МИНИСТЕРСТВО ОБРАЗОВАНИЯ КИРОВСКОЙ ОБЛАСТИ

Кировское областное государственное профессиональное

образовательное бюджетное учреждение

«КИРОВСКИЙ ПЕДАГОГИЧЕСКИЙ КОЛЛЕДЖ»

**Бусыгина Дарья Александровна**

*(специальность 46.02.01 «Документационное обеспечение управления и архивоведение»)*

**Особенности организации работы с документами с ограниченным доступом в** **отделе архива муниципального казенного учреждения** **«Центр ресурсного обеспечения образовательных учреждений города Кирова»**

ДИПЛОМНЫЙ ПРОЕКТ (РАБОТА)

Научный руководитель:

Гибадулина Г.В.

преподаватель дисциплин профессионального цикла

2022

СОДЕРЖАНИЕ

[ВВЕДЕНИЕ 4](#_Toc127558311)

[1 СПЕЦИФИКА КОНФИДЕНЦИАЛЬНОГО ДЕЛОПРОИЗВОДСТВА 7](#_Toc127558312)

[1.1 Сущность и особенности конфиденциального делопроизводства 7](#_Toc127558313)

[1.2 Особенности обработки, хранения и последующего использования конфиденциальных документов 9](#_Toc127558314)

[1.3 Носители конфиденциальной информации 11](#_Toc127558315)

[1.4 Персональные данные и их защита 12](#_Toc127558316)

[1.5 Технология работы с документами ограниченного доступа 17](#_Toc127558317)

[2 РАЗРАБОТКА ИНСТРУКЦИИ ПО КОНФИДЕНЦИАЛЬНОМУ ДЕЛОПРОИЗВОДСТВУ В МКУ ЦРО 20](#_Toc127558318)

[2.1 Организационная характеристика МКУ «Центр ресурсного обеспечения образовательных учреждений города Кирова» 20](#_Toc127558319)

[ЗАКЛЮЧЕНИЕ 21](#_Toc127558320)

[СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ 22](#_Toc127558321)

[ПРИЛОЖЕНИЯ 24](#_Toc127558327)

[ПРИЛОЖЕНИЕ А 24](#_Toc127558328)

[ПРИЛОЖЕНИЕ Б 26](#_Toc127558329)

[ПРИЛОЖЕНИЕ В 27](#_Toc127558330)

[ПРИЛОЖЕНИЕ Г 28](#_Toc127558331)

[ПРИЛОЖЕНИЕ Д 29](#_Toc127558332)

# ВВЕДЕНИЕ

Деятельность любой организации невозможно представить без сбора, обработки, накопления, хранения, поиска и распространения информации, при этом информация все чаще принимает фиксированный, документальный характер.

Безопасность ценной документируемой информации (документов) определяется степенью ее защищенности от последствий экстремальных ситуаций, в том числе стихийных бедствий. А также пассивных и активных попыток злоумышленника создать потенциальную или реальную угрозу несанкционированного доступа к документам с использованием организационных и технических каналов, в результате чего могут произойти хищение и неправомерное использование злоумышленником информации в своих целях, ее модификация, подмена, фальсификация, уничтожение.

В современной российской экономике обязательным условием успеха предприятия, фирмы, организации является обеспечение экономической безопасности их деятельности. Одна из главных составных частей экономической безопасности – информационная безопасность, достигаемая за счет использования комплекса систем, методов и средств зашиты информации предприятия, организации от злоумышленных действий конкурентов и с целью сохранения ее целостности и конфиденциальности.

Согласно общему подходу к составу защищаемой информации защите подлежит вся конфиденциальная информация, доступ к которой ограничен. Она должна защищаться от утраты и утечки.

Вопрос организации работы с документами с ограниченным доступом является **актуальным**, так как обработка и обеспечение сохранности конфиденциальных документов становятся все более сложными и значимыми в связи с массовым переходом на информационные технологии в управлении на безбумажную автоматизированную основу и электронный документооборот. При всей прогрессивности этого перехода одновременно существенно расширяется и содержательно обновляется комплекс организационных, технических и технологических трудностей в предотвращении вмешательства в информационные ресурсы. Правильная и грамотная организация работы с конфиденциальными документами, позволяет обеспечить их «закрытость», а также последующее их грамотное использование.

В настоящее время одной из наиболее актуальных **проблем** в области информационной безопасности является проблема защиты от утечки конфиденциальной информации.

**Проблемный вопрос:** каковы особенности работы с документами с ограниченным доступом в архиве?

**Цель исследования** – раскрыть особенности и разработать инструкции по работе с документами с ограниченным доступом в архиве.

**Объектом исследования** является организация работы с документами в архиве.

**Предмет исследования –** документы с ограниченным доступом в архиве.

В исследовательской работе мы выдвинули следующую **гипотезу –** мы предполагаем, что правильная организация работы с документами с ограниченным доступом в соответствии с ГОСТом, способствует их защите от несанкционированного доступа.

В соответствии с целью исследовательской работы и выдвинутой гипотезой были определены следующие **задачи:**

1. Рассмотреть понятие и сферу деятельности конфиденциального делопроизводства в архиве.
2. Изучить особенности организации работы с документами с ограниченным доступом.
3. Рассмотреть защиту и обработку конфиденциальных документов.
4. Моделирование инструкции по работе с документами с ограниченным доступом в архиве.

**Теоретико-методологическая основа:**

* ГОСТ Р 2.051‒2006 ЕСКД «Электронные документы. Общие положения» [9];
* ГОСТ Р 7.0.8 – 2013 «Система стандартов по информации, библиотечному и издательскому делу «Делопроизводство и архивное дело» [10];
* ГОСТ Р 7.0.8–2013 «СИБИД. Делопроизводство и архивное дело. Термины и определения» [11];
* труды отечественных и зарубежных ученых и специалистов, посвященные защите информации [13, 15, 16, 18, 20, 26, 29].

При выполнении дипломной работы был изучен ряд нормативно-правовых актов, таких как Федеральный закон «Об информации, информационных технологиях и о защите информации» и другие федеральные законы и нормативные акты РФ. Базой для написания работы стали труды ведущих специалистов в области документоведения М.И. Басакова [13], В.В. Галахова [15], А.В. Пшенко [26], Е.А. Степанова [29], Н.Н. Куняев [20], А.С. Дёмушкин [16] и другие.

**Методы исследования:** анализ и синтез научной литературы по теме исследования, сравнение и обобщение, системный подход к изучению конфиденциальных документов, разработка инструкции по работе с документами с ограниченным доступом в архиве.

**Опытно-экспериментальной базой исследования** является отдел архива муниципального казенного учреждения «Центр ресурсного обеспечения образовательных учреждений города Кирова».

**Теоретическая значимость** работы заключается в том, чтов работе обобщен опыт исследований по данной теме, раскрыто содержание понятий конфиденциального делопроизводства и персональных данных, рассмотрены особенности конфиденциального делопроизводства в образовательных учреждениях.

Приведены способы создания и редактирования инструкции по работе с документами с ограниченным доступом в архиве.

**Практическая значимость:** материалы работы могут быть использованы как руководство специалиста архива, деятельность которого связана с обработкой конфиденциальных документов.

# 1 СПЕЦИФИКА КОНФИДЕНЦИАЛЬНОГО ДЕЛОПРОИЗВОДСТВА

# 1.1 Сущность и особенности конфиденциального делопроизводства

**Конфиденциальность информации –** обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя. [статья 2 Федерального закона «Об информации, информационных технологиях и о защите информации»]

Конфиденциальное делопроизводство распространяется на документы, которые содержат в себе сведения, составляющие коммерческую и служебную тайну. Информация, составляющая коммерческую или служебную тайну, не существует сама по себе. Она отображается в различных носителях, которые могут ее сохранять, накапливать и передавать. И защита этих видов тайны в итоге сводится к защите ее носителей.

Документы, содержащие информацию, составляющие коммерческую и служебную тайну, принято называть конфиденциальными [4], а процесс их изготовления и организацию работы с ними — конфиденциальным делопроизводством.

Организация и технология конфиденциального делопроизводства не описана ни одним государственным нормативным актом – технологию обладатель такой информации должен определить самостоятельно.

Конфиденциальное делопроизводство [9] определяется как деятельность, обеспечивающая документирование конфиденциальной информации, организацию работы с конфиденциальными документами и защиту содержащейся в них информации. При этом под документированием информации понимается процесс подготовки и изготовления документов, под организацией работы с документами – их учет, размножение, прохождение, исполнение, отправление, уничтожение, режим хранения и обращения.

Важная составляющая конфиденциального делопроизводства – защита содержащейся в конфиденциальных документах информации. 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 или установленного круга лиц, имеющих право работать с ней, если этот выход привел к получению информации лицами, не имеющими к ней санкционированного доступа.

Уязвимость документированной информации 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;
* искажение информации (несанкционированное изменение, несанкционированная модификация, подделка, фальсификация);
* блокирование информации;
* разглашение информации.

Конфиденциальное делопроизводство решает 2 задачи:

1. Документационное обеспечение всех видов конфиденциальной деятельности.
2. Защита документированной информации, образующейся в процессе конфиденциальной деятельности.

Первая задача имеет своей целью организацию и бесперебойное функционирование конфиденциальной деятельности в сфере любого вида производства и управления. Это требует от делопроизводства обеспечения нужд конфиденциальной деятельности полной, своевременной и достоверной документной информацией, организации исполнения и использования документов. Полноту документной информации характеризует ее объем, который, с одной стороны, должен быть достаточным для принятия управленческих решений и выполнения производственных заданий, с другой стороны, являться действительно необходимым, не содержащим избыточной, не нужной для деятельности предприятия информации.

Достоверность документной информации заключается, во-первых, в ее соответствии объективному состоянию того или другого вопроса и, во-вторых, в ее юридической силе, характеризующейся наличием и правильностью оформления соответствующих реквизитов. Своевременность документной информации означает, что за время обработки и передачи информации не изменилось состояние вопроса, к которому она относится. Организация исполнения документов включает в себя и оперативное доведение их до исполнителей, и обеспечение своевременного и качественного решения содержащихся в документах вопросов. Организация использования документов состоит в обеспечении как текущего, так и последующего, использования документной информации.

Вторая задача имеет своей целью обеспечение сохранности и конфиденциальности документированной информации, что требует создания и поддержания специальных условий хранения и обработки документов, гарантирующих надежную защиту документов и содержащейся в них информации.

**Особенности конфиденциального делопроизводства:**

* нормативное закрепление правил и порядка работы со всеми видами конфиденциальной информации, а также правил обеспечения ее безопасности;
* обеспечение ограниченного доступа только для санкционированных пользователей;
* четкое разграничение порядка, уровней доступа и обязанностей санкционированных пользователей;
* установление ответственности за регистрационный учет и хранение информации, за соблюдение порядка пользования документами;
* жесткая регламентация процессов составления, печати, обработки и уничтожения документов, включая стадию подготовки черновиков и проектов;
* обязательный учет каждого документа;
* обязательная регистрация каждого документа и материального объекта в специальном журнале;
* строгий контроль сроков исполнения, изучения и обработки;
* фиксация перемещения и местонахождения каждого документа;
* периодические проверки наличия конфиденциальных документов у исполнителей;
* строгие требования к условиям хранения, обеспечивающий безопасность информации, закрепленные внутренними нормативными документами.

Конфиденциальное делопроизводство [5] и защита информации в компании регламентируются Инструкцией по конфиденциальному делопроизводству.

## 1.2 Особенности обработки, хранения и последующего использования конфиденциальных документов

Работники учреждения, допущенные к конфиденциальным сведениям и документам, прежде чем получить доступ к ним, должны пройти инструктаж и ознакомиться с памяткой о сохранении коммерческой тайны предприятия. Памятка составляется службой безопасности с учётом специфики конкретного предприятия, подписывается заместителем директора и утверждается директором предприятия.

Ведение делопроизводства, обеспечивающего учёт и сохранность документов, содержащих конфиденциальную информацию, предусматривает выполнение ряда рекомендаций.

Приказом руководителя учреждения назначается должностное лицо, ответственное за учёт, хранение и использование документов, содержащих конфиденциальные сведения. Это может быть сотрудник, для которого работа с конфиденциальными документами является основной служебной обязанностью, или секретарь-референт учреждения. Эти лица несут персональную ответственность за утерю или утечку информации из них. Вновь принятые на работу сотрудники предупреждаются о возможной уголовной, административной и иной ответственности в соответствии с законодательством.

Все документы, содержащие конфиденциальную информацию, подлежат учёту и специальному обозначению. На документе проставляют гриф ограничения доступа с указанием номера экземпляра, обладателя этой информации. Гриф конфиденциальности, или гриф ограничения доступа к традиционному, машиночитаемому или электронному документу, представляет собой реквизит формуляра документа, свидетельствующий о конфиденциальности содержащихся в документе сведений и проставляемый на самом документе или сопроводительном письме к нему [Приложение В].

В номенклатуру дел организации в обязательном порядке включаются дела с грифами конфиденциальности и журналы регистрации конфиденциальных документов. В номенклатуре дел в графе «Номер дела» к соответствующему номеру дела добавляется отметка «КТ» («коммерческая тайна») или «К» («конфиденциально»).

Наименование грифов конфиденциальности выносится и на обложку дела.

После исполнения документы подшиваются в соответствующие дела. Документы с грифами конфиденциальности группируются в дела отдельно от документов общего делопроизводства.

Все дела с грифами конфиденциальности независимо от срока их хранения должны иметь внутреннюю опись, которая выполняет функцию учета документов внутри каждого дела и заполняется по мере подшивки в дело документов [Приложение Г].

Передача и отправка документов с грифами конфиденциальности [Приложение Д]:

Любое перемещение документов между структурными подразделениями необходимо производить через подразделение, ответственное за ведение конфиденциального делопроизводства, с внесением соответствующей информации в учетные формы.

Отправку конфиденциальных документов сторонним организациям целесообразно осуществлять только с сопроводительными письмами.

Отправка документов, содержащих конфиденциальную информацию, осуществляется заказными почтовыми уведомлениями с описью вложения, экспресс-почтой или лично под роспись на визовом экземпляре или на реестре передачи документов.

При отправке конфиденциальных документов применяют двойное пакетирование (вкладывание конверта в конверт): на внутреннем конверте указывается номер исходящего письма и соответствующий гриф конфиденциальности, на внешнем конверте указывается адрес получателя и номер исходящего письма без грифа конфиденциальности.

Документы с грифами конфиденциальности должны храниться в сейфах отдельно от дел общего делопроизводства.

Вынос документов с грифами конфиденциальности запрещается или осуществляется по специальному разрешению при уведомлении службы безопасности организации.

## 1.3 Носители конфиденциальной информации

Самыми распространенными носителями документированной конфиденциальной информации являются машинные и бумажные носители.

**Машинные носители:**

* жесткие магнитные диски;
* гибкие магнитные диски (дискеты);
* магнитные ленты [Приложение Б];
* магнитооптические диски;
* оптические диски.

**Бумажные носители:**

* для текстовых документов – спецблокноты [Приложение Б], отдельные листы бумаги, типовые формы документов, стенографические и рабочие тетради;
* для чертежно-графических документов – ватман, калька, миллиметровая бумага.

Спецблокнот предназначен для составления черновиков документов. Он представляет собой сброшюрованные и пронумерованные листы бумаги с линией отрыва и контрольным листком, в котором проставляются номера листов блокнота.

Рабочие тетради (сброшюрованные листы бумаги без линии отрыва) – 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. При этом типовые формы документов (бланки с трафаретным текстом) должны содержать только открытую информацию и иметь в соответствующих местах пропуски для последующего внесения конфиденциальной информации, как правило, количественного характера.

Перед взятием на учет носители должны быть оформлены следующим образом:

На обложках спецблокнотов сотрудник подразделения конфиденциального делопроизводства пишет или проставляет штампом слово «Спецблокнот» и в правом верхнем углу гриф конфиденциальности. Если листы спецблокнота не пронумерованы типографическим способом, то они нумеруются сотрудником подразделения конфиденциального делопроизводства.

На обложках рабочих и стенографических тетрадей указываются вид носителя, гриф конфиденциальности и фамилия исполнителя. Листы тетради нумеруются, на обороте последнего листа составляется подписываемая сотрудником конфиденциального делопроизводства заверительная подпись 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 проставляется: на всех носителях – гриф конфиденциальности, номер листов; дополнительно для носителей, предназначенных для чертежно-графических документов – количество листов, подразделение и фамилия исполнителя. На любом носителе, предназначенном для составления одного конкретного документа, указывается наименование этого документа.

## 1.4 Персональные данные и их защита

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, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация. [6]

Защита персональных данных – это комплекс мероприятий, позволяющий выполнить требования законодательства РФ, касающиеся обработки, хранению и передачи персональных данных граждан.

**Виды персональных данных:**

* общие (общедоступные);
* специальные;
* биометрические;
* иные.

**Общие персональные данные**

К ним законодательство о персональных данных относит базовые личные данные: ФИО, место регистрации, информация о месте работы, номер телефона, e-mail. Обычно эти данные и так известны некоторым другим людям, могут быть опубликованы в общедоступных источниках.

**Специальные персональные данные**

Информация о личности человека: расовая и национальная принадлежность, политические, религиозные и философские взгляды, состояние здоровья, информация о судимостях.

Специальные категории персональных данных отличаются от общих тем, что обычно находятся в закрытом доступе. Их можно узнать только лично у человека, либо сделав официальный запрос в больницу, полицию или суд. Чаще всего сообщать эти данные человек не обязан.

**Биометрические персональные данные**

Это физиологические или биологические особенности человека, которые используют для установления его личности. К ним могут относиться фотографии, отпечатки пальцев, группа крови, генетическая информация.

Однако все эти данные не всегда являются биометрическими. Согласно [разъяснению правительства](https://www.garant.ru/products/ipo/prime/doc/70342932/), они становятся такими, только если вы храните их с целью идентификации личности. Например, если на проходной стоит камера с распознаванием лиц, фотографии сотрудников будут биометрическими данными – именно по ним вы определяете личность человека.

**Иные персональные данные**

К ним относят всё, что нельзя отнести к общедоступным, специальным или биометрическим данным: принадлежность к определенной социальной группе, к примеру, членство в клубе, или корпоративные данные, например, то, что хранится в бухгалтерии: зарплата, периоды отпусков, стаж и так далее.

Иные данные сложнее всего отличить от специальных. Разница, следующая:

1. Специальные данные характеризуют человека как личность, часто человеку важно, чтобы посторонние их не знали.
2. Иные данные – это просто дополнительная информация, они часто могут меняться.

Так как архив работает с документами, которые принимаются из образовательных организаций, **раскроем особенности защиты персональных данных в образовательных учреждениях.**

В настоящее время в образовательных учреждениях активно внедряются информационные системы, осуществляющие обработку персональных данных [6], делопроизводство, бухгалтерские программы и др. Эти системы предназначены для ведения базы данных воспитанников, обучающихся, родителей и работников образовательных учреждений, оперативного управления учреждением. Образовательные учреждения должны отреагировать на требования законодательства о защите персональных данных участников образовательного процесса в первую очередь, т. к. речь идет о защите сведений, незаконное использование которых может серьезно отразиться на правах граждан.

Положения о защите персональных данных работников регламентируются:

* Конституцией Российской Федерации;
* Федеральным законом от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации";
* Федеральным законом от 27.07.2006 № 152-ФЗ "О персональных данных";
* Трудовым кодексом РФ (далее – ТК РФ).

В целях обеспечения защиты персональных данных работников в соответствии с этими федеральными законами приняты подзаконные нормативные правовые акты.

В соответствии со статьёй 3 Закона № 152-ФЗ персональными данными является любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных): фамилия, имя, отчество; год, месяц, дата и место рождения; адрес; семейное, социальное, имущественное положение; образование, профессия, доходы и другая информация.

Согласно статье 2 Закона № 152-ФЗ его целью является защита прав и свобод человека и гражданина при обработке его персональных данных, в том числе защита прав на неприкосновенность частной жизни, личную и семейную тайну.

Персональные данные относятся к категории конфиденциальной информации, которые указаны в Перечне сведений конфиденциального характера, утвержденном указом Президента РФ от 06.03.1997 № 188. Следовательно, работодатель, получающий доступ к персональным данным, должен обеспечить их конфиденциальность.

Закон № 152-ФЗ определяет требования к сбору и обработке (хранению, актуализации, использованию, раскрытию и предоставлению) персональных данных физических лиц во всех сферах, где используются персональные данные, в том числе в сфере трудовых правоотношений.

Деятельность любой организации при работе с конфиденциальной информацией регламентируется рядом нормативных документов:

* [Положение](http://kp-kollege.ru/document/local/pol_pers_dan2.pdf) по обработке персональных данных;
* Инструкция о порядке обеспечении конфиденциальности при обращении с информацией, содержащей персональные данные;
* [Политика](http://kp-kollege.ru/document/local/politika_person_dan.pdf) в отношении обработки персональных данных;
* [Регламент](http://kp-kollege.ru/document/local/reglament_bezopasnosti.pdf)реагирования на инциденты информационной безопасности;
* [Порядок](http://kp-kollege.ru/document/local/pol_por_ogran_dostup.pdf) учёта, хранения, выдачи и работы с документами, содержащими информацию ограниченного распространения;

При оформлении документов рекомендуется использовать ГОСТ Р 7.0.97-2016 «Система стандартов по информации, библиотечному и издательскому делу. Организационно-распорядительная документация. Требования к оформлению документов».

Большой поток документов ежегодно обрабатывается в приемной комиссии. Абитуриенты предоставляют в приемную комиссию следующий перечень документов:

* оригинал или ксерокопия документа об образовании;
* ксерокопия паспорта;
* 4 фотографии размером 3х4 см;
* медицинская справка. Медицинская справка действительна в течение 6 месяцев;
* копия сертификата о прививках;
* копия медицинского полиса;
* документы, подтверждающие результаты индивидуальных достижений: дипломы, грамоты, сертификаты, характеристики;
* копия документа об образовании (с приложением);
* копия СНИЛС;
* копия ИНН.

**Общедоступные данные**, т.е. доступ к эти данным могут иметь неограниченный круг лиц без соблюдения требований конфиденциальности:

* фамилия;
* имя;
* отчество;
* пол;
* группа;
* номер студенческого билета и зачетной книжки;
* фотографии, полученные при съёмке на публичных мероприятиях, проводимых колледжем.

Эти данные могут публиковаться в общедоступных источниках: стенды, статьи, сайты и т.п. без дополнительного согласия субъекта персональных данных.

Обучающийся может в любой момент потребовать удаления данных из общедоступного источника, подав необходимый запрос.

**Персональные данные, подлежащие защите:**

* дата и место рождения;
* гражданство;
* фотография;
* информация о документе, удостоверяющем личность;
* номер пенсионного страхового свидетельства;
* ИНН;
* номер и дата выдачи медицинского полиса;
* место жительства;
* контактная информация;
* информация о родственниках;
* сведения о выплатах (стипендии).

# 1.5 Технология работы с документами ограниченного доступа

Положение о порядке обращения со служебной информацией ограниченного распространения, утвержденного постановлением Правительства РФ от 3 ноября 1994 года № 1233 (ред. от 06.08.2020)определяет порядок обращения с документами и другими материальными носителями информации, содержащими информацию ограниченного распространения в Учреждении и вышестоящих организациях.

Государственная тайна – это защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-разыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации согласно Закону РФ от 21.07.1993 № 5485-1 «О государственной тайне». Положения Закона обязательны для исполнения на территории РФ и за ее пределам органами представительной, исполнительной и судебной власти, местного самоуправления, предприятиями, учреждениями и организациями, независимо от их организационно-правовой формы и формы собственности, должностными лицами и гражданами РФ, взявшими на себя обязательства либо обязанными по своему статусу исполнять требования законодательства РФ о государственной тайне.

По степени важности сведений государственные секреты делятся на государственную тайну и служебную тайну. Государственную тайну составляют сведения, разглашение (передача, утечка и т.д.) которых может оказать отрицательное воздействие на качественное состояние военно-экономического потенциала страны или повлечь другие тяжкие последствия для обороноспособности, государственной безопасности, экономических и политических интересов страны. Служебную тайну составляют охраняемые государством сведения в любой области науки, техники, производства и управления, разглашение (передача, утечка и т.д.) которых, может нанести ущерб интересам государства.

Перечень сведений, отнесенных к государственной тайне, утвержден Указом Президента РФ от 30.11.1995 № 1203. (Указ Президента Российской Федерации от 25.03.2021 г. № 178 «О внесении изменений в перечень сведений, отнесенных к государственной тайне, утвержденный Указом Президента Российской Федерации от 30 ноября 1995 г. № 1203»).

Законодательно закреплено деление всего документного (информационного) массива на общедоступные документы и документы ограниченного доступа. Документы ограниченного доступа содержат сведения, составляющие государственную, коммерческую, служебную и иную тайну. Выделение секретного делопроизводства как самостоятельного направления вызвано его спецификой.

К служебной информации ограниченного распространения относится несекретная информация, касающаяся деятельности Учреждения, ограничение на распространение которой диктуется служебной необходимостью. На документах, содержащих служебную информацию ограниченного распространения, проставляется пометка «Для служебного пользования».

Гриф ограничения доступа свидетельствует о конфиденциальности информации, содержащейся в документе, и наличии ограничения доступа и ознакомления с ней. Он проставляется на самом документе и/или на сопроводительной документации к нему.

Реквизит располагается на правом верхнем углу документа на расстоянии 100 мм от границы левого поля.

При определении степени конфиденциальности документов следует руководствоваться Положением о коммерческой тайне.

Гриф ограничения доступа проставляется не только на самом документа, но и на всех его частях, способных выступать в качестве самостоятельной единицы при работе с данным документом в процессе решения того или иного вопроса, например на приложении к документу.

Одновременно с наименованием гриф ограничения доступа должен содержать указание на номер экземпляра данного документа, например:

1. Секретные документы;
2. Государственные документы;
3. Документы, содержащие конфиденциальную информацию;
4. Внутриорганизационные документы.

Установлены следующие категории должностных лиц, уполномоченных передавать служебную информацию:

* директор Учреждения;
* заведующий отделом управления;
* методист отдела управления.

Должностные лица, принявшие решение об отнесении служебной информации к разряду ограниченного распространения, несут персональную ответственность за обоснованность принятого решения.

За разглашение служебной информации ограниченного распространения, за нарушение порядка обращения с документами, содержащими такую информацию, ответственные лица могут быть привлечены к дисциплинарной ответственности.

Прием, учет (регистрация) документов, содержащих информацию ограниченного распространения, осуществляет делопроизводитель. Документы с пометкой «Для служебного пользования»:

* создаются на автоматизированном рабочем месте с закрытым доступом в общую информационную систему Учреждения;
* передаются ответственным лицам под расписку в запечатанном конверте;
* пересылаются по почте заказными почтовыми отправлениями;
* регистрируются в специальном журнале;
* хранятся в закрытом доступе.

Уничтожение документов с пометкой «Для служебного пользования», утративших свое практическое значение, производится по акту.

## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

1. Конституция Российской Федерации [Электронный ресурс] : [принята всенародным голосованием 12 декабря 1993 г. с изменениями, одобренными в ходе общероссийского голосования 01 июля 2020 г.] – <http://www.pravo.gov.ru/>
2. Гражданский кодекс Российской Федерации (часть первая, вторая, третья и четвертая) [Электронный ресурс] : по состоянию на 01 апреля 2015 г. – <https://base.garant.ru/10164072/>
3. Кодекс Российской Федерации об административных правонарушениях от 31.12. 2001 г. № 195 – ФЗ (ред. от 14.07.2015 г.). [Электронный ресурс] – <https://docs.cntd.ru/document/901807667>
4. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ // Собрание законодательства Российской Федерации. – 2006 г. – с изм. от 30.12.2021. [Электронный ресурс] – <https://docs.cntd.ru/document/901990051>
5. Федеральный закон от 29.07. 2004 г. №98-ФЗ «О коммерческой тайне» (с изменениями на 9 марта 2021 года) [Электронный ресурс] – <https://docs.cntd.ru/document/901904607>
6. ГОСТ Р 7.0.104 – 2019 «Система стандартов по информации, библиотечному и издательскому делу «Отчёт о научно-исследовательской работе» [Электронный ресурс] – <http://docs.cntd.ru/document/gost-7-32-2001-sibid>
7. ГОСТ Р 7.0.97 – 2016 «Система стандартов по информации, библиотечному и издательскому делу «Организационно-распорядительная документация» [Электронный ресурс] – <https://docs.cntd.ru/document/1200142871>
8. ГОСТ Р 7.0.8 – 2013 «Система стандартов по информации, библиотечному и издательскому делу «Делопроизводство и архивное дело» [Электронный ресурс] – <https://docs.cntd.ru/document/1200108447>
9. ГОСТ Р 2.051‒2006 ЕСКД «Электронные документы. Общие положения» [Электронный ресурс] − <https://docs.cntd.ru/document/1200045526>
10. ГОСТ Р 7.0.8 – 2013 «Система стандартов по информации, библиотечному и издательскому делу «Делопроизводство и архивное дело» [Электронный ресурс] − <https://docs.cntd.ru/document/1200108447>
11. ГОСТ Р 7.0.8–2013 «СИБИД. Делопроизводство и архивное дело. Термины и определения» [Электронный ресурс] − <https://docs.cntd.ru/document/1200108447>
12. Алексенцев, А.И. Конфиденциальное делопроизводство // Секретарское дело [Текст]. 2004. № 8-9. С. 109-191.
13. Басаков, М.И. Делопроизводство [Документационное обеспечение управления] [Текст]: учебник/Басаков М.И., Замыцкова О.И. – Ростов-на-Дону: Феникс, 2014. – 376 c.
14. Бурова Е.М. Архивоведение (теория и методика): учебник для вузов [Текст] / Е.М. Бурова, Е.В. Алексеева, Л.П. Афанасьева; под ред. Е.М. Буровой, – М.: Издательский дом МЭИ, 2012. – 483 с.
15. Галахов, В.В., Секретарское дело (образцы документов, организация и технология работы) [Текст] / В.В. Галахов, И.И. Корнеев – М.: Проспект, 2006. – 152 с.
16. Демушкин, А.С. Электронный документооборот: термины и определения // Служба кадров и персонал [Текст] / А.С. Демушкин. – ИрГУПС, 2008. №5. – 122 с.
17. Егоров, В.П. Делопроизводство и режим секретности [Текст]: учеб. пособие / Егоров В.П., Слиньков А.В.– М.: Юридический институт МИИТ, 2016. — 185 с.
18. Козырева, В. П. Организуем работу с документами ограниченного доступа [Текст] / В. П. Козырева // Делопроизводство и документооборот на предприятии. – 2007. – №12. – 7-21 с.
19. Кудряев, В.А. Организация работы с документами [Текст]: Учебник / под ред. проф. В. А. Кудряева. – М.: ИНФРА‒М, 2003. – 592 с.
20. Куняев, Н.Н., Дёмушкин А.С., Фабричников А.Г. Конфиденциальное делопроизводство и защищённый электронный документооборот [Текст]: учебник. – Москва: Логос, 2020. – 500 с.
21. Ларин, М.В. Электронные документы в управлении [Текст]: науч.‒метод. Пособие / М.В. Ларин, О.И. Расков. – М.:ВНИИДАД, 2005. – 57 с.
22. Суровцева, Н.Г. Электронный документ: к проблеме идентификации // Вестник РГГУ. [Текст] Серия: Документоведение и архивоведение. Информатика. Защита информации и информационная безопасность. 2017. № 3 (9). 18–28 с.
23. Шкаричев, А.В. Отличие конфиденциального делопроизводства от обычного [Текст] Шкаричев А.В. // Делопроизводство и документооборот на предприятии. – 2011. – №12. – 43-45 с.

**Электронные ресурсы**

1. Требования к защите персональных данных при их обработке в информационных системах персональных данных [сайт]: <http://www.consultant.ru/document/cons_doc_LAW_137356/8c86cf6357879e861790a8a7ca8bea4227d56c72/>
2. Аверченков, В.И. Защита персональных данных в организации / В.И. Аверченков, М.Ю. Рытов, Т.Р. Гайнулин. – 3-е изд., стер. – М. : Издательство «Флинта» [сайт], 2016. – 124 с. – Режим доступа: <https://biblioclub.ru/index.php?page=book&id=93260>
3. Корнеев*,* И.К. Документационное обеспечение управления : учебник и практикум для среднего профессионального образования / И.К. Корнеев, А.В. Пшенко, В.А. Машурцев. – 2-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2023. – 384 с. – (Профессиональное образование). — ISBN 978-5-534-05022-6. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – Режим доступа: <https://urait.ru/bcode/514640>
4. Сергеева, Ю.С. Защита информации: Конспект лекций / Ю.С. Сергеева. [сайт] – М. : АПриор, 2011. – 128 с. – Режим доступа: <https://biblioclub.ru/index.php?page=book&id=72670>
5. Спичак, А.В. Конфиденциальное делопроизводство : учебное пособие. – Нижневартовск [сайт]: НВГУ, 2020. – 118 с. – Режим доступа: <https://nvsu.ru/ru/Intellekt/2281/Spichak,_A._V._Konfidencialnoe_deloproizvodstvo1.pdf>
6. Степанова, В.В., Савельева А.В., Кайда О.А., Судник Т.В. «Документационное сопровождение кадровой деятельности» [сайт] – Режим доступа: <https://www.studmed.ru/stepanova-v-v-saveleva-a-v-kayda-o-a-sudnik-t-v-dokumentacionnoe-soprovozhdenie-kadrovoy-deyatelnosti_9448e52fcc5.html>

# ПРИЛОЖЕНИЯ

# ПРИЛОЖЕНИЕ А

**Понятийно-категориальный аппарат**

1. Документ – зафиксированная на носителе информация с реквизитами, позволяющими ее идентифицировать. [12]
2. Электронный документ (ЭД) – документ, информация которого представлена в электронной форме. [10]
3. Документационное обеспечение управления – деятельность, охватывающая организацию документирования и управления документацией в процессе реализации функций учреждения, организации и предприятия. [15]
4. Конфиденциальный документ – это необходимым образом оформленный носитель документированной информации, который содержит сведения ограниченного доступа или использования, которые составляют интеллектуальную собственность юридического или физического лица. [13]
5. Конфиденциальное делопроизводство – это деятельность, обеспечивающая не только документирование и организацию работы с конфиденциальными документами, но и защиту от несанкционированного доступа и использования. [13]
6. Персональные данные – это сведения, относящиеся к прямо или косвенно определённому или определяемому физическому лицу, которые могут быть предоставлены другим лицам. [13]
7. Гриф ограничения доступа к документу – это реквизит официального документа, свидетельствующий об особом характере информации, ограничивающий круг пользователей документа. [12]
8. Государственная тайна — это защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной, оперативно-розыскной деятельности, распространение которых может нанести ущерб государству. [13]
9. Шаблон документа – особый вид документа, предоставляющий специальные средства для стандартного оформления документа, содержащий одинаковый для этих документов текст, стили оформления, макросы, панели инструмента. [18]
10. Информация ограниченного доступа, не содержащая сведений, составляющих государственную тайну (конфиденциальная информация) – это информация, доступ к которой ограничен федеральными законами. [20]
11. Служебная тайна — служебные сведения, которые не относятся к государственной тайне, доступ к которым ограничен органами государственной власти и федеральными органами исполнительной власти в соответствии с законодательством.
12. Профессиональная тайна — сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ и федеральными законами.

# ПРИЛОЖЕНИЕ Б

**Носители информации**

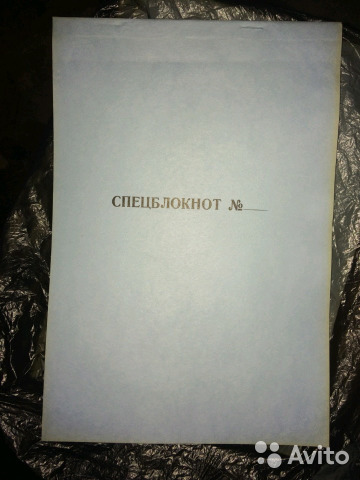


Рисунок 1 – Пример спецблокнота

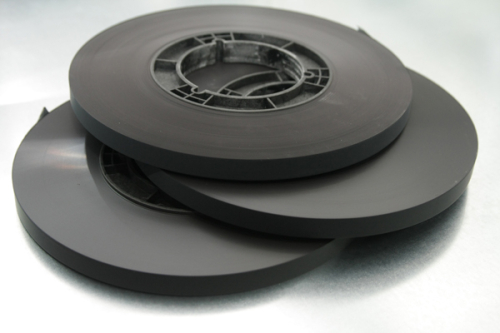


Рисунок 2 – Пример магнитных лент

# ПРИЛОЖЕНИЕ В

**Виды конфиденциальных документов**

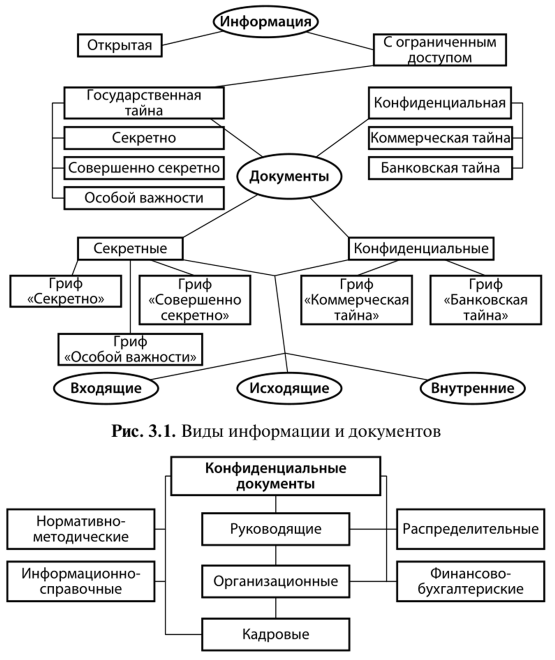


Рисунок 3 – Виды информации документов



Рисунок 4 – Конфиденциальные документы

# ПРИЛОЖЕНИЕ Г

**Учёт документов**



Рисунок 5 - Журнал регистрации внутренних документов с грифами конфиденциальности



Рисунок 6 – Внутренняя опись документов

# ПРИЛОЖЕНИЕ Д

**Конфиденциальный документооборот**

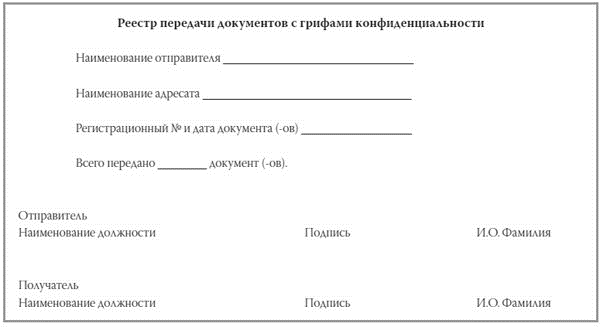


Рисунок 7 – Реестр передачи документов с грифами конфиденциальности

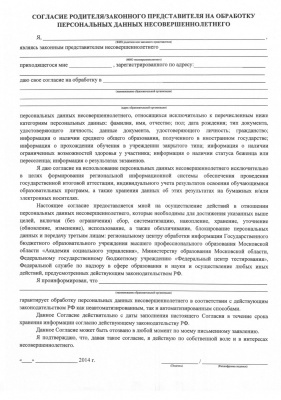


Рисунок 8 − Согласие на обработку персональных данных