальных документов с помощью средств электронно-вычислительной техники, их печатания, тиражирования, размножения.

5 Организация работы по изготовлению электронных конфиденциальных документов.

6 Размножение и тиражирование конфиденциальных документов.

Литература: [15, с.144-160],[16, с. 89-93], [9, с.29-33].

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

Печати и штампы

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

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». 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 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 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.

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.

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 штемпельногравернымипредприятиями, 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.

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.

Вопросы для самоконтроля

1 Кто занимается заявками на изготовление печатей?

2 Кто ведет общий учет имеющихся в организации печатей и штампов?

3 Как осуществляется хранение штампов и печатей в организации?

4 Что такое бланк? Каким способом оформляются бланки конфиденциальных документов?

Литература: [15, с.144-160],[16, с. 93-99], [9, с.29-33].

Тема 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. 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. Регистрацией документа является также запись учетных данных о документе по установленной форме, фиксирующая факт его получения, создания или отправления.

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.

Данные о конфиденциальном документе заносятся в журнал или карточку учета поступивших документов.

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.).

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, 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. Учет внутренних конфиденциальных документов ведется отдельно от их регистрации.

Порядок исполнения конфиденциальных документов предполагает в качестве одной из задач исполнителя ведение их учета.

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

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

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.

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.

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.

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.

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.

Учет конфиденциальной информации, циркулирующей в АИС или системах электронного документооборота, производится с помощью Реестра конфиденциальной информации и автоматизированной информационной системы организации.

Вопросы для самоконтроля

1 Дайте характеристику понятиям «документооборот» и «регистрация».

2 Какие этапы включают в себя учет и регистрация конфиденциальных документов?

3 Виды учета конфиденциальной документированной информации.

4 Порядок исполнения конфиденциальных документов.

5 Специфика учета электронных конфиденциальных документов.

Литература: [15, с.144-160],[16, с. 99-107], [9, с.29-33].

3.2 Обработка поступающих конфиденциальных документов, их учет и регистрация

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.

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.

После проставления подписи за принятые пакеты сотрудник Службы делопроизводства заполняет графы журнала учета поступивших пакетов.

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

На самом документе в правом углу нижнего поля первого листа проваляется отметка о поступлении, которая содержит учетный номер, присвоенный документу, гриф конфиденциальности, дату поступления, количество листов. При наличии сопроводительного письма указывается отдельно количество листов сопроводительного письма и через знак "+" общее количество листов всех конфиденциальных приложений. При наличии открытых (не конфиденциальных) приложений количество их

листов отражается отдельно через знак "+" с добавлением аббревиатуры "н/с" (несекретные), например:

Уч. №
47КТ
19.04.2003
л.л.
1+20+6 н/с

Если отметка проставляется с помощью штампа, то он может иметь следующую форму:

Уч. №
Дата
Кол-во
листов

Учет и регистрация поступивших конфиденциальных документов осуществляются одновременно в единой форме, 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.

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. Сопроводительное письмо подшивается в дело.

Вопросы для самоконтроля

1 Охарактеризуйте процесс экспедиционной обработки поступивших документов.

2 Какие действия должен выполнять сотрудник экспедиционного подразделения Службы делопроизводства?

3 Учет и регистрация поступивших (входящих) конфиденциальных документов.

Литература: [15, с.144-160],[16, с. 107-113], [9, с.29-33].

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

Учет и регистрация внутренних (созданных/изданных) конфиденциальных документов начинается на стадии подготовки их проектов.

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. 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.

Вопросы для самоконтроля

1 Кто осуществляет организацию конфиденциального делопроизводства?

2 Задачи и функции подразделения конфиденциального делопроизводства.

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

4 Охарактеризуйте процесс уничтожения указанных материалов сотрудником Службы делопроизводства.

Литература: [15, с.144-160],[16, с. 113-114], [9, с.29-33].

3.4 Технологии исполнения и контроля за исполнением конфиденциальных документов

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

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.

Разработку Перечня целесообразно возлагать на постоянно действующую Экспертную комиссию по защите конфиденциальной информации. 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.

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. 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.

О нарушении срока исполнения документа Служба делопроизводства извещает соответствующего руководителя. После исполнения документа исполнитель проставляет на нем отметку об исполнении.

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

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.

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.

Вопросы для самоконтроля

1 Кто занимается разработкой Перечня поступивших документов?

2 Ответственность за качество исполнения документов.

3 Сроки исполнения конфиденциальных документов.

4 Обязанности руководителей и исполнителей при работе с конфиденциальными документами.

5 Ответственность за сохранность конфиденциальной информации при их передаче.

Литература: [15, с.144-160],[16, с. 114-122], [9, с.29-33].

3.5 - 3.6 Учет и регистрация отправляемых (исходящих) конфиденциальных документов, их экспедиционная обработка и рассылка

Учет и регистрация отправляемых конфиденциальных документов

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

– в журнале или карточке учета проектов внутренних (созданных/изданных) конфиденциальных документов;

– в журнале или карточке учета и распределения внутренних (созданных/изданных) конфиденциальных документов;

– в журнале инвентарного (выделенного) учета.

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.

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.

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.

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.

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. Аналогичные меры могут приниматься и в негосударственных организациях.

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.

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 такого сообщения, в порядке, установленном федеральными законами, иными нормативными правовыми актами или соглашением сторон, рассматривается как обмен документами». 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.

Вопросы для самоконтроля

1 Учет и регистрация отправляемых конфиденциальных документов.

2 Перечислите регистрационные формы при отправлении документов.

3 Экспедиционные технологии обработки и рассылки отправляемой конфиденциальной документированной информации.

4 Меры по защите конфиденциальной информации и ее носителейв процессе экспедиционной обработки.

5 Варианты упаковки конфиденциальных документов.

6 Разрешается ли пересылка конфиденциальной информации по каналам сетей электросвязи и электронной почты в виде электронных сообщений в сети Интернет? Обоснуйте.

Литература: [15, с.144-160],[16, с. 122-130], [9, с.29-33].

3.7 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.

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

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.

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. 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

Вопросы для самоконтроля

1 Какие конфиденциальные документы берутся на инвентарный (выделенный или списочный) учет?

2 Перечислите регистрационные формы при отправлении документов.

3 Экспедиционные технологии обработки и рассылки отправляемой

конфиденциальной документированной информации.

4 Меры по защите конфиденциальной информации и ее носителей в процессе экспедиционной обработки.

5 Варианты упаковки конфиденциальных документов.

6 Разрешается ли пересылка конфиденциальной информации по каналам сетей электросвязи и электронной почты в виде электронных сообщений в сети Интернет? Обоснуйте.

Литература: [15, с.144-160],[16, с. 122-130], [9, с.29-33].

3.8 Учет конфиденциальной информации при ее автоматизированной обработке

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».

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.

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.

Технологии ведения Реестра

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.

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.

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.

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.

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.

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.

Вопросы для самоконтроля

1 В чем выражаются особенности автоматизированного учета?

2 Что представляет собой Реестр конфиденциальной информации автоматизированной информационной системы?

3 Что является объектами учета Реестра?

4 Что подлежит учету?

5 Какие потоки конфиденциальной информации, циркулирующие в АИС выделяют в организации?

6 Технологии ведения Реестра.

Литература: [15, с.144-160],[16, с. 134-143], [9, с.29-33].

Тема 4 Разрешительная система доступа к конфиденциальной информации

4.1 - 4.2 Основные требования к разрешительной системе доступа

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 та-

кой информации. **Доступ к информации** – это возможность ее получения и использования. **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.

Разрешительная система должна предусматривать порядок доступа к конфиденциальной информации граждан, других должностных лиц и организаций, например, при выполнении совместных работ и услуг. 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. За разглашение или неправомерное использование содержащейся в документах конфиденциальной информации данные органы несут перед обладателем этой информации правовую ответственность.

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 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.

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.

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.

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.

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.).

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.).

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;

– организация работы по формированию и созданию Реестра конфиденциальной информации и автоматизированной информационной системы;

– 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;

– 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.

Вопросы для самоконтроля

1 Что относится к разрешительной системе конфиденциальной информации?
2 Что представляет собой Регламент конфиденциальной информации?
3 Какие требования предъявляются к разрешительной системе?
4 Значение ЭК при защите конфиденциальной информации?
5 Кто должен входить в состав ЭК?
6 Перечислите функции экспертной комиссии.

Литература: [15, с.144-160],[16, с. 141-148], [9, с.29-33].

4.3 Особенности доступа к конфиденциальной документированной информации, составляющей служебную, коммерческую, профессиональную тайны, секрет производства 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». 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.

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 конфиденциальности.

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.

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.

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.

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.

Вопросы для самоконтроля

1 Какие существуют виды договоров, регулирующих ограничение доступа к секрету производства и служебному секрету производства?

2 Кто такой контрагент?

3 Какие обязанности возложены на контрагента?

4 Существует ли ответственность за нарушение положений договора?

5 Как называется типовая форма составляется в приложении к Регламенту?

Литература: [15, с.73-119],[16, с. 148-153], [9, с.38-54].

4.4 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.

Вопросы для самоконтроля

1 Что такое предоставление конфиденциальной информации?
2 Кто такой обладатель конфиденциальной информации?
3 Особенность доступа к предоставляемой конфиденциальной информации.

Литература: [15, с.73-119],[16, с. 154-161], [9, с.38-54].

4.5 Особенности доступа к конфиденциальной документированной информации, составляющей персональные данные

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. 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;

– 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, а также в соответствии с уголовно-исполнительным законодательством Российской Федерации;

– 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.

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, об оперативно-розыскной деятельности, о государственной службе, о порядке выезда из Российской Федерации и въезда на ее территорию.

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;

– 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;

– 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].

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.

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).

Под целью обработки персональных данных понимаются как цели, указанные в учредительных документах оператора, так и цели фактически осуществляемой оператором деятельности по их обработке.

Вопросы для самоконтроля

1 Письменное согласие субъекта персональных данных на доступ.

2 Какая информация вносится в согласие субъекта персональных данных в письменной форме?

3 Уведомление об обработке персональных данных

Литература: [15, с.73-119],[16, с. 154-161], [9, с.38-54].

4.6 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».

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.

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 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).

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 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.

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.

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.

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).

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.

Вопросы для самоконтроля

1 Каковы особенности доступа к архивным конфиденциальным документам?

2 Кем осуществляется отмена ограничения доступа?
3 Каковы условия доступа к архивным конфиденциальным документам?
4 Каким документом определен доступ пользователей к архивным документам?
5 Ограничения на доступ к сведениям о частной жизни.

Литература: [15, с.73-119],[16, с. 161-166], [9, с.38-54].

4.7 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. 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 под-*

разделения. 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.

Вопросы для самоконтроля

1 Особенности доступа должностных лиц при их командировании.

2 Какие документы выдаются должностным лицам при их командировании к конфиденциальным документам?

3 Что такое предписание?

4 Кем осуществляется доступ к конфиденциальным документам?

Литература: [16, с. 166-168], [9, с.70-83].

4.8 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.

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.

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.

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 в журнале-картотеке. 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.

Вопросы для самоконтроля

1 Особенность информационного обслуживания пользователей.

2 Назовите иерархическую последовательность доступа к информации?

3 Кем и при каких условиях осуществляется выдача допуска или санкций (разрешений) на доступ к конфиденциальной информации?

4 Что из себя представляет номенклатура должностей работников?

5 В каких формах производится учет работников, пользующихся конфиденциальной информацией?

6 Какой документ оформляется при обнаружении факта утраты конфиденциальной документированной информации?

Литература: [16, с. 168-173], [9, с.70-83].

Тема 5 Составление номенклатуры дел, формирование и оформление конфиденциальных дел

5.1 – 5.2 Документальный фонд организации

Общие положения

Документальный фонд федерального органа исполнительной власти формируется в порядке, установленном Правительством Российской Федерации в Правилах делопроизводства и документооборота.

Требования, установленные в Правилах делопроизводства, могут распространяться и на негосударственные структуры. В связи с этим в данном документе 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 «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.

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. 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.

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.

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 – 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, Реестром конфиденциальной информации и автоматизированной информационной системы и классификатором конфиденциальной информации, 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. 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.

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.

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.

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.

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».

Вопросы для самоконтроля:

1 Как формируется документальный фонд федерального органа исполнительной власти?

2 Какие функции выполняет организация (государственные и негосударственные структуры) по поводу документального фонда?

3Каким образом осуществляется передача дел в Архив организации?

4Особенности учета конфиденциальных дел.

5 Составление номенклатуры конфиденциальных дел.

Литература: [16, с. 173-184], [9, с.86-125].

5.3 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 поступившие (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 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-скоросшивателях 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.

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. 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. 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.

Вопросы для самоконтроля

1 Как происходит группировка при формировании дел?

2По какому принципу документы систематизируются внутри дел?

3Вместо изъятых документов что помещается в дело?

4 Кто принимает решение вопроса о снятии отметки конфиденциальности с дел?

Литература: [16, с. 184-187], [9, с.86-125].

5.4 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.

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 самого 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.

Данные о документах вносятся в опись в момент подшивки документов.

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.

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.

Вопросы для самоконтроля

1 Что включает в себя оформление конфиденциального дела?

2Какая информация выносится на обложку дела?

3Что такое крайняя дата? Когда она проставляется?

4 В каком случае заводится карточка выдачи дела?

5 Какие требования предъявляются к формированию документов внутри дела?

Литература: [16, с. 187-193], [9, с.86-125].

Тема 6 Подготовка конфиденциальных документов для архивного

хранения или уничтожения

6.1 Экспертиза ценности конфиденциальных документов

Согласно Федеральному закону «Об архивном деле в Российской федерации», 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.

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, персональные данные государственных служащих.

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.

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.

Нормативным актом, регламентирующим хранение и отбор на хранение, а также уничтожение типовых документов, служит Перечень типовых управленческих документов с указанием сроков хранения.

Таким образом, перечни служат целям охраны, организации и качественного пополнения состава Архивного фонда Российской Федерации.

Срок хранения дела в целом устанавливается по наивысшему сроку хранения документов, находящихся в деле.

Результаты экспертизы ценности документов целесообразно фиксировать в рабочей карточке (тетради) эксперта с отражением в ней номера дела (документа выделенного хранения), его заголовка, 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 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.

Вопросы для самоконтроля

1 Согласно какого ФЗ проводится экспертиза ценности документа?

2 Что является источниками комплектования Архивного фонда Российской Федерации применительно к конфиденциальным документам?

3 С какой периодичностью должна проводиться экспертиза ценности документов?

4 Кем проводится ЭЦД?

5 Что является нормативным актом, регламентирующим хранение, отбор на хранение, а также уничтожение типовых документов?

Литература: [16, с. 193-197], [9, с.86-125].

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 перенумерацией 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;

– передача снятых с ограничения доступа дел и документов выделенного хранения по акту в Службу делопроизводства с отметкой в графе 9 номенклатуры дел;

– 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.

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.

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.

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 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.

Вопросы для самоконтроля

1 В каких случаях производится частичное переформирование и дооформление соответствующих дел и документов?

2 Какая информация входит в заверительную подпись.

3 Сколько экземпляров описей составляется?

Литература: [16, с.197-201],[9, с.127-211].

6.3-6.4 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. 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».

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.

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.

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.

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.

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 описях 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».

Вопросы для самоконтроля

1 Каким документом оформляется отбор документов и дел к уничтожению?

2В каком документе представлена форма акта?

3 С какими документами идет сверка перед уничтожением включенных в акт дел?

4 Какие требования должны соблюдаться перед уничтожением дел?

Литература: [16, с.201-211],[9, с.229-256].

Тема 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 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, 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.

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.

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.

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 кон-

фиденциальной 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.

Вопросы для самоконтроля

1 Кому возможна передача конфиденциальных документов?

2 На какой срок разрешается выдавать конфиденциальные документы для работы?

3 Что такое спецпортфель? Где хранится спецпортфель?

4 Какие требования предъявляются к рабочему месту сотрудника, работающего с конфиденциальными документами?

5 Что запрещается сотрудникам, работающим с конфиденциальной документированной информацией?

Литература: [16, с. 211-215], [9, с.218-227], [15, с.168-175].

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. 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 журнал передачи-приема под охрану помещений и пеналов с ключами.

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.

Ежегодно должна проводиться проверка фактического наличия ключей от хранилищ и номерных печатей исполнителей.

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.

Вопросы для самоконтроля

1 Какие требования предъявляются к помещению Службы делопроизводства?

2 Кто может допускаться в помещения, где хранятся конфиденциальные документы?

3 Где хранятся экземпляры ключей от сейфов, шкафов, стеллажей, решеток?

4 Какие правила существуют для эвакуации конфиденциальных документов и дел?

Литература: [16, с. 215-221], [9, с.218-227], [15, с.168-175].

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.

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.

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, подтверждающего полномочия лица, может вноситься в список непосредственно перед началом совещания. Эти документы передаются участниками совещания ответственному организатору для хранения в Службе делопроизводства.

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.

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.

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.

Вопросы для самоконтроля

1 Кто выдает разрешение на проведение совещаний и переговоров, использующих конфиденциальную информацию?

2 Как осуществляется допуск работников на совещания?

3 Кто несет ответственность за обеспечение защиты конфиденциальной информации?

4 Кто осуществляет подготовку конфиденциального совещания?

5 Какие требования предъявляются к помещению, где проводится конфиденциальное совещание?

6 Какие приборы должны находится в данном помещении?

7 Что не разрешается участникам конфиденциального совещания?

Литература: [16, с. 221-226], [9, с.218-227], [15, с.168-175].

7.5 Особенности конфиденциального электронного документооборота

Правительство Российской Федерации утвердило Положение о системе межведомственного электронного документооборота. Федеральная информационная система обеспечивает в автоматизированном режиме защищенный обмен электронными сообщениями, в том числе сообщениями, содержащими информацию, отнесенную к сведениям, составляющим служебную тайну.

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.

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.

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.

Правилами делопроизводства в федеральных органах исполнительной власти 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 позволяет идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

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.

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.

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. 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.

В случае возникновения необходимости размещения у участников дополнительных технических средств и (или) их переноса в другие помещения финансирова-

ние 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.

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.

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.

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».

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.

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.

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.

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.

Вопросы для самоконтроля

1 На каких два вида можно разделить электронный документооборот?

2 Что такое электронный документ? Из каких частей состоит электронный документ?

3 Электронная цифровая подпись.

4 Функции электронной цифровой подписи?

5 В чем заключается информационная безопасность?

6 Назовите технические и организационные мероприятия, относящиеся к информационной безопасности?

7 Основные виды угроз информационной безопасности организации.

Литература: [16, с. 226-237], [9, с.218-227], [15, с.168-175].

7.6-7.7 Основные требования и меры по защите конфиденциальной информации, циркулирующей в эксплуатируемой автоматизированной информационной системе

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.

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.

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, 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;

– 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.

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.

Особенности и основные требования защиты персональных данных в АИС

В соответствии со ст. 19 Федерального закона «О персональных данных» Правительство Российской Федерации своим постановлением установило требования к обеспечению безопасности персональных данных при их обработке в информационных системах. На основе данного постановления ФСТЭК России своим приказом 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.

Работы по обеспечению безопасности персональных данных при их обработке в АИС являются неотъемлемой частью работ по созданию этих систем (ГОСТ 34.601–90 и ГОСТ Р 51583–2000).

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.

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;

– 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;

– 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;

– 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 нарушению 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.

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 ин-

тересам 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.

Определяются следующие категории обрабатываемых в информационной системе персональных данных (Хпд):

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 Хнпд 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 системы, 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.

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 безопасности 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 для самоконтроля

1 Основные требования по защите конфиденциальной информации.

2 Какие мероприятия относятся мерам по защите конфиденциальной информации?

3 Что такое профиль защиты?

4 Какие особенности и основные требования защиты персональных данных в АИС?

5 В чем заключается информационная безопасность?

6 Какие исходные данные учитываются при проведении классификации персональных данных?

7 Какие категории обрабатываемых в информационной системе персональных данных существуют?

Литература: [16, с. 246-268], [9, с.218-227], [15, с.168-175].

7.8 Организация работ при создании системы защиты электронного документооборота

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.

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.

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.

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.

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 и Реестру конфиденциальной информации и АИС. 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 приемосдаточного акта, подписываемого разработчиком и заказчиком;

– аттестация АИС на соответствие требованиям безопасности информации.

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.

Вопросы для самоконтроля

1 Какие основные требования по разработке системы защиты информации.

2 Назовите и дайте характеристику стадиям и этапам разработки системы защиты конфиденциальной информации.

3 Какие существуют стадии создания системы защиты АИС и циркулирующей в ней конфиденциальной информации?

4 Какие особенности и основные требования защиты персональных данных в АИС?

5 В чем заключается информационная безопасность?

Литература: [16, с. 268-282], [9, с.218-227], [15, с.168-175].

7.9 Организация проведения работ по защите конфиденциальной информации при ее автоматизированной обработке

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.

Доступ пользователей к конфиденциальной информации осуществляется в соответствии с разрешительной системой допуска исполнителей к документам и сведениям конфиденциального характера, действующей в организации.

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.

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, магнитооптические, 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.

Вопросы для самоконтроля

1 Общие положения организации работы по защите конфиденциальной информации при ее автоматизированной обработке.

2 Требования по защите конфиденциальной информации при ее автоматизированной обработке.

3 Как называется документ, который предназначен для классификации и кодирования конфиденциальной информации?

4 Назовите блоки описания объекта классификации?

5 В чем выражаются особенности защиты конфиденциальной информации на автоматизированных рабочих местах на базе автономных персональных ЭВМ?

Литература: [16, с. 268-282], [9, с.218-227], [15, с.168-175].

4 Вопросы для подготовки к зачету (экзамену)

1 Основные понятия конфиденциального делопроизводства, принципы его построения.

2 Понятие и особенности конфиденциальной информации. Режим защиты, содержание и порядок действий, направленных на защиту информации.

3 Понятие государственной тайны. Нормативные основы организации работы с документами, содержащими государственную тайну.

4 Персональные данные.

5 Тайна следствия и судопроизводства.

6 Служебная тайна.

7 Профессиональная тайна.

8 Коммерческая тайна.

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

10 Ответственность за нарушение правил работы с конфиденциальными документами.

11 Особенности документирования конфиденциальной информации.

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

13 Перечни конфиденциальной информации и документов. Разработка Перечня конфиденциальной документированной информации.

14 Учет бумажных носителей конфиденциальной информации.

15 Учет проектов конфиденциальной документированной информации.

16 Особенности создания и изготовления конфиденциальных документов с помощью средств электронно-вычислительной техники, их печатания, тиражирования, размножения.

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

18 Особенности учета и регистрации конфиденциальной документированной информации.

19 Обработка поступающих конфиденциальных документов, их учет и регистрация.

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

21 Технологии исполнения и контроля за исполнением конфиденциальных документов.

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

23 Учет конфиденциальной документированной информации инвентарного (выделенного) хранения.

24 Учет конфиденциальной информации при ее автоматизированной обработке.

25 Основные требования к разрешительной системе доступа.

26 Особенности доступа к конфиденциальной документированной информации, составляющей служебную, коммерческую, профессиональную тайны, секрет производства и служебный секрет производства.

27 Особенности доступа к конфиденциальной документированной информации при ее предоставлении уполномоченным органам государственной власти.

28 Особенности доступа к конфиденциальной документированной информации, составляющей персональные данные.

29 Особенности доступа к архивным конфиденциальным документам.

30 Особенности доступа должностных лиц при их командировании к конфиденциальной документированной информации.

31 Учет персонала, получившего доступ к конфиденциальной документированной информации, и (или) лиц, которым она была передана или предоставлена.

32 Документальный фонд организации.

33 Формирование конфиденциальных дел.

34 Оформление конфиденциальных дел.

35 Экспертиза ценности конфиденциальных документов.

36 Подготовка конфиденциальных документов и дел для архивного хранения.

37 Подготовка конфиденциальных документов и дел к уничтожению.

38 Режим обмена конфиденциальной документированной информацией.

39 Режим сохранности конфиденциальных документов и дел.

40 Режим конфиденциальности при проведении совещаний и переговоров.

41 Проверка наличия носителей конфиденциальной информации.

42 Особенности конфиденциального электронного документооборота.

43 Основные требования и меры по защите конфиденциальной информации, циркулирующей в эксплуатируемой автоматизированной информационной системе.

44 Организация работ при создании системы защиты электронного документооборота.

45 Организация проведения работ по защите конфиденциальной информации при ее автоматизированной обработке.

Варианты контрольных работ

Вариант 1

1Понятие государственной тайны. Нормативные основы организации работы с документами, содержащими государственную тайну.

2 Организация проведения работ по защите конфиденциальной информации при ее автоматизированной обработке.

3 Характеристика Федерального закона «О персональных данных»

Вариант 2

1 Персональные данные.

2 Организация работ при создании системы защиты электронного документооборота.

3 Характеристика Федерального закона «О коммерческой тайне».

Вариант 3

1Тайна следствия и судопроизводства.

2 Основные требования и меры по защите конфиденциальной информации, циркулирующей в эксплуатируемой автоматизированной информационной системе.

3 Характеристика Федерального закона «Об информации, информационных технологиях и защите информации».

Вариант 4

1Служебная тайна.

2 Особенности конфиденциального электронного документооборота.

3 Характеристика Федерального закона «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства».

Вариант 5

1 Профессиональная тайна.

2 Проверка наличия носителей конфиденциальной информации.

3 Характеристика Федерального закона «О государственной тайне».

Вариант 6

1 Коммерческая тайна.

2 Режим конфиденциальности при проведении совещаний и переговоров.

3 Характеристика Федерального закона «Об обороне».

Вариант 7

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

2 Режим сохранности конфиденциальных документов и дел.

3ХарактеристикаПостановления Правительства Российской Федерации «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

Вариант 8

1Ответственность за нарушение правил работы с конфиденциальными документами.

2Режим обмена конфиденциальной документированной информацией.

3 Характеристика Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти

Вариант 9

1 Особенности документирования конфиденциальной информации.

2 Подготовка конфиденциальных документов и дел к уничтожению.

3 Характеристика Федерального закона «О службе в таможенных органах Российской Федерации».

Вариант 10

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

2 Подготовка конфиденциальных документов и дел для архивного хранения.

3 Характеристика Федерального закона«О Центральном банке Российской Федерации (Банке России)».

Вариант 11

1 Перечни конфиденциальной информации и документов. Разработка Перечня конфиденциальной документированной информации.

2 Экспертиза ценности конфиденциальных документов.

3 Характеристика Федерального закона«Об основах муниципальной службы Российской Федерации».

Вариант 12

1Учет бумажных носителей конфиденциальной информации.

2 Оформление конфиденциальных дел**.**

3 Характеристика основ Налогового кодекса.

Вариант 13

1Учет проектов конфиденциальной документированной информации.

2 Формирование конфиденциальных дел**.**

3 Характеристика Федерального закона «О почтовой связи».

Вариант 14

1Особенности создания и изготовления конфиденциальных документов с помощью средств электронно-вычислительной техники, их печатания, тиражирования, размножения.

2 Документальный фонд организации.

3 Характеристика Федерального закона «Об аудиторской деятельности».

Вариант 15

1Учет использования и хранения печатей, штампов, бланков, необходимых для оформления конфиденциальных документов.

2 Учет персонала, получившего доступ к конфиденциальной документированной информации, и (или) лиц, которым она была передана или предоставлена.

3 Характеристика Федерального закона «О противодействии легализации (отмыванию) доходов, полученных преступным путем»

Вариант 16

1 Особенности учета и регистрации конфиденциальной документированной информации.

2 Особенности доступа должностных лиц при их командировании к конфиденциальной документированной информации.

3 Характеристика Федерального закона «О страховании вкладов физических лиц в банках Российской Федерации».

Вариант 17

1 Обработка поступающих конфиденциальных документов, их учет и регистрация.

2 Особенности доступа к архивным конфиденциальным документам.

3 Характеристика Федерального закона «Об информации, информационных технологиях и защите информации».

Вариант 18

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

2 Особенности доступа к конфиденциальной документированной информации, составляющей персональные данные.

3 Характеристика Федерального закона «О коммерческой тайне».

Вариант 19

1 Технологии исполнения и контроля за исполнением конфиденциальных документов.

2 Особенности доступа к конфиденциальной документированной информации при ее предоставлении уполномоченным органам государственной власти.

3 Характеристика основ Трудового кодекса в области конфиденциальной информации.

Вариант 20

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

2 Особенности доступа к конфиденциальной документированной информации, составляющей служебную, коммерческую, профессиональную тайны, секрет производства и служебный секрет производства.

3 Характеристика основ Гражданского кодекса в области конфиденциальной информации.

Вариант 21

1 Учет конфиденциальной документированной информации инвентарного (выделенного) хранения.

2 Основные требования к разрешительной системе доступа.

3 Характеристика Федерального закона «О почтовой связи».

Вариант 22

1 Учет конфиденциальной информации при ее автоматизированной обработке.

2 Понятие государственной тайны. Нормативные основы организации работы с документами, содержащими государственную тайну.

3 Характеристика Федерального закона «О персональных данных».

Список рекомендуемых источников

Нормативно-правовые акты

1 Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) // Российская газета. 1993. № 237. 25 декабря.

2 Гражданский кодекс Российской Федерации (Ч. 4) от 18.12.2006 5. № 230-ФЗ // Собрание законодательства Российской Федерации. 2006. № 52 (Ч. 1). Ст. 5496.

3 Трудовой кодекс Российской Федерации от 30.12.2001 г. № 197-8. ФЗ // Собрание законодательства Российской Федерации. 2002, № 1 (Ч. 1), Ст. 3.

4 Кодекс Российской Федерации об административных право-9. нарушениях от 30.12.2001 № 195-ФЗ // Собрание законодательства Российской Федерации. 2002. № 1 (Ч. 1). Ст. 1.

5 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.

6 Федеральный закон 27.07.2006 № 152-ФЗ «О персональных данных» // Российская газета. 2006. № 165.

7 Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Российская газета. 2006. № 165.

8 Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» (ред. 24.07.2007) // Парламентская газета. 2004. № 144.

9 Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» // 32. Российская газета. 2003. № 135.

10 Федеральный закон от 10.01.2002 № 1-ФЗ «Об электронной цифровой подписи» // Российская газета. 2002. № 6.

11 Федеральный закон от 08.08.2001 № 128-ФЗ «О лицензировании отдельных видов деятельности» // Российская газета. 2001. № 153-154.

12 Федеральный закон от 07.08.2001 № 119-ФЗ (ред. от 01.07.2010) 40. «Об аудиторской деятельности» // Российская газета. 2008. № 267.

13 Федеральный закон от 17.07.1999 № 176-ФЗ «О почтовой связи» // Собрание законодательства Российской Федерации. 1999. № 29. Ст. 3697.

14 Федеральный закон от 26.09.1997 № 125-ФЗ «О свободе совести и о религиозных объединениях» // Собрание законодательства Российской Федерации. 1997. № 39. Ст. 4465.

15 Закон Российской Федерации от 21.07.1993 № 5485-1 «О государственной тайне» // Собрание законодательства Российской Федерации. 1997. № 41. С. 8220–8235.

16 Указ Президента Российской Федерации 17.03.2008 59. № 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.

17 Указ Президента Российской Федерации от 30.05.2005 № 609 61. «Об утверждении Положения о персональных данных государственного гражданского служащего и ведение его личного дела» // Собрание законодательства Российской Федерации. 2005. № 23. Ст. 2242.

18 Постановление Правительства Российской Федерации от 78. 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.

19 Постановление Правительства Российской Федерации от 79. 06.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных вне информационных систем» // Российская газета. 2008. № 148.

Основная литература

1 Алексенцев А.И. Конфиденциальное делопроизводство / А.И. Алексенцев. – М.: Бизнес-школа «Интел-Синтез», 2019.

2 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».

3 Белопушкин В.И., Кириллычев А.Н. Правовые аспекты обеспечения информационной безопасности / В.И. Белопушкин, А.Н. Кириллычев. – М.: Изд-во МГТУ, 2019.

4 Бардаев Э.А. Документоведение: учеб. для вузов по специальностям «Организация и технология защиты информации» и «Комплексная защита объектов информации» / Э. А. Бардаев, В. Б. Кравченко, -2-е изд. Стер. –М.: Академия, 2018. – 300.

5 Говорухин О.Э. Служебная тайна // Служба кадров и персонал. – М.: ВНИИДАТ, 2016. № 4.

6 Говорухин О.Э. Когда персональные данные – коммерческая тайна // Служба кадров и персонал. 2016. № 7.

7 Говорухин О.Э. Служебная и профессиональная тайна // Делопроизводство. 2016. № 3.

8 Демушкин А.С. Документы и тайна / А.С. Демушкин. – М.: Городец-издат, 2018.

9 Демушкин А.С. Организация работы с документированной информацией ограниченного доступа // Делопроизводство. 2019. № 1.

10 Демушкин А.С. Организация работы с документами ограниченного доступа // Отечественные архивы, 2018.

11 Демушкин А.С. Классификация тайн // Секретарское дело. 2019. № 12.

12 Демушкин А.С. Документы и коммерческая тайна // Служба кадров и персонал. 2019. № 12.

13 Демушкин А.С. Защита коммерческой тайны: опыт США // Служба кадров и персонал. 2005. № 7. 242. Демушкин А.С. «Электронный чиновник» // Делопроизводство. 2018. № 4.

14 Куняев Н. Н. Документоведение: учеб. для вузов по специальности "Документоведение и документационное обеспечение управления" / Н. Н. Куняев, Д. Н. Уралов, А. Г. Фабричнов ; под ред. Н. Н. Куняева, -М.: Логос, 2018. – 348 с.

15 Куняев Н.Н. Конфиденциальное делопроизводство и защищенный электронный документооборот: учебник / Н.Н. Куняев, А.С. Дёмушкин, А.Г. Фабричнов; под общ. ред. Н.Н. Куняева. – М.: Логос, 2018. – 452 с.

16 Некраха А.В., Шевцова Г.А. Организация конфиденциального делопроизводства и защиты информации. – М.: Академический проект, 2017.

17 Погуляев В.В., Моргунова Е.А. Комментарий к Федеральному закону «Об информации, информатизации и защите информации» / В.В. Погуляев, Е.А. Моргунова. – М.: Юстицинформ, 2017.

18 Ярочкин В.И. Безопасность информационных систем / В.И. Ярочкин. – М.: Ось, 2016.