Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет»

Кафедра вычислительной техники и защиты информации

ЗАЩИТА И ОБРАБОТКА КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ

Методические указания

Составитель:
Е.В. Бурькова

Рекомендовано к изданию редакционно-издательским советом федерального государственного бюджетного образовательного учреждения высшего образования «Оренбургский государственный университет» для обучающихся по образовательной программе высшего образования по направлению подготовки 10.03.01 Информационная безопасность

Оренбург
2020

УДК 342.7
ББК 67.401 я7
340

Рецензент – кандидат технических наук А.А. Рычкова

340 Защита и обработка конфиденциальных документов: методические указания / составитель Е.В. Бурькова; – Оренбургский гос. ун-т. – Оренбург: ОГУ, 2020. – 59 с.

Методические указания содержат теоретические сведения и рекомендации по выполнению лабораторных работ по дисциплине «Защита и обработка конфиденциальных документов».

Методические указания предназначены для обучающихся по образовательной программе высшего образования по направлению подготовки 10.03.01 Информационная безопасность.

УДК 342.7
ББК 67.401 я7

Содержание

Введение

Проблемы обеспечения информационной безопасности становятся все более сложными и значимыми, находятся в центре внимания государства. В условиях постоянно меняющейся ситуации информационных угроз, стали востребованы новые знания и умения в сфере информационной безопасности. Требования, предъявляемые работодателями к специалисту в области информационной безопасности, достаточно высокие сегодня востребованы кадры нового поколения, способные быстро адаптироваться к постоянно изменяющимся угрозам информационной безопасности, обладающие высоким уровнем профессиональной компетентности.

Для обеспечения высокого качества подготовки специалистов в области информационной безопасности в университете должны быть реализованы следующие основные принципы:

− активное взаимодействие с работодателями сферы информационной безопасности как при разработке содержательной части образовательных программ, так и выполнении совместных проектов, предоставлении своей производственной базы для реализации практических задач;

− ориентация образовательного процесса на динамичные изменения профессиональной среды, синхронизацию с потребностями региона;

− усиление внимания на изучении нормативно-законодательных документов, национальных и международных стандартов в сфере обеспечения информационной безопасности;

− приобретение практических навыков использования средств защиты информации в условиях современных угроз информационной безопасности.

Данные методические указания содержат теоретические сведения и рекомендации по выполнению лабораторных работ по дисциплине «Защита и обработка конфиденциальных документов» и предназначены для обучающихся по образовательной программе высшего образования по направлению подготовки 10.03.01 Информационная безопасность.

Основные понятия и определения

Адекватность информации - это определенный уровень соответствия создаваемого с помощью полученной информации образа реальному объекту, процессу, явлению и т.п. Адекватность информации может выражаться в трех формах: семантической, синтаксической, прагматической.

Полнота - это соотношение между всей имеющейся информацией по проблеме и информацией, доступной пользователю (т.е. той частью, которую он может получить).

Аутентичность – гарантия того, что источником информации является именно то лицо, которое заявлено как ее автор; нарушение этой категории также называется фальсификацией, но уже автора сообщения.

Безопасность информации - состояние защищенности данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность информации при обработке в информационных системах.

Документ - зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

Документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством РФ случаях ее материальный носитель.

Достоверность информации – показатель качества информации, означающий её полноту и общую точность, свойство информации быть правильно воспринятой.

Доступность информации - состояние информации, при котором субъекты, имеющие право доступа, могут реализовывать их беспрепятственно.

Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

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

Информационная система - это система, представляющая собой совокупность данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких данных с использованием средств автоматизации или без использования таких средств.

Информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Источник информации – субъекты и объекты, от которых может быть получена информация с характеристиками, позволяющими оценить ее достоверность.

Источник угрозы безопасности информации - это субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации.

Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определённой информации, требование не передавать такую информацию третьим лицам без согласия её обладателя.

Конфиденциальность информации — принцип аудита, заключающийся в том, что аудиторы обязаны обеспечивать сохранность документов, получаемых или составляемых ими в ходе аудиторской деятельности, и не вправе передавать эти документы или их копии каким бы то ни было третьим лицам, либо разглашать устно содержащиеся в них сведения без согласия собственника экономического субъекта, за исключением случаев, предусмотренных законодательными актами.

Конфиденциальная информация - информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации и представляет собой коммерческую, служебную или личную тайны, охраняющиеся её владельцем.

Конфиденциальность информации — принцип аудита, заключающийся в том, что аудиторы обязаны обеспечивать сохранность документов, получаемых или составляемых ими в ходе аудиторской деятельности, и не вправе передавать эти документы или их копии каким бы то ни было третьим лицам, либо разглашать устно содержащиеся в них сведения без согласия собственника экономического субъекта, за исключением случаев, предусмотренных законодательными актами.

Модель угроз (безопасности информации) - физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации.

Нарушитель — лицо, пытающееся проникнуть или проникшее в помещение (на территорию), защищенное системой охранной или охранно-пожарной сигнализации без разрешения ответственного лица, пользователя, владельца, а также лицо, оказывающее ему содействие в этом.

Несанкционированное действие - хищение или попытка хищения носителей конфиденциальной информации и материальных средств предприятия, осуществление или попытка осуществления несанкционированного доступа, проноса (провоза) запрещенных предметов, совершения диверсии, вывода из строя средств физической защиты.

Несанкционированный доступ - проникновение лиц, не имеющих права доступа, в охраняемые зоны, на объекты, в служебные помещения предприятия.

Носитель информации - материальный объект, специально предназначенный для записи, хранения и передачи информации.

Носитель информации - физическое лицо или материальный объект, в том числе физическое поле, о котором информация находит свое отображение в виде

символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Разрешительная система доступа к конфиденциальным документам представляет собой совокупность установленных руководством предприятия нормативных положений, обеспечивающих обоснованный и правомерный доступ пользователей к необходимому им для выполнения служебных обязанностей объему конфиденциальных документов.

Угроза – это совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности защищаемого объекта.

Уязвимость - это слабое место в системе защиты объекта, обусловливающее возможность реализации угроз безопасности.

Целостность информации – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

Электронные ресурсы – разновидность информационных ресурсов, для создания, сбора, хранения, обработки, поиска, вывода, копирования, передачи и распространения которых необходимы средства вычислительной техники и системы связи.

Электронный документ – ограниченный и завершенный на конкретный момент времени массив информации, зафиксированный на физическом носителе в виде файла (набора файлов) с едиными техническими и общими содержательными характеристиками.

1 Лабораторная работа 1. Нормативно-правовые основы защиты конфиденциальных документов

1.1 Цель работы

- Анализ структуры и деятельности объекта защиты;
- Изучение нормативно-правовой базы по защите конфиденциальных документов.

1.2 Теоретические сведения

Информация – сведения (сообщения, данные) независимо от формы их представления. Обладателем информации является лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

Доступ к информации – это возможность получения информации и еѐ использование. Информация может являться объектом публичных, гражданских и иных правовых отношений. Информация может свободно использоваться любым лицом и передаваться одним лицом другому лицу, если федеральными законами не установлены ограничения доступа к информации либо иные требования к порядку ее предоставления или распространения.

Конфиденциальность информации — обязательное для выполнения лицом, получившим доступ к определённой информации, требование не передавать такую информацию третьим лицам без согласия её обладателя.

Указ Президента РФ N 188 «Об утверждении перечня сведений конфиденциального характера» содержит список информации, которая может быть отнесена к конфиденциальной:

*1) **персональные данные;***

*2) **тайна следствия и судопроизводства;***

3) ***служебная тайна*** *(с*лужебные сведения, доступ к которым ограничен органами государственной власти в соответствии с гражданским кодексом Российской Федерации и ФЗ*;*

4) ***профессиональная тайна*** (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее)*;*

5) ***коммерческая тайна****;*

6) ***сведения о сущности изобретения****;*

7) ***сведения, содержащиеся в личных делах осужденных***, а также сведения о принудительном исполнении судебных актов, актов других органов и должностных лиц.

Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на **доступ** к информации.

Для выполнения задачи защиты конфиденциальных документов на предприятии необходимо провести изучение организационной структуры предприятия, построение иерархической структурной схемы всех подразделений; изучение деятельности, осуществляемой на предприятии; построение перечня основных задач; проведение анализа информационных процессов на предприятии. Изучить характеристики защищаемой информации предприятия, правила разграничения доступа к защищаемой информации на предприятии. Изучение организационной структуры предприятия необходимо для определения места заданного защищаемого объекта (подразделения) в общей структуре.

В результате изучения деятельности предприятия и решаемых задач строят перечень документированной информации ограниченного доступа.

Конфиденциальные документы должны издаваться только при действительной необходимости в письменном удостоверении наличия и содержания управленческих, производственных и иных действий, передаче информации, хранении и использовании ее в течение определенного времени и в определенном количестве экземпляров.

Обязательность письменного удостоверения информации закрепляется перечнем издаваемых предприятием конфиденциальных документов, где также указываются конкретные лица, имеющие право составлять и подписывать (утверждать) документы. Перечень издаваемых конфиденциальных документов разрабатывается только на основе и в рамках перечня сведений, составляющих коммерческую тайну.

Перечень сведений, составляющих коммерческую тайну, разрабатывается для каждого предприятия самим предприятием – обладателем (собственником) информации. Разработкой перечня сведений, составляющих коммерческую тайну, должна заниматься **постоянно действующая экспертная комиссия (*ПДЭК)***.

Конфиденциальность является правовой формой и одновременно инструментом обеспечения неизвестности информации. Законодательством введены два ограничения на отнесение информации к коммерческой тайне:

− к коммерческой тайне не может быть отнесена информация, составляющая государственную тайну;

− к коммерческой тайне нельзя относить информацию, которая должна быть общедоступной в целях предупреждения сокрытия правонарушений и предотвращения нанесения ущерба законным интересам государства, физических или юридических лиц.

1.3 Задание

1.3.1 Построить схему организационной структуры объекта защиты. Провести анализ деятельности для заданного объекта информатизации. Составить перечень решаемых задач, оформить в виде таблицы. Пример организационной структуры предприятия представлен на рисунке 1.1

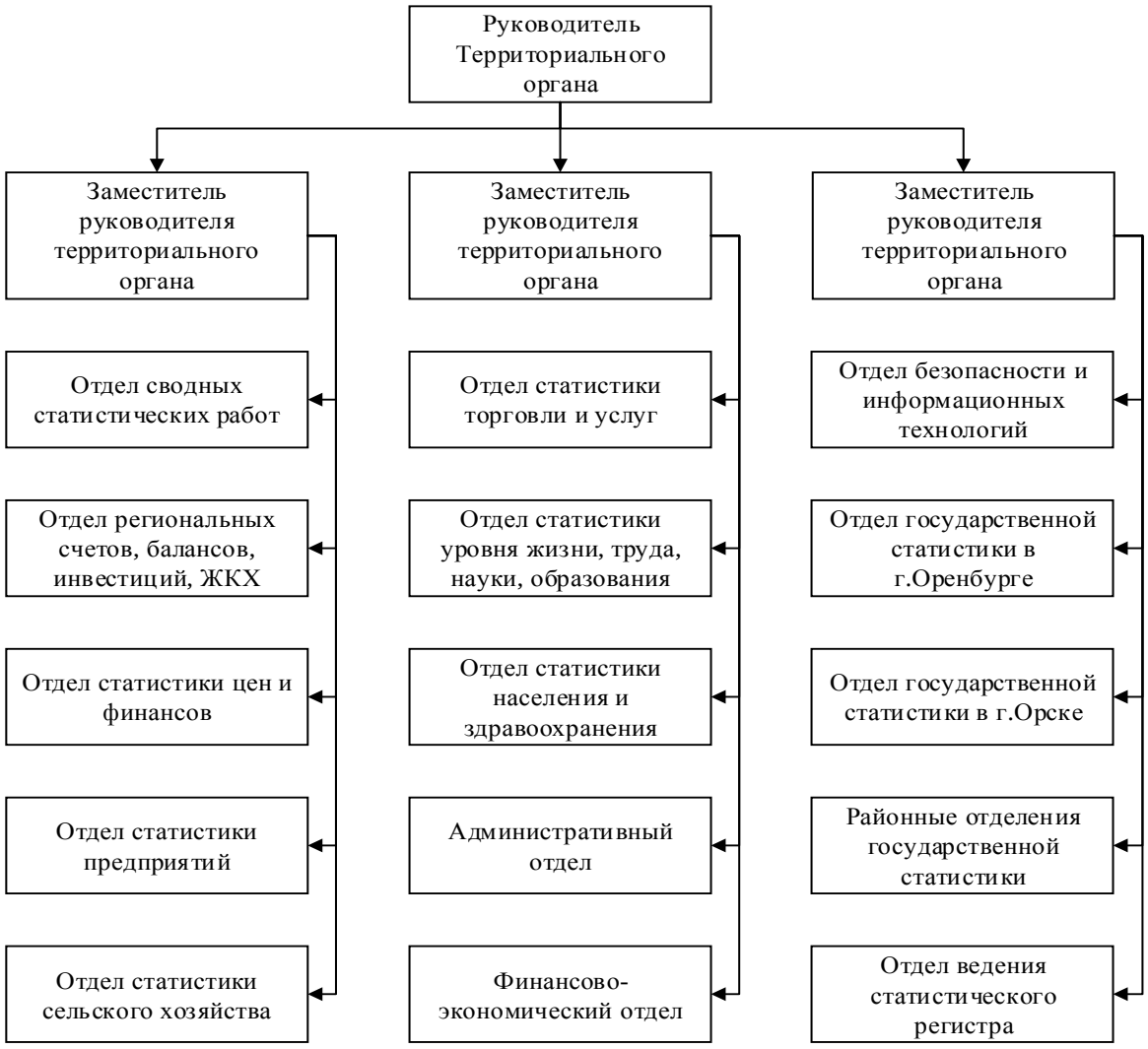

Рисунок 1.1 – Схема организационной структуры предприятия

Пример оформления информации о решаемых задачах предприятия приведен в таблице 1.1.

Таблица 1.1 – Описание деятельности подразделений объекта защиты

Наименование отдела	Решаемые задачи
1	2
Отдел статистики торговли и услуг	Формирует статистическую информацию об экономических процессах в Оренбургской области по торговле и услугам для последующего представления в установленном порядке в Росстат

Продолжение таблицы 1.1

1	2
Отдел безопасности и информационных технологий	Внедряет информационные технологии в работу организации, с целью создания интегрированных информационных ресурсов государственной статистики и организации доступа к ним на основе использования технологий хранилищ данных, а также обеспечение информационной безопасности информационных технологий

1.3.2 Создать перечень всей документированной информации заданного объекта (без учета грифа конфиденциальности). Определить виды носителей информации. Определить виды тайн для документированной информации заданного объекта. Результаты занести в таблицу 1.2.

Таблица 1.2 – Анализ документированной информации объекта

Наименование документированной информации	Вид тайны	Носитель информации
Трудовой договор с сотрудниками	*ПДн*	*Бумажный*
Договор о поставке оборудования	*Коммерческая тайна*	*Бумажный, электронный*
Приказ о разграничении прав доступа к конфиденциальной информации	*Служебная тайна*	*Бумажный, электронный*
Заполнить	*Заполнить*	*Заполнить*
Заполнить	*Заполнить*	*Заполнить*
Заполнить	*Заполнить*	*Заполнить*
Заполнить	*Заполнить*	*Заполнить*

1.3.3 Провести анализ нормативно-правовых документов по защите конфиденциальных документов на данном объекте информатизации, учитывая разделение на документы федерального уровня и внутреннего уровня предприятия. Результаты занести в таблицу 1.3.

Таблица 1.3 – Анализ нормативно-правовой базы защиты конфиденциальных документов

Вид документа	Название нормативного документа	Краткое пояснение
Федеральные	Постановление Правительства Российской Федерации N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»	Настоящий документ устанавливает требования к защите персональных данных при их обработке в информационных системах персональных данных и уровни защищенности таких данных.
	Заполнить	*Заполнить*
	Заполнить	*Заполнить*
Внутренние	*Приказ о разграничении прав доступа к конфиденциальной информации*	*Заполнить*
	Политика безопасности предприятия	
	Заполнить	*Заполнить*
	Заполнить	*Заполнить*

В таблице 1.4 Приведены варианты объектов защиты.

Таблица 1.4 - Варианты объектов защиты

№ варианта	Объект информатизации
1	2
1	администрация завода железобетонных изделий
2	офис торговой фирмы
3	поликлиника
4	детский сад
5	научно-производственное предприятие
6	фармацевтическая фирма
7	ИП «Проектирование и монтаж систем охранной сигнализации»

Продолжение таблицы 1.4

1	2
8	Филиал банка
9	патентное бюро
10	редакция научного журнала
11	склад лекарственных средств
12	склад текстильной продукции
13	студия дизайна
14	нотариальная контора
15	администрация птицефабрики
16	республиканская библиотека
17	музей изобразительных искусств
18	общеобразовательная школа
19	больница
20	районный суд
21	ИП «Изготовление и установка пластиковых окон»
22	ИП «Проектирование и монтаж систем пожарной сигнализации»
23	спортивный комплекс
24	ИП «Изготовление детского игрового оборудования»
25	ИП Продовольственный магазин
26	рекламное агентство
27	медицинская лаборатория
28	почтовое отделение
29	отдел научных исследование университета
30	избирательная комиссия

1.4 Контрольные вопросы

1 Определение понятий «информация», «информационные технологии», «информационные системы», «оператор информационной системы».

2 Дать определение понятия «конфиденциальный документ».

3 Определение свойств информации «конфиденциальность», «целостность», «доступность».

4 Дать определение понятия «конфиденциальное делопроизводство».

5 Условия, при которых информация может быть отнесена к конфиденциальной. Назвать нормативный документ.

6 Дать определение понятий «документ», «документированная информация», «электронный документ», «носитель информации».

7 Дать определение понятий «защищаемая информация», «обладатель информации», «предоставление», «распространение» информации.

8 На что направлены меры по защите конфиденциальной информации? Нормативный документ, в котором определены цели защиты информации.

9 Дать характеристику сведений конфиденциального характера. Указать нормативный документ, перечислить все виды конфиденциальной информации.

10 Какая информация составляет коммерческую тайну. Привести примеры. Нормативный документ.

11 Что такое государственная тайна, какие сведения составляют государственную тайну? Нормативный документ. Назвать грифы документов.

12 Служебная тайна, определение. Какая информация относится к служебной тайне. Нормативный документ.

13 Какая информация составляет профессиональную тайну. Привести примеры. Нормативный документ.

14 Персональные данные, определение, примеры. Основной нормативный документ по защите ПДн, пояснения по разделам документа.

15 Что такое интеллектуальная собственность. Привести примеры. Указать и пояснить нормативный документ.

2 Лабораторная работа № 2. Определение состава конфиденциальных документов

2.1 Цель работы

- Определение состава конфиденциальных документов;
- Освоение навыков разработки проектов конфиденциальных документов.

2.2 Теоретические сведения

Состав документируемой конфиденциальной информации зависит от компетенции и функций предприятия, характера его деятельности, взаимосвязей с другими предприятиями, порядка разрешения вопросов. В свою очередь, этот состав влияет на качество соответствующей области деятельности, организацию и надежность обработки и защиты документов.

Обязательность письменного удостоверения информации закрепляется **перечнем издаваемых предприятием конфиденциальных документов.** Целями разработки такого перечня должны являться не только определение состава издаваемых документов, необходимых и достаточных для деятельности предприятия, но и установление конкретных лиц, имеющих право составлять и подписывать (утверждать) документы, а также предотвращение необоснованной рассылки документов.

Перечень издаваемых конфиденциальных документов разрабатывается только на основе и в рамках перечня сведений, составляющих коммерческую тайну. Поэтому определение состава издаваемых конфиденциальных документов должно начинаться с разработки перечня сведений, составляющих коммерческую тайну. **Перечень сведений, составляющих коммерческую тайну;** разрабатывается для каждого предприятия самим предприятием - обладателем (собственником) информации. Это вытекает из действующего законодательства, которым установлено, что состав и объем таких сведений определяется обладателем информации.

Разработкой перечня сведений, составляющих коммерческую тайну, должна заниматься постоянно действующая экспертная комиссия.

На первом этапе работы на основе анализа задач, функций, компетенции, направлений деятельности предприятия необходимо установить весь состав циркулирующей на предприятии информации, отображенной на любом носителе, любым способом и в любом виде, а также с учетом перспектив развития предприятия и его взаимоотношений с партнерами определить характер дополнительной информации, которая может возникнуть в результате деятельности предприятия. Эта информация классифицируется по тематическому признаку.

На втором этапе определяется, какая из установленной информации должна быть конфиденциальной и отнесена к коммерческой тайне. Базовым критерием при этом является возможность получения преимуществ от использования информации за счет неизвестности ее третьим лицам. Этот критерий имеет две составляющие: неизвестность информации третьим лицам и получение преимуществ в силу этой неизвестности. Конфиденциальность является правовой формой и одновременно инструментом обеспечения неизвестности информации.

Степень конфиденциальности – это показатель уровня закрытости информации.

Уровень закрытости зависит от величины ущерба, который может наступить при утечке информации. Чем больше этот ущерб, тем выше должна быть и степень конфиденциальности.

Наиболее распространенным является деление информации на две степени:

- конфиденциально
- строго конфиденциально.

Гриф конфиденциальности – это реквизит, свидетельствующий о степени конфиденциальности сведений, содержащихся в их носителе, проставляемый на самом носителе и (или) в сопроводительной документации на него. Наименование грифа должно соответствовать наименованию степени конфиденциальности.

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 перечнем сведений, составляющих коммерческую тайну. Перечень подписывается председателем и всеми членами ПДЭК, утверждается и вводится в действие приказом руководителя предприятия.

В приказе должны быть определены мероприятия по обеспечению функционирования перечня и контролю его выполнения. С приказом и перечнем необходимо ознакомить под расписку всех сотрудников предприятия, работающих с конфиденциальной информацией. Копии перечня или выписки из него должны быть направлены (под расписку) конфидентам (владельцам) 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 перечня могут осуществляться с разрешения руководителя предприятия и вноситься за подписями руководителя подразделения по принадлежности сведений и руководителя службы безопасности. При существенном изменении состава сведений перечень должен составляться заново.

После установления состава документов определяются круг лиц, имеющих право составлять и подписывать (утверждать) каждый вид документа, а также предприятия, которым данный документ должен направляться.

К числу документов, подлежащих утверждению в соответствии с существующими нормативными актами, относятся: уставы, положения о представительствах, филиалах и структурных подразделениях предприятия,

структура, штатное расписание, должностные инструкции, акты проверок (ревизий) сметы, расценки на проведение работ и оказание услуг и др.

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

Внесение возможных последующих частичных уточнений или изменений в перечень может быть возложено на руководителя службы безопасности.

При изменении перечня сведений, составляющих коммерческую тайну, соответствующие изменения вносятся и в перечень издаваемых конфиденци-альных документов. О снятии грифа конфиденциальности с отправленных документов должны быть письменно оповещены предприятия-адресаты.

В случаях возникновения необходимости издания разовых документов, не включенных в перечень, или дополнительных, не предусмотренных перечнем экземпляров документов, их изготовление может производиться по совместному разрешению руководителей соответствующего подразделения и службы безопасности. Одновременно определяется целесообразность включения таких документов (дополнительных экземпляров) в перечень.

2.3 Задание

2.3.1 Разработать перечень сведений, относящихся к конфиденциальной информации. Для выполнения этого задания необходимо использовать перечень всей циркулирующей на предприятии документации, составленный в работе № 1, распределить все виды документов по видам тайн, к которым они могут относиться. Выделить перечень общедоступных документов организации.

2.3.2 Выделить список документов относящихся к коммерческой тайне. Установить для каждого документа степень конфиденциальности и срок конфиденциальности. Результаты занести в таблицу 2.1.

Таблица 2.1 – Перечень сведений, составляющих коммерческую тайну

Номер по порядку	Наименование сведений	Степень конфиденциальности	Срок конфиденциальности
заполнить	*заполнить*	*заполнить*	*заполнить*

2.3.3 Установить круг лиц, имеющих право составлять и подписывать каждый вид документа и предприятия, которым данный документ должен направляться. Заполнить таблицу 2.2.

Таблица 2.2 – Перечень издаваемых конфиденциальных документов и круг лиц, имеющих определенные права

Номер по порядку	Наименование документа	Гриф конфиденциальности	Срок конфиденциальности	ФИО лиц, имеющих право составлять документы	ФИО лиц, имеющих право подписывать документы	Количество изготовляемых документов	Куда отправляются
1	2	3	4	5	6	7	8

2.3.4 Определить все носители конфиденциальной информации. Подготовить таблицу учета носителей по образцу таблицы 2.3.

Таблица 2.3 - Учет носителей конфиденциальной информации

Учетный номер и гриф конфиденциальности	Дата регистрации	Вид носителя	Наименование или назначение	Количество листов	ФИО лица получившего	Подпись за получен	Подпись за возврат	Отметка об уничтожении
1К	12.09.19	бланк	Для письма	1	Иванов В.И.	Иванов 13.09.19	Петров 13.09.19	-

2.4 Контрольные вопросы

1 Какие факторы влияют на определение состава документируемой конфиденциальной информации?

2 На основе какого документа разрабатывается перечень издаваемых конфиденциальных документов? Дать описание.

3 Какой орган уполномочен заниматься разработкой перечня сведений, составляющих коммерческую тайну? Каким образом создается этот орган и кто входит в его состав?

4 Какие ограничения на отнесение информации к коммерческой тайне введены законодательством? Какая информация не может быть отнесена к коммерческой тайне?

5 Дать определение понятия «степень конфиденциальности»? Назовите существующие степени конфиденциальности. Что такое уровень закрытости информации, чем он определяется?

6 Каковы этапы определения перечня конфиденциальной информации на объекте? Какие документы должны быть оформлены по результатам составления перечня?

7 Каким образом определяется срок конфиденциальности информации?

8 На кого возлагается ответственность за внесение возможных последующих частичных уточнений или изменений в перечень конфиденциальных документов?

9 Каковы условия издания конфиденциальных документов?

10 Что необходимо учитывать при переводе информации в разряд коммерческой тайны?

3 Лабораторная работа № 3. Изучение документопотоков

3.1 Цель работы

- Определение состава внутреннего и внешнего документопотоков;
- Освоение навыков оформления журналов документопотоков.

3.2 Краткие теоретические сведения

Под документопотоком понимается структурированная совокупность перемещаемых в заданном направлении документов (документированной информации), предназначенных для обеспечения выполнения персоналом управленческих функций и принятия решений.

Под внутренним документооборотом понимается движение документов внутри учреждения, фирмы с момента их создания или получения до завершения исполнения или отправления.

Под внешним документооборотом понимается движение документов между учреждениями, организациями и предприятиями.

Целью документооборота является информационное обеспечение управленческой деятельности, т. е. своевременная доставка ценной, полезной, своевременной, полной и достоверной информации руководителям и специалистам учреждения, фирмы, необходимой им для выполнения возложенных на них функций, принятия решений и фактического претворения их в жизнь. Основной характеристикой движения документированной информации является целевая комплексность документооборота, т. е. соединение в единую совокупность его управленческой, делопроизводственной и почтовой функций.

К документообороту предъявляется ряд принципиальных требований:

1) прямоточность движения документов, прохождение документов до потребителя информации (исполнителя) кратчайшим путем через наименьшее количество пунктов (инстанций), исключающее или сводящее к минимуму

возвратные перемещения документов;

2) избирательность распределения документов между руководителями и специалистами в соответствии с их функциональными обязанностями;

3) обусловленность перемещения документов деловой необходимостью, исключение лишних, дублирующих инстанций и действий;

4) единообразие маршрута движения и состава технологических

процедур и операций для массовых категорий документов, однократность выполнения каждой процедуры;

5) приспособленность организационной и технологической характеристик документооборота к новой информационной технологии, регламентирующей состав и назначение автоматизированных рабочих мест и баз данных, способы и условия передачи информации между центральной и локальными базами данных.

Документооборот делится на несколько составляющих его частей – документопотоков:

1) поток поступающих документов (входной, входящий документопоток);

2)поток отправляемых документов (выходной, исходящий документопоток);

3) поток внутренних документов (внутренний документопоток).

Последние два потока характеризуются значительным технологическим единообразием и могут рассматриваться как единый поток или документопоток подготовленных и изданных документов. **Входной документопоток** несет исходную (первичную) информацию и включает документы вышестоящих органов управления. **Выходной документопоток** несет информацию, выработанную в процессе функционирования органа управления в целях ее передачи (отправления) вышестоящим или нижестоящим организациям, неподчиненным учреждениям, гражданам.

Внутренний документопоток обеспечивает решение задач и реализацию функций в пределах данного аппарата управления без направления информации за его пределы. Как правило, в этом потоке решается задача правового и информационного обеспечения принимаемых решений. Во внутренний документопоток не включаются письма, так как переписка между структурными

подразделениями не разрешается.

Документопоток разбивается на достаточно автономные и законченные технологические стадии (этапы). **Стадия** состоит из совокупности технологических процедур.

Входной документопоток содержит следующие стадии:

- прием и первичная обработка документов;
- предварительное рассмотрение и распределение документов;
- регистрация документов и формирование справочно-информационного банка данных по документам;
- рассмотрение документов руководителем и передача их сотрудникам для исполнения, ознакомления или использования в работе;
- исполнение, использование документов или ознакомление персонала с документами.

Выходной и внутренний документопотоки включают следующие стадии обработки:

- исполнение документов;
- контроль за исполнением документов и поручений;
- регистрация изданных отправляемых и внутренних документов, формирование справочно-информационного банка данных по документам;
- отправка документов, передача внутренних документов на рассмотрение и исполнение;
- систематизация исполненных документов;
- оформление, формирование и хранение дел;
- передача дел в архив;
- уничтожение документов и дел с истекшими сроками хранения.

Документопотоки организовываются на основе централизованной, децентрализованной или смешанной системы обработки документов.

Централизованная система предполагает концентрацию всех стадий, процедур и операций по обработке и хранению документов в единой для учреждения, фирмы службе ДОУ.

При смешанной системе одна часть стадий (например, прием документов, их отправка, контроль над исполнением, ознакомление с документами персонала и др.) осуществляется централизованно, а другая (регистрация документов, их распределение по исполнителям, хранение) – децентрализовано по структурным подразделениям учреждения, фирмы и выполняется секретарями и лицами, ответственными за обработку документов этих подразделений.

В территориально раздробленном учреждении применяется **децентрализованная система,** при которой все стадии рассредоточены по структурным подразделениям или филиалам. Документирование информации, исполнение и использование документов всегда выполняется децентрализовано в структурных подразделениях руководителями и специалистами-исполнителями.

Документооборот одновременно с технологическими характеристиками обеспечения документированной информацией процесса управления обладает **количественными показателями**, также имеющими большое значение для организации управления.

Количество документов в сумме документопотоков за определенный промежуток времени (месяц, квартал, год) составляет **объем документооборота.** Одновременно может учитываться **количество экземпляров до**кументов и количество листов в документах. Учет количества документовосуществляется по месту их регистрации или исполнения и хранения. Отдельно учитываются обращения (предложения, заявления и жалобы) граждан. Количество тиражированных копий документов учитывается в службах оперативной полиграфии.

3.3 Задание

3.3.1 Для защищаемого объекта по варианту из лабораторной работы № 1 определить документы входного документопотока. Оформить журнал регистрации входящих конфиденциальных документов по образцу таблицы 3.1. Количество документов должно быть десять.

Таблица 3.1 – Журнал регистрации входящих конфиденциальных документов

Дата регистрации	Дата и номер документа	Откуда поступил	Краткое содержание (наименование)	Количество листов	Количество экземпляров	Исполнитель	Примечание
10.10.19	09.10.19 № 314	ООО «Техносервис»	Заявка на услуги сервиса	2	1	Иванов И.П.	-
12.10.19	10.10.19	Головной офис	Инструкция по защите ИР	5	1	Петров А.В.	-

3.3.2 Определить документы внутреннего выходного документопотока. Оформить журнал учета выдачи внутренних конфиденциальных документов по образцу таблицы 3.2. Количество документов должно быть десять.

Таблица 3.2 – Журнал учета выдачи внутренних КД

Номер документа	Дата выдачи	Краткое содержание (наименование)	Количество		Кому выдан	Подпись получателя	Отметка о возврате
			Листов	Экземпляров			

3.3.3 Определить порядок работы с входящими документами. Построить схему движения входящих документов. Пример приведен на рисунке 3.1.

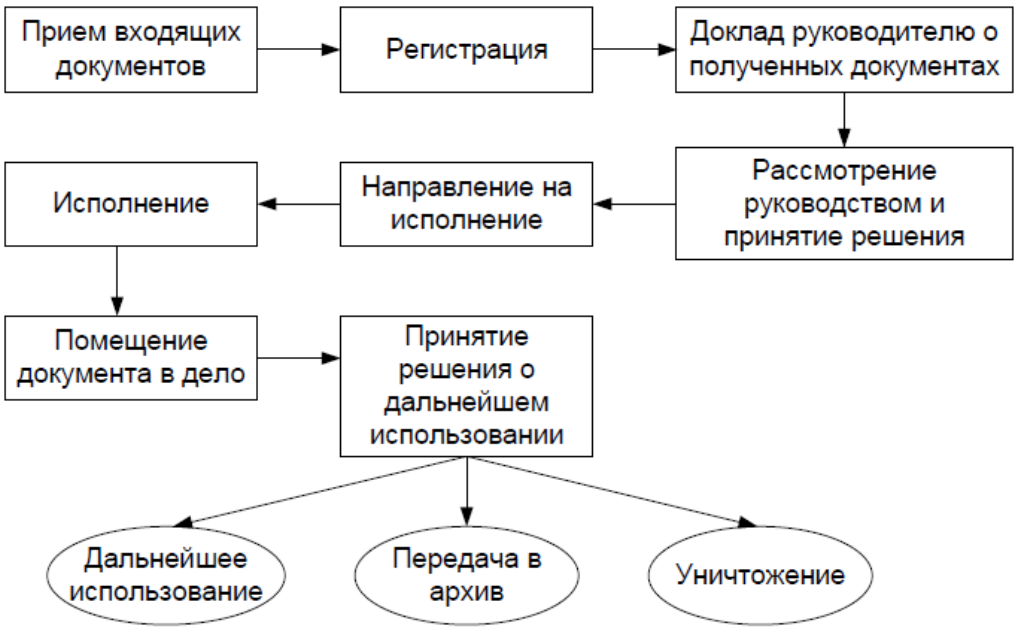

Рисунок 3.1 – Схема движения входящих документов

3.3.4 Определить документы внешнего выходного документопотока. Оформить журнал регистрации исходящих конфиденциальных документов по образцу таблицы 3.3. Количество документов должно быть десять.

Таблица 3.1 – Журнал регистрации исходящих документов

Дата регистрации	Номер документа	Куда отправляется	Краткое содержание (наименование)	Количество листов	Количество экземпляров	Исполнитель	Примечание
15.10.19	№ 614	ООО «Исток»	Проект договора	6	2	Иванов И.П.	-

3.3.5 Определить порядок работы с исходящими документами. Построить схему движения исходящих документов – внешнего и внутреннего потоков по примеру рисунков 3.2 и 3.3.

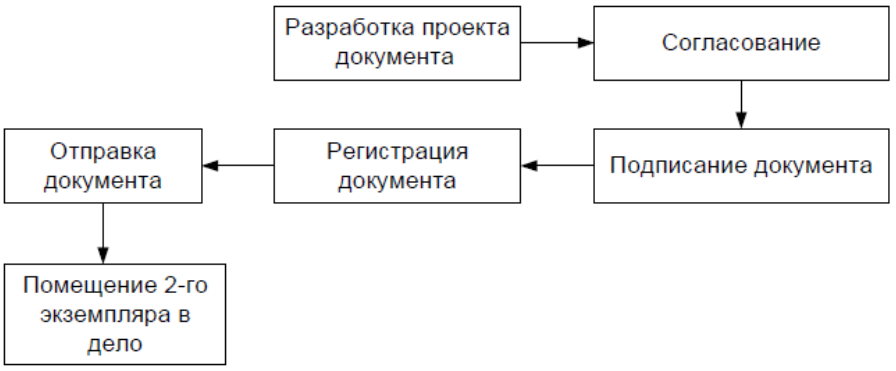

Рисунок 3.2 – Порядок обработки исходящих документов

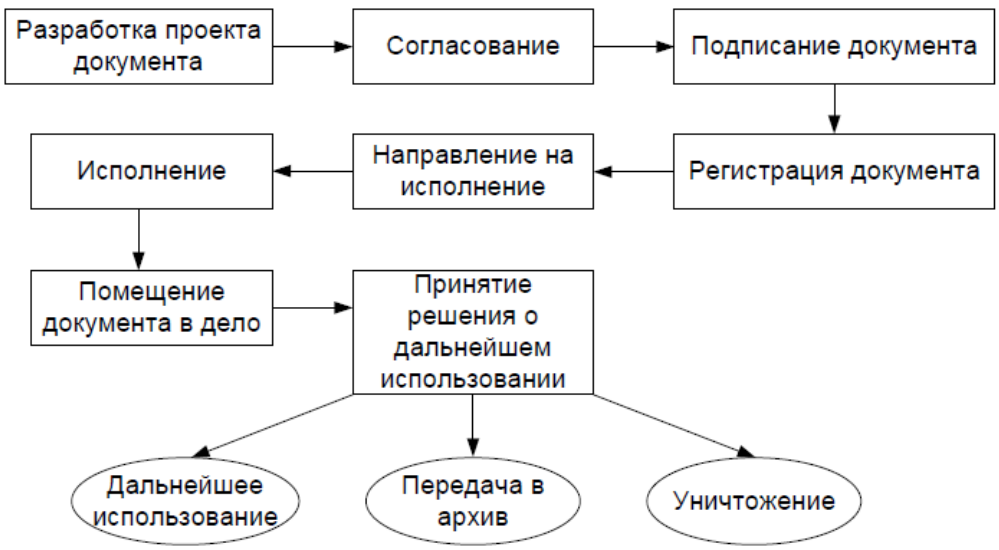

Рисунок 3.3 – Схема движения исходящих документов

3.4 Контрольные вопросы

1 Дать определение понятия «документопоток». Назовите и опишите все виды документопотоков.

2 Что является целью документооборота? Какие требования предъявляются к документопотоку?

3 Охарактеризуйте стадии входного и выходного докуметопотоков.

4 Определите, порядок работы с входящими конфиденциальными документами.

5 Укажите, какие графы содержит «Журнал регистрации входящих конфиденциальных документов».

6 Перечислите этапы работ с исходящими конфиденциальными документами.

7 Перечислите этапы работ с конфиденциальными внутренними документами.

8 Какие существуют системы обработки документов на объектах информатизации? Дайте характеристики этих систем.

9 Какие существуют количественные показатели документооборота?

10 Перечислите основные способы нанесения ущерба посредством разного рода воздействий на информацию и системы ее обработки.

11 Что входит в состав внутреннего документопотока? Какие документы нельзя включать во внутренний документопоток?

12 Что подразумевают под комплексностью документооборота?

4 Лабораторная работа № 4. Уязвимости документооборота

4.1 Цель работы

- Определение уязвимостей документооборота;
- Определение каналов утечки и воздействий на конфиденциальный документооборот.

4.2 Краткие теоретические сведения

Документооборот как объект защиты представляет собой упорядоченную совокупность (сеть) каналов объективного, санкционированного распространения конфиденциальной документированной информации в процессе управленческой и производственной деятельности пользователей (потребителей) этой информации.

Уязвимость конфиденциального документа – это возможность возникновения на каком-либо этапе жизненного цикла документа такого его состояния, при котором создаются условия для реализации угроз безопасности.

Угрозами безопасности конфиденциального документа являются события или действия, которые могут вызвать изменение его свойств.

Реализация преднамеренной угрозы безопасности **называется атакой** или нападением на информацию, документ, ее содержащий, или компьютерную систему обработки документа. Обработка конфиденциального документа предполагает его изготовление, хранение, передачу.

Угрозы конфиденциальным документам в документопотоках:

1) несанкционированный доступ постороннего лица к документам, делам и базам данных за счет его любопытства или провоцирующих действий, а также случайных или умышленных ошибок персонала учреждения, фирмы;

2) утрата документа или его отдельных частей (листов, приложений, схем, копий, экземпляров, фотографий и др.), носителя чернового варианта документа или рабочих записей в случае кражи, утери, уничтожения;

3) утрата информацией конфиденциальности при ее разглашении персоналом или утечке по техническим каналам, считывания данных в чужих массивах, использовании остаточной информации при копировании на бумаге, дисках;

4) подмена документов, носителей и их отдельных частей с целью фальсификации и сокрытия факта утери, хищения;

5) случайное или умышленное уничтожение ценных документов и баз данных, несанкционированная модификация и искажение текста, реквизитов, фальсификация документов;

6) гибель документов в условиях экстремальных ситуаций.

Классификация угроз безопасности персональных данных представлена на рисунке 4.1.

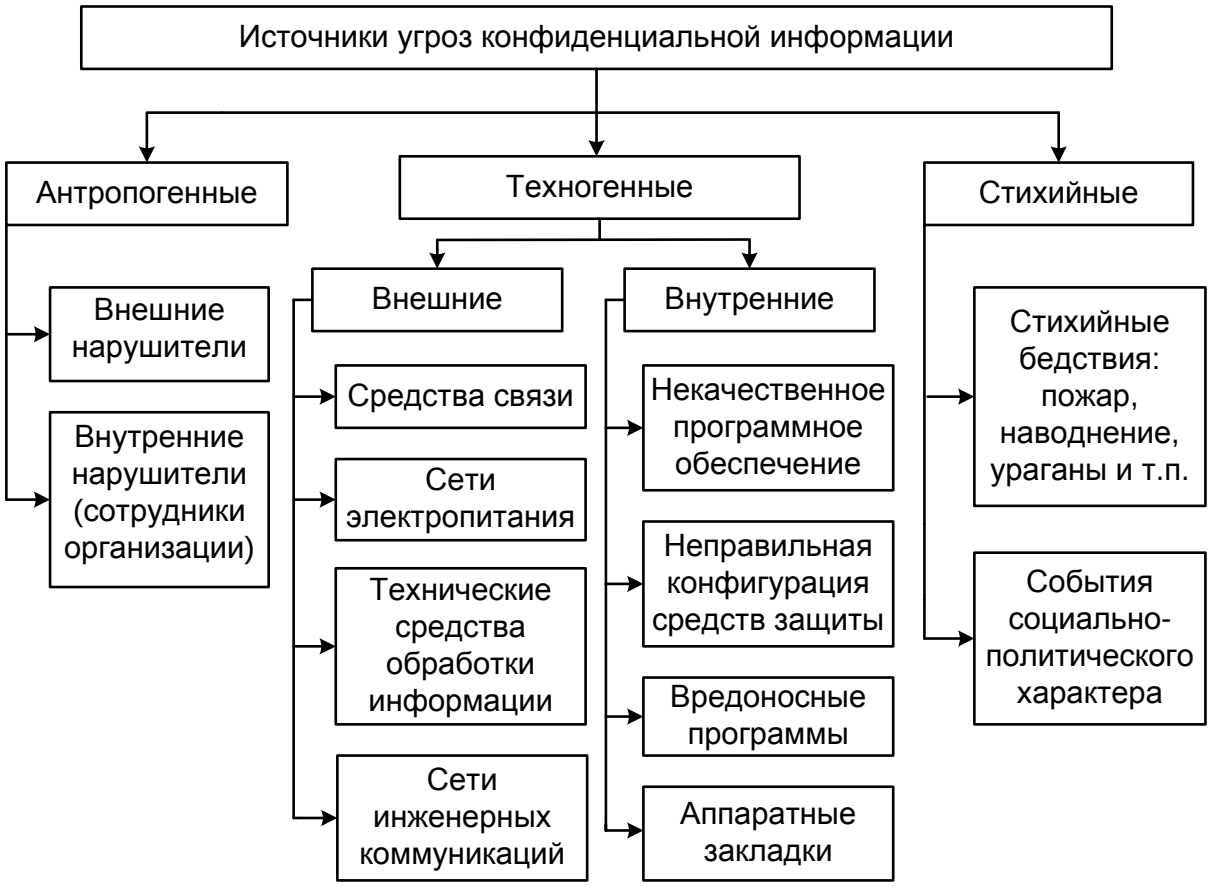

Рисунок 4.1 – Источники угроз конфиденциальной информации

Состав и содержание угроз безопасности конфиденциальной информации в информационных системах определяется совокупностью условий и факторов,

создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным. Все множество источников угроз можно разделить на антропогенные (искусственные) и естественные. Естественные источники угроз включают техногенные и стихийные источники.

Стихийные источники угроз включают обстоятельства, составляющие непреодолимую силу, носящие объективный и абсолютный характер. К стихийным источникам относятся: природные катаклизмы; события социально-политического характера.

Техногенные источники угроз - это технические средства и технологии, которые могут выйти из-под контроля человека. Техногенные источники угроз могут быть как внешними, так и внутренними. К техногенным источникам угроз относятся: средства связи; сети электропитания; системы кондиционирования; технические средства обработки информации; программное обеспечение (ПО).

Антропогенные источники - субъекты внутри или вне Организации, целенаправленные или ошибочные действия которых являются причиной нарушения безопасности КД. К ним относятся нарушители внешние и внутренние.

В соответствии с характером вышеуказанных угроз формируются задачи обеспечения защиты информации в документопотоках, направленные на предотвращение или ослабление этих угроз. **Главным направлением защиты документированной информации от возможных опасностей является:**

- формирование защищенного документооборота;
- использование в обработке и хранении документов специализированной технологической системы, обеспечивающей безопасность информации на любом типе носителя.

Под защищенным документооборотом (документопотоком) понимается контролируемое движение конфиденциальной документированной информации по регламентированным пунктам приема, обработки, рассмотрения, исполнения, использования и хранения в условиях организационного и технологического обеспечения безопасности, как носителя информации, так и самой информации.

Помимо общих для документооборота принципов, защищенный документооборот основывается на ряде следующих дополнительных принципов:

1) ограничения доступа персонала к документам, делам и базам данных деловой, служебной или производственной необходимостью;

2) персональной ответственности должностных лиц за выдачу разрешения на доступ сотрудников к конфиденциальным сведениям и документам;

3) персональной ответственности каждого сотрудника за сохранность доверенного ему носителя и конфиденциальность информации;

4) жесткой регламентации порядка работы с документами, делами и базами данных для всех категорий персонала, в том числе первых руководителей.

Защищенность документопотоков достигается за счет:

1) одновременного использования режимных (разрешительных, ограничительных) мер и технологических приемов, входящих в систему обработки и хранения конфиденциальных документов;

2) нанесения отличительной отметки (грифа) на чистый носитель конфиденциальной информации или документ, в т. ч. сопроводительный, что позволяет выделить их в общем потоке документов;

3) формирования самостоятельных изолированных потоков конфиденциальных документов и дополнительного их разбиения на подпотоки в соответствии с уровнем конфиденциальности перемещаемых документов;

4) использования автономной технологической системы обработки и хранения конфиденциальных документов, не соприкасающейся с системой обработки открытых документов;

5) регламентации движения документов как внутри учреждения, фирмы, так и между фирмами, т. е. с момента необходимости создания документа и до окончания работы с документом и передачи его в архив;

6) организации самостоятельного подразделения конфиденциальной документации или аналогичного подразделения, входящего (или не входящего) в состав службы безопасности или аналитической службы;

7) перемещения документов между руководителями, исполнителями и иным персоналом только через службу КД.

4.3 Задание

4.3.1 Определить уязвимости конфиденциального документооборота. Указать дестабилизирующие воздействия (в количестве 10-12), нарушаемые свойства информации и факторы уязвимостей. Результаты оформить в виде таблицы 4.1.

Таблица 4.1 – Анализ уязвимостей конфиденциальной информации на защищаемом объекте

Вид уязвимости	Дестабилизирующее воздействие	Нарушаемое свойство информации			Факторы уязвимости
		Конфиденциальность	Целостность	Доступность	
Утрата	Хищение носителя	+	-	+	отсутствие технических средств защиты доступа к носителям
	Потеря носителя	+	-	+	нарушение инструкции по работе с носителями
	Несанкционированное уничтожение	+	+	+	непрофессионализм сотрудников, преднамеренное нарушение правил обработки; сбои в работе техническтх средств обработки
	Внедрение вирусных программ	+	+	+	*заполнить*
	заполнить				*заполнить*
Утечка	Разглашение	+	-	-	Несоблюдения регламента работы с КД
	Утечка при передаче по каналам связи	+	+	+	Отсутствие защищенного канала передачи данных; отсутствие криптозащиты
	Утечка по каналам ПЭМИН	+	-	+	электромагнитное излучение технических средств обработки информации
	Утечка по акустическим каналам	+	-	+	нарушение технологии обработки и хранения информации
	заполнить				*заполнить*

4.3.2 Определить источники угроз безопасности конфиденциальной информации заданного объекта. Привести их текстовое описание и результаты оформить в виде таблицы по примеру таблицы 4.2.

Таблица 4.2 – Анализ источников угроз безопасности КД

Вид источника угроз безопасности ПДн	Перечень источников угроз безопасности
Техногенные	средства связи
	сети электропитания
	системы кондиционирования
	технические средства обработки информации
	Продолжить по объекту
Антропогенные	внешние нарушители: *перечислить*
	внутренние нарушители: *перечислить*
Стихийные	Пожар, наводнение, взрыв газа

4.3.3 Провести анализ каналов утечки документированной информации. Привести их текстовое описание и результаты оформить в виде таблицы по примеру таблицы 4.3.

Таблица 4.3 – Анализ каналов утечки конфиденциальной информации

Каналы утечки информации с объекта защиты	
1	2
Электромагнитный канал	Электромагнитные излучения технических средств обработки информации
	Просачивание электромагнитных сигналов по цепи электропитания
	Просачивание электромагнитных сигналов по цепи заземления
	заполнить
Электрический	Кабельные линии связи
	Телефонные линии
	заполнить
Оптический канал	Видеонаблюдение через окна, выходящие на улицу
	Фотографирование бумажных носителей
	заполнить

Продолжение таблицы 4.3

1	2
Радиоэлектронный канал	Стоянка автотранспорта на просп.
	Система часофикации
	Телефон
	Розетки
	ПЭВМ
	Воздушная линия электропередачи
	Система оповещения
	Система пожарной сигнализации
	заполнить
Акустический и электроакустический канал	Система отопления (батареи)
	Водопровод подземный
	Стены помещения
	заполнить
Материально-вещественный канал	Документы на бумажных носителях
	Персонал предприятия
	Производственные бумажные отходы

4.3.4 Провести анализ методов и средств несанкционированного получения документированной информации (6 видов действий). Привести их текстовое описание и результаты оформить в виде таблицы по примеру таблицы 4.4.

Таблица 4.4 - Анализ методов и средств несанкционированного получения документированной информации

Действие человека (типовая ситуация)	Каналы утечки информации	Методы и средства получения информации	Методы и средства защиты информации
Документ на бумажном носителе	Наличие	Кража, копирование, фотографирование	Разграничение доступа, применение аппаратных средств доступа
Изготовление документа на электронном носителе	Изображение на мониторе	Копирование, фотографирование, применение специальных радиотехнических устройств перехвата	Контроль доступа, криптозащита
Передача документа по каналу связи	Электрические и оптические сигналы	Несанкционированное подключение, имитация зарегистрированного пользователя	криптозащита
заполнить	*заполнить*	*заполнить*	*заполнить*

4.4 Контрольные вопросы

1 Дать определение понятия «уязвимость конфиденциальной информации». Что такое статус документированной информации?

2 Пояснить понятие «Документооборот как объект защиты».

3 Что называется угрозами безопасности конфиденциального документа? Что подразумевается под атакой на конфиденциальную информацию?

4 Перечислить угрозы конфиденциальным документам в документопотоках.

5 Назовите два вида уязвимости конфиденциальных документов. Дайте их определения и характеристику.

6 Дайте характеристику трех наиболее опасных форм проявления уязвимости.

7 Перечислите способы дестабилизирующего воздействия на информацию.

8 Чем отличаются формы проявления уязвимостей от способов дестабилизирующего воздействия? Привести пример.

9 Назовите основные источники угроз конфиденциальной информации. Дайте их характеристику.

10 Охарактеризуйте основные виды технических каналов утечки информации в зависимости от физической природы первичных источников сигналов.

11 Что называют защищенным документооборотом и каковы главные направления защиты документированной информации?

12 Какие стадии обработки конфиденциальных документов включает входной документопоток?

13 Какие стадии обработки конфиденциальных документов включает выходной документопоток?

14 За счет чего достигается защищенность документопотоков?

5 Лабораторная работа № 5. Технология подготовки, издания и учета конфиденциальных документов

5.1 Цель работы

- Изучение технологии подготовки носителей КД;
- Изучение порядка издания и учета КД.

5.2 Краткие теоретические сведения

Подготовка конфиденциальных документов должна начинаться с учета, оформления и выдачи исполнителям бумажных носителей информации, на которых будут составляться черновики или сразу проекты конфиденциальных документов.

Бумажными носителями могут быть:

− для текстовых документов - спецблокноты, отдельные листы бумаги, типовые формы документов, стенографические и рабочие тетради;

− для чертежно-графических документов - ватман, калька, миллиметровка.

Спецблокнот предназначен для составления черновиков документов. Он 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, на некоторых предприятиях не учитываются, а лишь производится отметка об их уничтожении в учетных формах соответствующих документов после печатания проектов документов.

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 издаваемых конфиденциальных документов.

Основные задачи учета носителей конфиденциальной информации:

1) закрепление факта присвоения носителю категории конфиденциальности, ограниченного доступа;

2) присвоение носителю учетного номера и включение его в справочно-информационный банк данных для контроля за использованием и проверки наличия;

3) документирование фактов перемещения носителя между сотрудниками учреждения, закрепление персональной ответственности за его сохранность;

4) контроль за работой исполнителя над документом и своевременным уничтожением носителя или его частей, потерявших практическое значение.

Учет носителей осуществляется подразделением конфиденциального делопроизводства. Перед взятием на учет носители должны быть оформлены следующим образом. На обложках спецблокнотов сотрудник подразделения конфиденциального 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 сотрудником подразделения конфиденциального делопроизводства.

На обложках рабочих и стенографических тетрадей указываются вид носителя, гриф конфиденциальности, инициалы и фамилия исполнителя.

Листы тетрадей нумеруются, на обороте последнего листа составляется, подписываемая сотрудником подразделения конфиденциального делопроизводства, заверительная надпись с указанием количества листов в

тетради. Листы типовых форм документов нумеруются исполнителем, на первом листе проставляется гриф конфиденциальности.

На отдельных листах бумаги, ватмана, миллиметровки, кальки в соответствующих графах основных надписей штампов или других установленных местах исполнителем проставляются:

− на всех носителях - гриф конфиденциальности, номера листов;

− дополнительно на носителях, предназначенных для чертежно-графических документов, - количество листов, подразделение и фамилия исполнителя.

На любом носителе, предназначенном для составления одного конкретного документа, указывается наименование этого документа.

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

Носители конфиденциальной информации учитываются в журналах или карточках, имеющих графы, показанные в таблице 5.1.

Таблица 5.1 - Журнал учета носителей конфиденциальной информации

Учетный номер и гриф конфи-денциаль-ности носителя	Дата реги-стра-ции	Вид носите-ля	Наимено-вание или назначени е носителя	Кол-во листо в	Фамилия лица, получивше го носитель	Подпись за получе-ние и дата	Подпись за возврат и дата	Отметка об уничтожени и носителя или переводе его на учет документов выделенног о хранения
1 Н. №-12. 1К	2 11.12. 2018	3 Бланк	4 Для письма	5 1	6 Иванов И.А.	7 Иванов 12.11.20 18	8 Петров 12.11.20 18	9 -

Если на предприятии носители не переводятся на учет документов выделенного хранения, то графа 9 формулируется «Отметка об уничтожении носителя».

При взятии на учет заполняются графы 1 -6. В графе 1 рядом с номером носителя начальными буквами (аббревиатурой) проставляется его гриф конфиденциальности: 1КТ (коммерческая тайна), 2СК (строго конфиденциально) и др. Если издаваемые документы имеют только один гриф конфиденциальности, то в наименовании графы 1 слова «и гриф конфиденциальности» опускаются, рядом с номерами носителей гриф не проставляется.

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

*Индекс «Н» (носитель) проставляется для того, чтобы отличать номера носителей от номеров изданных документов, которые могут проставляться на отдельных носителях при наличии на них и номеров носителей. В журнале учета носителей индекс не проставляется.*С указанием учетного номера 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 и количества листов;

На отдельных листах бумаги, типовой формы документа, ватмана, кальки, миллиметровки: в верхней части левого поля первого листа такой же штамп с указанием учетного номера и количества листов (на носителях чертежно-графической информации - только учетного номера); на левом поле остальных листов штамп «К Н №» с указанием номера.

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

При необходимости взятия на учет дополнительных листов носителя (при нехватке ранее взятых листов для составление черновика документа или для замены испорченных листов) они нумеруются от последнего листа ранее учтенного по этому номеру носителя, регистрируются в журнале учета носителей за 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 подразделения конфиденциального делопроизводства. Выдача дополнительных листов производится под отдельную подпись в графе 7 журнала учета носителей.

Оформление конфиденциальных документов.

Официальные конфиденциальные документы должны быть оформлены и удостоверены в установленном порядке.

Чертежно-графические документы оформляются в соответствии с нормами, существующими для систем проектной, конструкторской и технологической документации, текстовые документы - по установленным правилам оформления различных систем управленческой документации.

Самой многочисленной по составу и объему документов, присущей всем организациям и предприятиям независимо от формы собственности и организационно-правовой формы, является **система организационно-распорядительной документации, применяемая для фиксации решений административных и организационных вопросов, а также вопросов управления, взаимодействия, обеспечения и регулирования деятельности организаций и предприятий.**

Состав организационно-распорядительных документов определен Общероссийским классификатором управленческой документации (ОКУД-93).

К ним отнесены следующие документы, имеющие отношение к коммерческой деятельности:

- документация по созданию организации, предприятия;
- документация по реорганизации организации, предприятия;
- документация по ликвидации организации, предприятия;
- документация по приватизации государственных и муниципальных организаций, предприятий;
- документация по распорядительной деятельности организации, предприятия;
- документация по организационно-нормативному регулированию деятельности организации, предприятии;
- документация по оперативно-информационному регулированию деятельности организации, предприятия;
- документация по приему на работу;
- документация по переводу на другую работу и другие.

Правила оформления организационно-распорядительных документов установлены ГОСТ 6.30-2003 «Унифицированные системы документации. Система организационно-распорядительной документации. Требования к оформлению документов»

Эти требования в целом применимы и для конфиденциальных документов, однако специфика конфиденциальных документов вызывает необходимость частичного уточнения некоторых положений стандарта.

ГОСТ установил:

- состав реквизитов организационно-распорядительных документов, которыми являются элементы оформления официального документа;
- требования к оформлению реквизитов;
- требования к бланкам документов и оформлению документов;
- требования к изготовлению, учету, использованию и хранению бланков с воспроизведением Государственного герба Российской Федерации, гербов субъектов Российской Федерации.

5.3 Задание

5.3.1 Определить основные носители конфиденциальной информации заданного объекта защиты. Оформить журнал учета носителей конфиденциальной информации по образцу таблицы 5.1. При этом задать номера документов и присвоить им гриф конфиденциальности.

5.3.2 Составить журнал учета изданных конфиденциальных документов по образцу таблицы 5.2.

Таблица 5.2 - Журнал учета изданных конфиденциальных документов

Учетный номер и гриф конфиденциаль-ности	Дата документа	Вид и заголовок документа	Номер носителя и черновика	Фамилия исполни-теля	Количество		Подпись за получение	Подпись за возврат и дата
					Экземпляров документа	Листов в экземпляре		
1	2	3	4		5	6	7	8
1КТ	14.01.2019	АКТ об уничтожении маккулатуры	Рукопись без черновика	Смирнов А.А.	1	1	Иванов 12.04.2019	Петров 12.04. 2019

Отметка об уничтожении черновиков	Отметка об уничтожении проекта или лишнего экземпляра	Куда отправлен документ	Номер экземп-ляров	Наименование, номер и дата сопроводительного документа	Отметка о возврате	Индекс, дата, номер листов	Номер по учету документов выделенного хранения, количество экземпляров
10	11	12	13	14	15	16	17

5.3.3 Составить следующие конфиденциальные документы и присвоить им все необходимые реквизиты в соответствии с ГОСТ 6.30-2003:

- приказ о распределении обязанностей между начальниками управлений предприятия;
- приказ о проведении внутреннего аудита;
- положение о структурном подразделении предприятия.

5.4 Контрольные вопросы

1 Назовите основные задачи учета носителей конфиденциальной информации.

2 Назовите и дайте описание основных бумажных носителей конфиденциальной информации.

3 Какие реквизиты оформляются только для конфиденциальных документов?

4 Какие реквизиты содержат признаки конфиденциальных документов?

5 Какую информацию включает реквизит «Гриф ограничения доступа к документу»?

6 Поясните состав организационно-распорядительных документов.

7 Кто осуществляет учет носителей конфиденциальных документов?

8 Какой нормативно-правовой документ регламентирует правила оформления организационно-распорядительных документов?

9 Кем и каким образом проводится уничтожение черновиков конфиденциальных документов и каким образом этот процесс подтверждается?

10 Где на документе проставляется учетный номер по Журналу учета изданных документов?

11 Какие три цели преследует учет носителей конфиденциальных документов?

12 Кто на предприятии составляет и утверждает перечень сведений, составляющих коммерческую тайну?

6 Лабораторная работа № 6. Защита конфиденциальных документов при исполнении, хранении и уничтожении

6.1 Цель работы

- Изучение основ защиты конфиденциальных документов;
- Изучение правил хранения и уничтожения документов.

6.2 Краткие теоретические сведения

В соответствии с утвержденным положением о разрешительной системе доступа к конфиденциальной информации после учета документов осуществляется их рассмотрение и передача для исполнения.

При большом объеме поступающих документов целесообразно осуществлять их предварительное рассмотрение и распределение по уровням принятия решений по ним.

С этой целью разрабатывается Перечень поступивших документов, направляемых на исполнение без доклада руководителю предприятия. В этом перечне полномочия по принятию решений по исполнению документов делегируются на соответствующий уровень управления. В перечень включаются конкретные наименования поступающих документов, имеющих, как правило, типовой и повторяющийся характер, которые адресуются заместителям руководителя предприятия, руководителям подразделений или непосредственным исполнителям без рассмотрения этих документов руководителем предприятия.

Перечень может иметь следующую форму:

№ п/п	Наименования адресуемых документов	И., О., фамилия лица, которому адресуются документы	И., О., фамилии лиц, которым адресуются документы при временном отсутствии основных адресатов
1	2	3	4

Разработку перечня целесообразно возлагать на постоянно действующую, экспертную комиссию. При подготовке перечня необходимо учитывать требования Положения о разрешительной системе доступа к конфиденциальной информации в части обеспечения правомерности доступа к документам в процессе делегирования полномочий по их рассмотрению.

Перечень подписывается председателем и членами ПДЭК и вводится в действие приказом руководителя предприятия.

Копирование и размножение документов.

Конфиденциальные документы могут копироваться и тиражироваться с помощью соответствующей организационной техники и в случае соблюдения действующих требований защиты информации и сохранности всех сопровождающих этот процесс промежуточных носителей (печатных форм).

Копирование и тиражирование конфиденциальных документов всегда письменно санкционируется полномочным должностным лицом. После этого вносятся необходимые записи в учетной форме основного документа и на самом документе. Копировальная техника должна располагаться в помещении службы КД. Множительная техника обслуживается специалистами соответствующего структурного подразделения, учреждения, фирмы.

Контроль исполнения документов.

Документы, требующие подготовки ответа или принятия решения, подлежат контролю.

Организация контроля должна обеспечивать качественное и своевременное исполнение документов.

Ответственность за качество исполнения документов несут исполнители и руководители подразделений, в которых работают исполнители.

Контроль за сроками исполнения документов осуществляет наряду с руководителями соответствующих структурных подразделений подразделение конфиденциального делопроизводства.

Если исполнение документа поставлено на контроль, то для его осуществления при карточном способе учета используются дополнительные

экземпляры учетных карточек, в которых для перенесения резолюции руководителя и контрольных отметок используются графы, отражающие движение документов в ходе их исполнения.

Подготовка конфиденциальных документов для архивного хранения и уничтожения.

Экспертиза ценности конфиденциальных документов.

По истечении времени хранения дел в структурных подразделениях и службе ДОУ учреждения, фирмы (один-два года) и миновании текущей управленческой значимости хранимых документов дела передаются в ведомственный архив (архив учреждения, фирмы).

Подготовка документов к сдаче в ведомственный архив включает следующие процедуры:

1. проведение экспертизы ценности документов;
2. оформление дел;
3. составление описей дел;
4. составление актов о выделении к уничтожению документов и дел.

Под экспертизой ценности документов понимается изучение документов на основе принципов и критериев их ценности в целях определения сроков хранения документов и отбора их для хранения. В число основных принципов ценности включаются принципы историзма, комплексности и всесторонности оценки документов с точки зрения их экономического, научно-технического и социально-культурного значения. К критериям ценности относятся происхождение документов, их содержание и внешние особенности.

Экспертиза ценности документов проводится постоянно действующей экспертной комиссией учреждения, фирмы. В крупных учреждениях, фирмах формируется центральная экспертная комиссия, которая объединяет и координирует работу экспертных комиссий структурных подразделений. Персональный состав экспертной комиссии утверждается приказом первого руководителя учреждения, фирмы. В комиссию включаются наиболее квалифицированные работники, имеющие большой опыт работы в сфере

деятельности учреждения, фирмы, а также руководители службы ДОУ, ведомственного архива и бухгалтерии. Комиссия состоит из трех-пяти человек и работает под председательством одного из заместителей первого руководителя.

В результате проведения экспертизы ценности документов выделяются четыре категории дел:

1. Дела постоянного хранения, подлежащие в последующем передаче в государственный архив.

2. Дела долговременного хранения в ведомственном архиве учреждения, фирмы (свыше 10 лет).

3. Дела временного хранения (до 10 лет).

4. Дела, подлежащие уничтожению в связи с истечением срока хранения.

По окончании проведения экспертизы ценности документов и отбора дел с документами постоянного и долговременного срока хранения приступают к их оформлению.

Оформление дела - это подготовка дела к хранению в соответствии с установленными правилами. Дела оформляются и готовятся к сдаче в ведомственный архив в соответствии с Основными правилами работы ведомственных архивов. Оформление дел проводится работниками службы ДОУ учреждения, фирмы и структурных подразделений, в ведении которых находились заведенные и сформированные дела, при методической помощи и под контролем ведомственного архива.

Номенклатура дел – это систематизированный перечень документов, образующихся в деятельности организации, с указанием сроков их хранения, а по истечении календарного года – с указанием их количества. Номенклатура дел является обязательным документом для федеральных органов исполнительной власти и государственных учреждений. Что касается коммерческих организаций, то в обязательном порядке ее должны разрабатывать только организации – источники комплектования государственных (муниципальных) архивов. Для прочих номенклатура теоретически не обязательна.

Однако на практике любая организация рано или поздно приходит к необходимости ее создать: когда нужно избавиться от скопившихся за годы работы документов, установить сроки их хранения. А перечень дел и документов организации с указанием сроков хранения – это и есть номенклатура дел. Все это касается, конечно, тех организаций, которые растут и развиваются, а не топчутся годами на одном месте в ожидании штрафов от проверяющих органов.

При работе над номенклатурой дел следует руководствоваться двумя документами (первый носит нормативный характер, второй – рекомендательный):

Правила организации хранения, комплектования, учета и использования документов Архивного фонда РФ и других архивных документов в органах государственной власти, органах местного самоуправления и организациях (утверждены приказом Минкультуры России от 31.03.2015 № 526,);

Основные правила работы архивов организаций (одобрены решением Коллегии Росархива от 06.02.2002**.**

Алгоритм работы с номенклатурой дел представлен на рисунке 6.1.

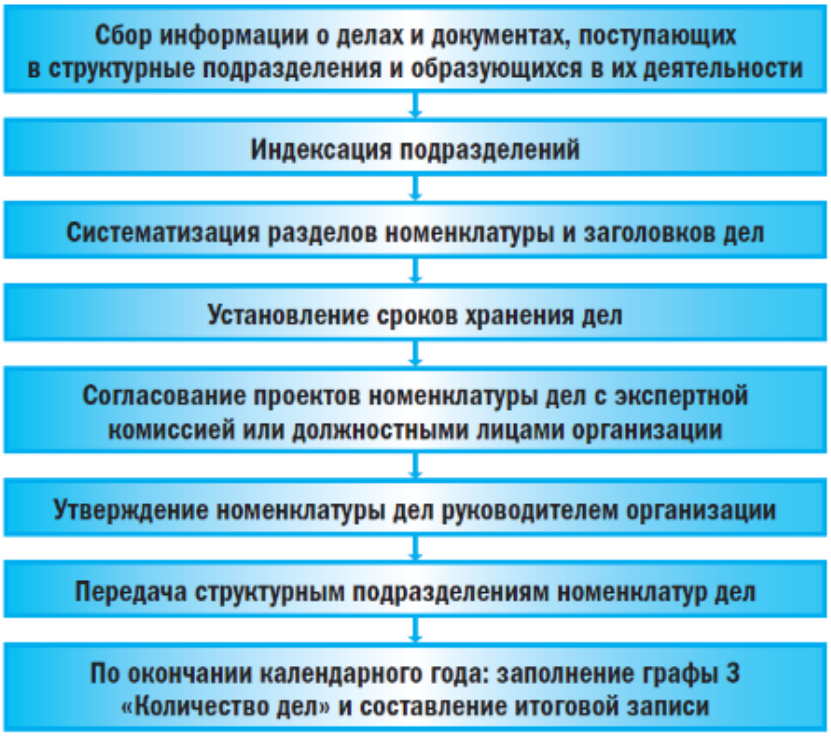

Рисунок 6.1 - Алгоритм работы с номенклатурой дел

6.3 Задание

6.3.1 Составить приказ о создании комиссии по проведению экспертизу ценности конфиденциальных документов в организации.

6.3.2 Для защищаемого объекта провести экспертизу ценности конфиденциальных документов, используя перечень конфиденциальных документов, составленный в предыдущих работах. Результаты оформить в виде таблицы по примеру таблицы 6.1. Количество наименований в каждой строке – не менее 5.

Таблица 6.1 – Распределение документов на категории дел

Дела постоянного хранения	Дела долговременного хранения	Дела временного хранения	Дела, подлежащие уничтожению
Положения о структурных подразделениях и подразделениях в составе структурных подразделений	Реестры акционеров, выписки из реестров акционеров	Акты приема-передачи с приложениями	Докладные записки, справки, отчеты
Заполнить	*Заполнить*	*Заполнить*	*Заполнить*

6.3.3 Составить номенклатуру дел защищаемого объекта по приведенной форме.

Форма примерной номенклатуры дел

Наименование органа управления
ПРИМЕРНАЯ НОМЕНКЛАТУРА ДЕЛ
(наименование организаций, на которые распространяется примерная номенклатура)
_____ N _____

УТВЕРЖДАЮ
Должность руководителя организации

Подпись Расшифровка подписи

место составления Дата

Индекс дела	Заголовок дела	Срок хранения и N статьи по перечню	Примечания
1	2	3	4
НАЗВАНИЕ РАЗДЕЛА			

Должность составителя Подпись Расшифровка подписи

Виза зав. архивом организации

СОГЛАСОВАНО
Протокол ЦЭК (ЭК)
_____ N _____

СОГЛАСОВАНО
Протокол ЭПК
архивного учреждения
_____ N _____

6.4 Контрольные вопросы

1 Как формируются дела постоянного хранения?

2 Каковы правила архивного хранения документов?

3 Как определяются сроки хранения документов в организации? Какой орган выполняет эту работу и какой документ оформляют в результате?

4 Что такое номенклатура дел, каковы правила формирования номенклатуры?

5 Приведите описание алгоритма работы с номенклатурой дел.

6 Как определяются сроки хранения номенклатуры дел?

7 В каких случаях проводится экспертиза ценности конфиденциальных документов?

8 Как отметить архивные дела в номенклатуре дел?

9 Каким образом проводится индексация разделов номенклатуры?

7 Лабораторная работа № 7. Обработка конфиденциальных документов в электронном виде

7.1 Цель работы

Изучение современных систем электронного документооборота (СЭД).

7.2 Краткие теоретические сведения

Первые системы электронного документооборота разрабатывались непосредственно на предприятиях и были полностью индивидуализированными. Изменить структуру такой системы было практически невозможно, а стоимость программы была весьма высокой. Применяли электронный документооборот только в тех компаниях, где исключение ручной обработки документов могло принести немалую экономию. Остальные организации по-прежнему работали с бумажными носителями.

Электронный документооборот (ЭДО) — это система автоматизированных процессов обработки электронных документов, реализующая концепцию «безбумажного делопроизводства».

Основным элементом электронного документооборота является электронный документ, создаваемый с помощью средств компьютерной обработки информации и хранящийся в виде файла того или иного формата на машинном носителе.

Внедрение электронного документооборота позволяет предприятию получить следующие преимущества:

− однократная регистрация документа, позволяющая безошибочно идентифицировать его в системе;

− параллельное выполнение нескольких операций, сокращающее время движения документа и повышающее оперативность исполнения;

− непрерывное движение документа, дающее возможность выявить ответственного за его исполнение в любой момент процесса;

− единая база документов, исключающая возможность их дублирования;

− результативный поиск документа при наличии о нем минимальной информации;

− эффективная система отчетности, позволяющая контролировать движение документа на каждом этапе документооборота.

В зависимости от специфики деятельности организации выделяют несколько видов электронного документооборота:

− производственный ЭДО;

− управленческий ЭДО;

− архивное дело;

− кадровый ЭДО;

− бухгалтерский ЭДО;

− складской ЭДО;

− технологический ЭДО;

− секретный и конфиденциальный ЭДО.

Систем электронного документооборота может быть столько же, сколько существует видов деятельности. При необходимости можно автоматизировать любой частный документооборот. Функции и эффективность ЭДО

Набор необходимых функций ЭДО определяется задачами, стоящими перед автоматизацией документооборота в компании. Базовые функции ЭДО могут быть следующими:

− создание электронной версии документа;

− создание атрибутной карточки документа;

− формирование текста из готового шаблона с подстановкой в него значений переменных из карточки документа;

− поиск карточек документов;

− формирование электронного документа с использованием шаблона на бланке организации;

− сохранение документов в различных форматах;

− создание маршрутов документа и управление его движением;

− ведение журналов, классификаторов и справочников;

− регистрация и классификация документов, регистрируемых в программе;

− рассылка напоминаний и уведомлений;

− согласование документов;

− формирование отчетов о движении и исполнении документов.

Эффективность использования электронного документооборота в организациях оценивается количественно и качественно. Количественные показатели могут быть измерены и оценены с точки зрения материальных и временных затрат:

− сокращение времени в среднем на 75% на обработку и создание документов: регистрация, рассылка, поиск, выполнение контрольных операций;

− ускорение движения информационных потоков: передача документа от подразделения к подразделению или компании-партнеру, подготовка типовых документов, согласование, скорость распространения информации внутри компании;

− экономия материалов и ресурсов в виде сокращения расходов на канцелярские принадлежности, расходные материалы и хранение документов.

Качественные показатели оцениваются с точки зрения улучшения и развития нескольких аспектов деятельности компании:

− рост производительности труда работников до 25%, благодаря наличию единого информационного пространства, упрощению процессов коллективной работы, эффективному контролю над исполнением документов;

− снижение рисков потери документов;

− увеличение скорости согласования и утверждения документов;

− повышение корпоративной культуры.

Как показывает практика, экономический эффект от внедрения системы электронного документооборота на предприятии будет тем больше, чем больше сотрудников будут вовлечены в ЭДО.

Требования к системам электронного документооборота.

Система электронного документооборота (СЭД) — это специальное приложение, обеспечивающее участникам обмен электронными документами, имеющими юридическую значимость. Все системы электронного документооборота могут быть классифицированы по нескольким признакам:

− СЭД с развитыми системами хранения и поиска информации. Их второе название — электронные архивы.

− СЭД с развитыми системами маршрутизации, обеспечивающие движение документов по заданным маршрутам.

− СЭД с системой поддержки управления организацией и накопления знаний. Обычно эти системы сочетают в себе свойства двух предыдущих. При этом в такой системе возможно использование как жесткой, так и свободной маршрутизации. Подобные СЭД используются в крупных компаниях и государственных структурах.

− СЭД с поддержкой совместной работы сотрудников. Такие системы нацелены на организацию коллективной работы сотрудников даже в том случае, если они разделены территориально. Предоставляют возможность поиска информации, обсуждений и назначения встреч, включая реальные и виртуальные, а также сервисы хранения и публикации документов.

− СЭД с дополнительными сервисами: управление проектами, электронная почта, биллинг, сервис CRM.

7.3 Задание

Осуществить поиск информации о системе электронного документооборота согласно варианту по списку.

Составить характеристику системы электронного документооборота, его конкретного назначения, выполняемых функций, преимуществ перед другими системами, привести области применения. Для составления характеристики СЭД использовать параметры, представленные в таблицах источника: https://www.ixbt.com/soft/sed.shtml .

Привести изображения оконных форм заданной системы электронного документооборота.

Оформить отчет о работе.

Directum (Directum),

DocsVision (DocsVision),

Globus Professional (Проминфосистемы),

PayDox (Paybot),

1С:Документооборот (1С),

Босс-референт (БОСС — Референт, ГК АйТи),

ДЕЛО (ЭОС),

ЕВФРАТ (Cognitive Technologies),

МОТИВ (Мотив).

Documentum (EMC Documentum),

Кларис,

CompanyMedia,

Логика ECM (БОСС-Референт)

Lotus Domino.Doc,

OPTIMA-WorkFlow,

LanDocs,

1С:Архив,

ЭЛАР Контекст

WSS Docs

КРОК инкорпорейтед»,

«ИнтерТраст» (CompanyMedia),

«Парма-Телеком» (на базе SAP /R3)

«Хоулмонт»

ТЕЗИС

Список использованных источников

1 Артемов, А. В. Информационная безопасность курс лекций. [Электронный ресурс] А. В. Артемов – Орел: МАБИБ, 2014. – 257 с. ЭБС УНИВЕРСИТЕТСКАЯ БИБЛИОТЕКА. Режим доступа: http://biblioclub.ru/index.php?page=book_view_red&book_id=428605

2 Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных : Руководящий документ ФСТЭК России 15.02.2008 г. [Электронный ресурс]. – Режим доступа: https://fstec.ru/component/attachments/download/289

3 Бурькова, Е. В. Профессиональная подготовка специалистов в области информационной безопасности [Электронный ресурс] / Бурькова Е. В. // Вестник Оренбургского государственного университета,2016. - № 2. - С. 3-9.

4 Бурькова, Е. В. Модель защиты документооборота в распределенной информационной системе медицинского учреждения [Электронный ресурс] / Е. В. Бурькова, С. Н. Небогатов // Теоретические и прикладные вопросы комплексной безопасности: материалы III Междунар. науч.-практ. конф.: Санкт-Петерб. ГПС МЧС России,2020. - С. 148-152.

5 Делопроизводство: образцы, документы, организация и технология работы: с учетом нового ГОСТ 6.30-2003 "Унифицированные системы документации. Унифицированная система организационно-распорядительной документации. Требования к оформлению документов" / В. В. Галахов [и др.]; ред. И. К. Корнеев, В. А. Кудряев.- 3-е изд. перераб. и доп. - М. : Проспект, 2008. – 480 с.

6 Мельников, В. П. Защита информации: учебник / В. П. Мельников, А. И. Куприянов, А. Г. Схитладзе; под ред. В. П. Мельникова. – М.: Академия, 2014. – 297 с.

7 Некраха, А. В. Организация конфиденциального делопроизводства и защита информации: учеб. пособие / А. В. Некраха, Г. А. Шевцова. - М. :

Академический проект, 2007. - 224 с.

8 Об информации, информационных технологиях и о защите информации: Федеральный Закон от 26.07.07 № 149-ФЗ // Собрание законодательства Российской Федерации. – 2005. – 609 с.

9 Обзор систем электронного документооборота. Режим доступа: https://www.ixbt.com/soft/sed.shtml

10 Садердинов, А. А. Информационная безопасность предприятия: учеб. пособие для вузов / А. А. Садердинов, В. А. Трайнев, А. А. Федулов.- 2-е изд. - М.: Дашков и К, 2005. - 336 с.

11 Скрипник, Д. А. Общие вопросы технической защиты информации / Д.А. Скрипник – М.: Национальный Открытый Университет «ИНТУИТ», 2016. – 425 с. ЭБС УНИВЕРСИТЕТСКАЯ БИБЛИОТЕКА. Режим доступа: http://biblioclub.ru/index.php?page=book_view_red&book_id=429070

12 Стенюков, М. В. Документоведение и делопроизводство [Текст] : конспект лекций / М. В. Стенюков . - М. : А-Приор, 2007. - 174 с. - (В помощь студенту). - Словарь терминов: с. 158-167. - Библиогр.: с. 168.

13 Стрельцов, А. А. Организационно-правовое обеспечение информационной безопасности: учебное пособие / А. А. Стрельцов, В. С. Горбатов, Т.А. Полякова. – М.: Издательский центр «Академия», 2008. - 256 с.

14 Электронный документооборот как способ оптимизации бизнес-процессов. Режим доступа: https://www.kp.ru/guide/ielektronnyi-dokumentooborot-na-predprijatii.html