Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «Нижневартовский государственный университет»
Гуманитарный факультет
Кафедра документоведения и всеобщей истории

А.В. Спичак

КОНФИДЕНЦИАЛЬНОЕ ДЕЛОПРОИЗВОДСТВО

Учебное пособие

Нижневартовск
2020

ББК 60.844я73
С 72

Печатается по постановлению редакционно-издательского совета
Нижневартовского государственного университета

Рецензенты:

доктор исторических наук, доцент, профессор кафедры государственного
и муниципального управления Поволжского института управления им. П.А. Столыпина
(филиал ФГБОУ ВО «Российская академия народного хозяйства и государственной
службы при Президенте Российской Федерации»)
А.В. Ермолаева;
кандидат исторических наук, доцент, заведующая кафедрой менеджмента
БУ ПО ХМАО-Югры «Нижневартовский социально-гуманитарный колледж»
Т.В. Судник;
кандидат исторических наук, доцент, ведущий специалист
учебно-методического управления ФГБОУ ВО «Российская академия народного
хозяйства и государственной службы при Президенте Российской Федерации»
М.В. Угрюмова

Спичак, А.В.

С 72 **Конфиденциальное делопроизводство** : учебное пособие. – Нижневартовск: НВГУ, 2020. – 118 с.

ISBN 978-5-00047-558-4

В учебном пособии рассмотрены актуальные проблемы организации конфиденциального делопроизводства и защиты конфиденциальной информации в организациях. Пособие призвано содействовать складыванию устойчивых и целостных представлений о документировании конфиденциальной информации, организации конфиденциального документооборота и разрешительной системы доступа в организациях, выявлении потенциальных угроз безопасности информации и защите конфиденциальных сведений.

Для студентов, обучающихся по направлениям 46.03.02 «Документоведение и архивоведение» (бакалавриат, профили «Документоведение» и «Кадровое делопроизводство») и 46.04.02 «Документоведение и архивоведение» (магистратура, профиль «Документационное обеспечение органов государственной и муниципальной власти»).

ББК 60.844я73

ISBN 978-5-00047-558-4

ПРЕДИСЛОВИЕ

Конфиденциальное делопроизводство следует определять как деятельность, обеспечивающую документирование конфиденциальной информации, организацию работы с конфиденциальными документами и защиту содержащейся в них информации.

Конфиденциальное делопроизводство в целом базируется на тех же принципах, что и открытое делопроизводство, но в то же время имеет отличия, обусловленные конфиденциальностью документированной информации. Эти отличия касаются сферы конфиденциального делопроизводства и охватываемых им видов работ с документами.

По видам работ конфиденциальное делопроизводство отличается от открытого, с одной стороны, бóльшим их количеством, с другой – содержанием и технологией выполнения многих видов. Помимо этого, третья составляющая конфиденциального делопроизводства – защита содержащейся в конфиденциальных документах информации – вообще не предусмотрена в определении открытого делопроизводства, хотя определяемая собственником часть открытой информации должна защищаться от утраты. Конфиденциальная информация должна защищаться от утраты и утечки.

Конфиденциальное делопроизводство шире открытого и по своим задачам. Если задачей открытого делопроизводства является документационное обеспечение управленческой деятельности, то конфиденциальное делопроизводство должно осуществлять решение двух задач: документационное обеспечение всех видов конфиденциальной деятельности; защита документированной информации, образующейся в процессе конфиденциальной деятельности.

Цель дисциплины «Конфиденциальное делопроизводство» заключается в формировании у студентов представления об основных этапах организации конфиденциального делопроизводства в организации.

Место дисциплины в структуре ООП: относится к циклу профессиональных дисциплин.

Для освоения курса конфиденциального делопроизводства студенты используют знания, умения и навыки, сформированные в ходе изучения дисциплин «Документоведение», «Архивоведение», «Организация и технология документационного обеспечения управления», «Системы электронного документооборота», «Нормативная правовая основа документоведения и архивоведения», «Организация и технологии хранения документов» и т. д.

Процесс изучения дисциплины направлен на формирование следующих компетенций:

ПК-17. Владение методами защиты информации	ПК-17.1. *Знает:* основные понятия информационных ресурсов и параметры информации; информационной безопасности; современных методов и средств защиты информации в информационно-телекоммуникационных системах. ПК-17.2. *Умеет:* проводить оценку угроз безопасности объекта информатизации; применять методики оценки уязвимости в информационно-телекоммуникационных сетях. ПК-17.3. *Владеет:* методами и средствами защиты информации.
ПК-25. Владение навыками подготовки управленческих документов и ведения деловой переписки	ПК-25.1. *Знает:* характеристики и состав различных систем документации; правила составления и требования к оформлению документов. ПК-25.2. *Умеет:* составлять документы на любом носителе в зависимости от назначения, содержания и вида документа; самостоятельно разрабатывать проекты управленческих документов в соответствии с нормативными требованиями; унифицировать и проектировать формы документов.

	ПК-25.3. *Владеет:* знаниями нормативных требований в области документационного обеспечения управления; навыками использования правил подготовки управленческих документов и ведения деловой переписки.
ПК-26. Владение навыками обработки документов на всех этапах документооборота, систематизации, составления номенклатуры дел	ПК-26.1. *Знает:* теоретические подходы и основные принципы и методы упорядочения документов; порядка организации документов в комплексы. ПК-26.2. *Умеет:* анализировать состав документации организации в соответствии с установленными требованиями; реализовывать на практике упорядочение комплексов документов и информационных потоков в соответствии с установленными методами и приемами; обрабатывать документы на всех этапах документооборота, систематизировать и составлять номенклатуру дел. ПК-26.3. *Владеет:* принципами и методами упорядочения состава документов и информационных показателей; навыками обработки документов на всех этапах документооборота; навыками сбора, обобщения, систематизации и анализа фактических данных; навыками составления номенклатуры дел.

Глава 1
НОРМАТИВНАЯ БАЗА ДЛЯ РАБОТЫ С КОНФИДЕНЦИАЛЬНЫМИ ДОКУМЕНТАМИ

1.1. Конфиденциальная информация: содержание понятия и особенности

Конфиденциальность информации – понятие объемное. Оно охватывает разные отрасли экономики и сферы общественной жизни, для каждой из которых есть свои особенности правового регулирования.

Следующий обзор российского законодательства поможет разобраться в том, какие данные следует отнести к конфиденциальной информации и какие законы определяют сохранность конфиденциальности [16].

Определение конфиденциальности информации дается в Федеральном законе Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – Закон об информации).

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

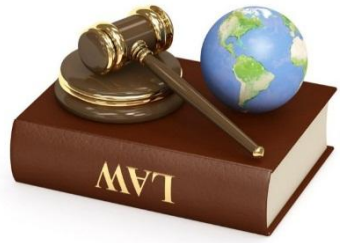
Обладатель информации – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам [6].

Обладателями информации могут быть гражданин (физическое лицо), юридическое лицо, государственные органы и органы местного самоуправления в пределах их полномочий [15, с. 18].

Согласно ГОСТ Р 7.0.8-2013 **документированная информация** – это структурированная информация, зафиксированная на носителе, а **документ** – зафиксированная на носителе информация с реквизитами, позволяющими ее идентифицировать [9].

Соответственно, документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации, является конфиденциальной документированной информацией (далее – КДИ) или конфиденциальным документом (далее – КД), за исключением информации, которая составляет государственную тайну, имеющую свой правовой режим. Защита информации, составляющей государственную тайну, осуществляется в соответствии с законодательством Российской Федерации о государственной тайне [15, с. 11].

1.2. Международная охрана интеллектуальной собственности



Получив патент, владелец объекта интеллектуальной собственности приобретает законодательную защиту от неправомерных действий третьих лиц. Однако охрана интеллектуальной собственности будет осуществляться только в пределах страны, аналогичные защитные меры за границей будут установлены только при регистрации прав на международном уровне.

Правовая основа международной охраны интеллектуальной собственности

Национальное законодательство в сфере авторского и патентного права распространяется только на правоотношения в пределах страны. В Российской Федерации базовым законодательным актом является часть четвертая Гражданского кодекса Российской Федерации. Получив авторское свидетельство или патент, правообладатель может требовать устранения нарушений своих интересов, взыскать компенсацию убытков и т. д.

При осуществлении деятельности на территории одного или нескольких иностранных государств наличие национального патента не поможет защитить свою интеллектуальную собственность. Однако на международном уровне уже более века существует система договоров и конвенций, позволяющих регистрировать и защищать интеллектуальные права.

Выделим наиболее важные международные акты, которые направлены на охрану интеллектуальной собственности:

- Мадридское соглашение о регистрации товарных знаков (1891 г.), а также Мадридский протокол к указанному документу;
- Конвенция по охране промышленной собственности (1883 г.);
- Договор о патентной кооперации (1970 г.);
- Евразийская патентная конвенция (1994 г.);
- Всемирная конвенция об авторском праве (1952 г.);
- Бернская конвенция по охране литературных и художественных произведений (1886 г.).

По правилам указанных международных актов интеллектуальная собственность будет защищаться путем подачи заявки через национальное патентное ведомство. Охрана отдельных объектов будет осуществляться по специальным принципам. Например, положения Бернской конвенции предусматривают режим охраны литературных произведений на территории всех стран-участниц, если авторское право было зарегистрировано в одном из указанных государств.

Общие принципы охраны интеллектуальных прав на международном уровне таковы:

- большинство международных актов в сфере интеллектуальной собственности позволяют оформить патент для охраны на территории одного или нескольких государств, указанных в заявке, однако Евразийская конвенция распространяет режим защиты патентных прав сразу на все страны (если такое условие было включено в заявку);
- лицо, обладающее действующим патентом на территории своего государства, получает приоритет заявки при обращении за охраной в страну – участницу Конвенций (срок приоритета составляет 12 месяцев);

- охрана предоставляется на определенный срок (например, на 10 лет), после чего необходимо обратиться за продлением патента.

Таким образом, международное патентное право признает приоритет авторов и правообладателей при условии подачи ими заявки на установление охраны за пределами своего государства.

Рассмотрим, как происходит установление охраны интеллектуального права на территории одного или нескольких иностранных государств.

Международная охрана промышленной собственности

Необходимость установления охраны объекта за пределами страны определяет сам правообладатель. Как правило, это связано с предстоящим выходом бизнеса на новые рынки, а наличие патента позволит устранить любые попытки конкурентов воспользоваться чужими разработками и идеями. Алгоритм действий, которые предстоит выполнить правообладателю для получения международной охраны своего объекта, выглядит следующим образом:

- подается заявка в национальное патентное ведомство, т. е. в службу Роспатента, при этом подтверждается легальность прав на объект в пределах страны (процедура получения международной охраны может быть начата сразу после подачи заявки по внутреннему законодательству);
- в заявке приводится перечень иностранных государств, для территории которых испрашивается охрана (Евразийской конвенций установлен иной порядок регистрации прав);
- проводится поиск по международным реестрам интеллектуальной собственности, публикуется заявка, осуществляется предварительная экспертиза патентоспособности для каждого из выбранных государств;
- после получения информации соискатель должен еще раз подтвердить перечень стран, в которых будет установлена охрана;
- через национальное патентное ведомство заявки направляются в аналогичные органы выбранных государств.

Приоритет, устанавливаемый для защиты интересов правообладателя, позволяет устранить регистрацию аналогичных объектов интеллектуальной собственности со стороны конкурентов.

Особенности Евразийской конвенции при международной охране прав

Евразийская патентная конвенция была утверждена государствами, входящими в СНГ. Ключевая цель этого акта – распространить охрану права интеллектуальной собственности сразу на территорию всех стран-участниц. Правовой режим охраны будет установлен после выдачи евразийского патента, а заявку будет рассматривать Евразийское патентное ведомство. Подать заявку также допускается через национальные структуры.

Выделим особенности, которыми характеризуется охрана объектов по евразийскому патенту:

- охрана устанавливается на 20 лет, однако правообладатель обязан ежегодно перечислять пошлины на поддержание его в силе;
- правообладатель должен ежегодно подтверждать перечень государств СНГ, на территории которых будет действовать охрана (размер пошлин также рассчитывается в зависимости от количества выбранных стран);
- одновременно с Евразийской конвенций РФ заключены отдельные прямые соглашения с несколькими странами СНГ (например, с Республикой Беларусь), которые вводят дополнительные правила по регистрации и охране интеллектуальной собственности.

Оформление и подача заявок для международной охраны может осуществляться правообладателем самостоятельно либо через патентные бюро. Во втором случае намного

проще и быстрее пройдет процедура поиска аналогичных объектов интеллектуальной собственности через международные реестры [13].

Международные учреждения по охране интеллектуальной собственности

В области охраны интеллектуальной собственности существует два основных института международного уровня и ряд региональных организаций. Основными международными организациями являются Всемирная организация интеллектуальной собственности (ВОИС) и Всемирная торговая организация (ВТО). Важнейшей среди региональных организаций является Европейский союз. Эти организации выполняют очень важные функции. ВОИС и ВТО отвечают за составление и пересмотр основных международных договоров в области охраны интеллектуальной собственности. Они не только разрабатывают такие договоры, но и в определенных случаях принудительно осуществляют их исполнение. Европейский союз открыл региональное бюро по товарным знакам и в настоящее время занимается разработкой регионального законодательства о товарных знаках. Кроме того, вынашиваются планы создания Европейского патентного союза [14].

Всемирная организация интеллектуальной собственности (ВОИС) – это старейшая и наиболее крупная из всех международных организаций, занимающихся вопросами интеллектуальной собственности. Всемирная торговая организация (ВТО) была создана в 1995 г. в результате многосторонних переговоров о совершенствовании Генерального соглашения по тарифам и торговле [18].

Роспатент представляет интересы Российской Федерации во Всемирной организации интеллектуальной собственности (ВОИС) (http://www.wipo.int), принимает активное участие в работе руководящих органов и комитетов экспертов ВОИС, выполняет функции Получающего ведомства, Международного поискового органа, Органа международной предварительной экспертизы в рамках Договора о патентной кооперации (PCT), а также функции в рамках Мадридской системой международной охраны товарных знаков.

Роспатент – это федеральное агентство, ведущее контроль за использованием прав на интеллектуальную собственность.

Начиная с 2006 г., у российских заявителей, подающих международные заявки на изобретения по системе PCT, появилась возможность использования двух основных бланков (Заявление и Требование), разработанных в редактируемом PDF-формате.

С 1 декабря 2007 г. в рамках Соглашения о взаимодействии с помощью электронных средств между ВОИС и Роспатентом в соответствии с процедурами Мадридской системы международной регистрации товарных знаков осуществлен первый этап перехода на электронный документооборот с ВОИС, позволяющий значительно снизить трудозатраты экспертного состава на подготовку решений по быстрорастущему числу международных регистраций товарных знаков, содержащих указание Российской Федерации.

Роспатент, как и другие патентные ведомства, предпринимает координируемые ВОИС усилия по гармонизации соответствующих национальных норм и правил. Гармонизация направлена на установление одинаковых или совместимых процедур приобретения

прав интеллектуальной собственности, разрешения споров, борьбы с нарушением прав интеллектуальной собственности.

5 февраля 2009 г. на территории Российской Федерации вступили в силу Договор ВОИС по исполнениям и фонограммам (ДИФ) и Договор ВОИС по авторскому праву (ДАП).

Роспатентом подготовлены и направлены на согласование в соответствующие органы исполнительной власти пакеты документов для осуществления внутригосударственной процедуры по присоединению Российской Федерации к Договору о патентном праве (PLT) и ратификации Сингапурского договора о законах по товарным знакам (STLT).

В результате многолетнего сотрудничества Роспатента с Всемирной академией ВОИС (ВА ВОИС) успешно действует курс дистанционного обучения «Основы интеллектуальной собственности» на русском языке. Курс позволяет учащимся как из России, так и из других стран получить представление об основных объектах интеллектуальной собственности, а также о функционировании международных договоров в этой области. По результатам обучения выдается свидетельство ВА ВОИС. Более подробная информация о сотрудничестве с ВОИС содержится в годовых отчетах Роспатента на официальном сайте агентства.

Международные конвенции и договоры по линии ВОИС

В области охраны промышленной собственности

- Парижская конвенция по охране промышленной собственности;
- Мадридское соглашение о международной регистрации знаков;
- Протокол к Мадридскому соглашению о международной регистрации знаков;
- Мадридское соглашение о пресечении ложных и вводящих в заблуждение указаний происхождения на товарах;
- Гаагское соглашение о международной регистрации промышленных образцов;
- Ниццкое соглашение о международной классификации товаров и услуг для регистрации знаков;
- Лиссабонское соглашение об охране наименований мест происхождений и их международной регистрации;
- Конвенция, учреждающая Всемирную организацию интеллектуальной собственности;
- Локарнское соглашение о международной классификации промышленных образцов;
- Договор о патентной кооперации (PCT);
- Страсбургское соглашение о международной патентной классификации;
- Венское соглашение об учреждении Международной классификации изобразительных элементов знаков;
- Будапештский договор о международном признании депонирования микроорганизмов для целей патентной процедуры;
- Найробский договор об охране олимпийского символа;
- Договор о законах по товарным знакам (TLT 1994);
- Договор о патентном праве (PLT);
- Сингапурский договор о законах по товарным знакам.

В области охраны авторского права и смежных прав

- Бернская конвенция об охране литературных и художественных произведений;
- Международная конвенция об охране прав исполнителей, изготовителей фонограмм и вещательных организаций (Римская конвенция);

- Конвенция об охране интересов производителей фонограмм от незаконного воспроизводства их фонограмм (Женевская конвенция);
- Конвенция о распространении несущих программы сигналов, передаваемых через спутник (Брюссельская конвенция);
- Договор о международной регистрации аудиовизуальных произведений;
- Договор ВОИС по авторскому праву;
- Договор ВОИС по исполнениям и фонограммам;
- Пекинский договор по аудиовизуальным исполнениям;
- Марракешский договор для облегчения доступа слепых и лиц с нарушениями зрения или иными ограниченными способностями воспринимать печатную информацию к опубликованным произведениям;
- договоры, не вступившие в силу;
- Вашингтонский договор об интеллектуальной собственности в отношении интегральных микросхем [15].

Всемирная торговая организация (ВТО) – единственный международный орган, занимающийся глобальными правилами торговли между государствами, заменившая собой в 1995 г. Генеральное соглашение по тарифам и торговле (ГАТТ).

В Европейский союз входят страны, в которых уже в течение длительного времени действуют эффективные системы охраны интеллектуальной собственности. Страны – члены ЕС и руководящие органы ЕС в политике охраны интеллектуальной собственности ставят ряд задач:

- усиление охраны интеллектуальной собственности;
- предупреждение использования прав на интеллектуальную собственность в недобросовестной конкуренции;
- гармонизация законодательства об интеллектуальной собственности;
- снижение уровня дублирования усилий национальных патентных служб и структур, занимающихся товарными знаками;

Для достижения этих целей в ЕС используется ряд механизмов:

- издание обязательных директив;
- участие в работе основных международных организаций и в подготовке договоров;
- подготовка договоров присоединения для стран – членов ЕС (в некоторых случаях открытых и для других стран);
- создание собственных институтов, в частности Европейского патентного бюро и Европейского бюро по товарным знакам.

В 1994 г. Российской Федерацией и Европейским союзом подписано Соглашение о партнерстве и сотрудничестве, которое вступило в силу для России 1 декабря 1997 г. Указанное Соглашение носит комплексный характер, поскольку предусматривает развитие политического диалога, содействие торговле, инвестициям и гармоничным экономическим отношениям между сторонами. Особое внимание в Соглашении уделено обеспечению

должного уровня охраны и реализации прав интеллектуальной собственности, чему посвящены ст. 54 Соглашения и Приложение 10 [14].

Охрана коммерческой тайны в международных договорах

Минимальные международные стандарты по защите коммерческой тайны установлены в некоторых конвенциях и в Соглашении ТРИПС.

Соглашение по торговым аспектам прав интеллектуальной собственности (ТРИПС) или Соглашение ТРИПС (англ. Agreement on Trade-Related Aspects of Intellectual Property Rights, сокращенно TRIPS) – это первое крупное многостороннее международное соглашение, обеспечивающее охрану коммерческой тайны и входящее в пакет документов о создании Всемирной торговой организации.

Так, в ст. 10 bis Парижской конвенции по охране промышленной собственности говорится:

«1. Страны Союза обязаны обеспечить гражданам стран, участвующих в Союзе, эффективную защиту от недобросовестной конкуренции.

2. Актом недобросовестной конкуренции считается всякий акт конкуренции, противоречащий честным обычаям в промышленных и торговых делах».

Сложно утверждать, что смыслом изложенного охватывается понятие коммерческой тайны. Тем не менее, в ст. 39 Соглашения ТРИПС говорится:

«1. В процессе обеспечения эффективной защиты от недобросовестной конкуренции, как это предусмотрено ст. 10 bis Парижской конвенции (1967), страны-участницы должны охранять закрытую информацию ... и данные, предоставляемые их правительствам ...». Далее в названной статье детализируются правила охраны закрытой информации.

В тексте же рассматриваемого документа термин «закрытая информация» использован для того, чтобы подчеркнуть, что защита должна идти значительно дальше узких концепций XIX в., например таких, как «секреты производства».

Положениями Соглашения ТРИПС определяется минимальный объем понятия охраны коммерческой тайны как защиты информации, которая на законных основаниях контролируется юридическим или физическим лицом и которая

- является секретной в том смысле, что она либо в целом, либо в конкретном сочетании или расположении ее компонентов не является известной или легко доступной лицам, принадлежащим к определенному кругу, обычно имеющему дело с подобными видами информации;
- имеет коммерческую ценность ввиду ее секретности;
- в конкретных обстоятельствах была подвергнута определенным разумным мерам охраны лицом, контролирующим эту информацию на законных основаниях, в целях сохранения ее секретности.

Данное определение включает три элемента:

- секретность;
- коммерческая ценность;
- меры по сохранению секретности [14].

Международные правовые нормы в сфере защиты персональных данных

Можно выделить три основные тенденции международно-правового регулирования института защиты персональных данных, относимого к процессам автоматизированной обработки информации.

1) Декларирование права на защиту персональных данных как неотъемлемой части фундаментальных прав человека в актах общегуманитарного характера, принимаемых в рамках международных организаций.

2) Закрепление и регулирование права за защиту персональной информации в актах регулятивного характера Европейского союза, Совета Европы, отчасти Содружества Независимых Государств и некоторых региональных международных организаций. Этот класс норм – наиболее универсальный и непосредственно касается прав на защиту персональных данных в процессах автоматизированной обработки информации.

3) Включение норм об охране конфиденциальной информации (в том числе персональной) в международные договоры.

Первый способ исторически появился раньше остальных. В современном мире информационные права и свободы являются неотъемлемой частью фундаментальных прав человека.

Всеобщая декларация прав человека 1948 г. провозглашает: «Никто не может подвергаться произвольному вмешательству в личную и семейную жизнь, произвольным посягательствам на … тайну его корреспонденции», и далее: «Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств». Международный пакт о гражданских и политических правах 1966 г. в этой части повторяет декларацию. Европейская Конвенция 1950 г. детализирует это право: «Каждый человек имеет право на свободу выражения своего мнения. Это право включает свободу придерживаться своего мнения, получать и распространять информацию и идеи без вмешательства со стороны государственных органов и независимо от государственных границ».

Указанные международные документы закрепляют информационные права человека.

В настоящее время на международном уровне сформировалась устойчивая система взглядов на информационные права человека. В обобщенном плане это право на получение информации, право на частную жизнь с точки зрения охраны информации о ней, право на защиту информации как с точки зрения безопасности государства, так и с точки зрения безопасности бизнеса, включая финансовую деятельность.

Второй способ – более детального регулирования права на защиту персональной информации – связан со всевозрастающей в последние годы интенсивностью обработки персональной информации с помощью автоматизированных компьютерных информационных систем. В последние десятилетия в рамках ряда международных организаций был принят комплекс международных документов, развивающих основные информационные права в связи с интенсификацией трансграничного обмена информацией и использованием современных информационных технологий. Среди таких документов можно назвать следующие акты.

Совет Европы в 1980 г. разработал Европейскую конвенцию о защите физических лиц в вопросах, касающихся автоматической обработки личных данных, вступившую в силу в 1985 г. В Конвенции определяется порядок сбора и обработки данных о личности, принципы хранения и доступа к этим данным, способы физической защиты данных. Конвенция гарантирует соблюдение прав человека при сборе и обработке персональных данных, принципы хранения и доступа к этим данным, способы физической защиты данных, а также запрещает обработку данных о расе, политических взглядах, здоровье, религии без соответствующих юридических оснований. Россия присоединилась к Европейской конвенции в ноябре 2001 г.

В Европейском союзе вопросы защиты персональных данных регулируются целым комплексом документов. В 1979 г. была принята Резолюция Европарламента «О защите прав личности в связи с прогрессом информатизации». Резолюция предложила Совету и Комиссии Европейских сообществ разработать и принять правовые акты по защите данных о личности в связи с техническим прогрессом в области информатики. В 1980 г. при-

няты рекомендации Организации по сотрудничеству стран – членов Европейского союза «О руководящих направлениях по защите частной жизни при межгосударственном обмене данными персонального характера». В настоящее время вопросы защиты персональных данных детально регламентируются директивами Европарламента и Совета Европейского союза. Это директивы № 95/46/ЕС и № 2002/58/ЕС Европейского парламента и Совета Европейского союза от 24 октября 1995 г. «О защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных», директива № 97/66/ЕС Европейского парламента и Совета Европейского союза от 15 декабря 1997 г., касающаяся использования персональных данных и защиты неприкосновенности частной жизни в сфере телекоммуникаций, и другие документы.

Межпарламентской ассамблеей государств – участников СНГ 16 октября 1999 г. принят Модельный закон «О персональных данных».

По закону «персональные данные» – это информация (зафиксированная на материальном носителе) о конкретном человеке, которая отождествлена или может быть отождествлена с ним. К персональным данным относятся биографические и опознавательные данные, личные характеристики, сведения о семейном, социальном положении, образовании, профессии, служебном и финансовом положении, состоянии здоровья и прочие. В законе также перечислены принципы правового регулирования персональных данных, формы государственного регулирования операций с персональными данными, права и обязанности субъектов и держателей персональных данных.

Третий способ закрепления норм о защите персональных данных – закрепление их правовой охраны в международных договорах.

Статьи об обмене информацией включаются в международные договоры о правовой помощи, об избежании двойного налогообложения, о сотрудничестве в определенной общественной, культурной сфере.

По ст. 25 Договора между Российской Федерацией и США об избежании двойного налогообложения и предотвращении уклонения от налогообложения в отношении налогов на доходы и капитал, государства обязаны предоставлять информацию, составляющую профессиональную тайну. Договор между Российской Федерацией и Республикой Индией о взаимной правовой помощи по уголовным делам содержит ст. 15 «Конфиденциальность»: запрашиваемая сторона может потребовать сохранения конфиденциальности переданной информации. Практика заключения международных договоров показывает стремление договаривающихся государств соблюдать международные стандарты защиты персональных данных [12].

1.3. Характеристика основной нормативно-правовой базы Российской Федерации при работе с конфиденциальной информацией

В соответствии с Законом об информации в широком понимании она подразделяется на общедоступную информацию и информацию ограниченного доступа. В зависимости от порядка ее предоставления или распространения она подразделяется на:

- информацию, свободно распространяемую;
- информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;

- информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;
- информацию, распространение которой в Российской Федерации ограничивается или запрещается.

Говоря о нормативном регулировании работы с информацией ограниченного доступа, **важно помнить**, что ограничения на доступ к такой информации устанавливаются только федеральными законами (ст. 5, п. 2 Закона об информации). Законодательно установлено, что информация ограниченного доступа может составлять государственную тайну или относиться к конфиденциальной информации [16].

Законодательством введены два ограничения на отнесение информации к конфиденциальной: к ней не может быть отнесена информация, во-первых, составляющая государственную тайну, и, во-вторых, информация, которая должна быть общедоступной в целях предупреждения сокрытия правонарушений и предотвращения нанесения ущерба законным интересам государства, физических и юридических лиц. Более подробно перечень информации, которую нельзя относить к информации ограниченного доступа, приведен в приложении 1 учебника Н.Н. Куняева [15, с. 21].

Отношения, возникающие при создании, накоплении, обработке, хранении и использовании документов, содержащих конфиденциальную информацию, регулируются соответствующими законодательными и подзаконными актами.

К числу базовых относится в первую очередь Конституция РФ от 12 декабря 1993 г. В ст. 23 установлено право неприкосновенности личной жизни, личной и семейной тайны, тайны телефонных переговоров, почтовых и иных сообщений. При этом ограничение этого права допускается только на основании судебного решения. Конституцией РФ (ст. 24) не допускается сбор, хранение, использование и распространение информации о частной жизни лица без его согласия.

Государственная тайна

Отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации, регулируются законом Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне».

К **государственной тайне** относятся защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации [16].

Техническая защита конфиденциальной информации

Порядок лицензирования деятельности по технической защите конфиденциальной информации (не содержащей сведения, составляющие государственную тайну, но защищаемой в соответствии с законодательством Российской Федерации), осуществляемой юридическими лицами и индивидуальными предпринимателями, определяет «Положение о лицензировании деятельности по технической защите конфиденциальной информации», утвержденное постановлением Правительства РФ от 3 февраля 2012 г. № 79.

Под **технической защитой конфиденциальной информации** понимается выполнение работ и (или) оказание услуг по ее защите от несанкционированного доступа, от утечки по техническим каналам, а также от специальных воздействий на такую информацию в целях ее уничтожения, искажения или блокирования доступа к ней.

Лицензирование деятельности по технической защите конфиденциальной информации осуществляет Федеральная служба по техническому и экспортному контролю [7].

Виды конфиденциальной информации

Виды конфиденциальной информации установлены Указом Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера». К ней относятся:

1. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.
2. Сведения, составляющие тайну следствия и судопроизводства, а также сведения о защищаемых лицах и мерах государственной защиты, осуществляемой в соответствии с Федеральным законом от 20 августа 2004 г. № 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства» и другими нормативными правовыми актами Российской Федерации.
3. Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна).
4. Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и т. д.).
5. Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна).
6. Секрет производства (ноу-хау), т. е. сведения любого характера (производственные, технические, экономические, организационные и др.), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности.

Персональные данные

Нормативно-правовые акты:

- *Трудовой кодекс Российской Федерации от 30 декабря 2001 г. № 197-ФЗ;*
- *Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ;*
- *Кодекс Российской Федерации об административных нарушениях от 30 декабря 2001 г. № 195-ФЗ;*
- *Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;*
- *Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;*
- *Федеральный закон Российской Федерации от 15 ноября 1997 г. № 143-ФЗ «Об актах гражданского состояния»;*
- *Федеральный закон Российской Федерации от 27 июля 2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации»*;
- *Указ Президента Российской Федерации от 30 мая 2005 г. № 609 «Об утверждении Положения о персональных данных государственного гражданского служащего и ведении его личного дела»;*
- *Постановление Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».*

В соответствии с Федеральным законом Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»

> **персональными данными** признается любая информация, относящаяся к прямо или косвенно определенному или определяемому 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 [16].

Персональные данные физического лица (гражданина) или личная тайна (тайна частной жизни) – это конфиденциальная документированная информация, незаконное собирание или распространение которой причиняет вред правам и законным интересам этого лица и предоставляет ему право на защиту в соответствии с законодательством Российской Федерации [15, с. 38].

Законом об информации (ст. 11) установлено, что **не допускаются** сбор, хранение, использование и распространение информации о частной жизни, а равно информации, нарушающей личную тайну, семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений физического лица без его согласия, кроме как на основании судебного решения.

Порядок обработки персональных данных в рамках трудовых отношений установлен Трудовым кодексом Российской Федерации (глава 14), где, в частности, говорится, что работники и их представители должны быть ознакомлены под расписку с документами работодателя, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

Положение о неразглашении персональных данных содержится и в Федеральном законе Российской Федерации от 15 ноября 1997 г. № 143-ФЗ «Об актах гражданского состояния», где говорится о том, что сведения, ставшие известными работнику органа записи актов гражданского состояния в связи с государственной регистрацией акта гражданского состояния, в том числе персональные данные, являются информацией, доступ к которой ограничен в соответствии с федеральными законами, и разглашению не подлежат (ст. 12) [16].

Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Правила обработки персональных данных, осуществляемой без использования средств автоматизации, установленные нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами организации, должны применяться с учетом требований постановления Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» [8].

Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ст. 137) предусматривает **уголовную ответственность** за незаконное собирание и распространение сведений о частной жизни лица, составляющих его личную и семейную тайну (ст. 137), тайну переписки, телефонных переговоров и иных сообщений (ст. 138), тайну голосования (ст. 142), тайну усыновления (ст. 155). Примерный перечень преступлений и администра-

тивных правонарушений в информационной сфере изложен в приложении 6 к учебнику Н.Н. Куняева [15, с. 33].

В ряде случаев персональные данные (личная тайна) составляют врачебную, адвокатскую, нотариальную, налоговую тайны, тайну почтово-телеграфных отправлений и др., которые одновременно считаются служебной и профессиональной тайнами. Нарушение установленного Федеральным законом Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) влечет за собой административную ответственность в соответствии со ст. 13.1 Кодекса Российской Федерации об административных нарушениях [15, с. 37].

Сведения, составляющие тайну следствия и судопроизводства

Нормативно-правовые акты:

- *Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ*;
- *Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ;*
- *Гражданско-процессуальной кодекс Российской Федерации от 14 ноября 2002 г. № 138-ФЗ;*
- *Федеральный закон Российской Федерации от 20 августа 2004 г. № 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства».*

Согласно ст. 310 Уголовного кодекса Российской Федерации, разглашение данных предварительного расследования лицом, предупрежденным в установленном законом порядке о недопустимости их разглашения, если оно совершено без согласия следователя или лица, производящего дознание (в ред. Федерального закона Российской Федерации от 24 июля 2007 г. № 214-ФЗ), наказывается штрафом в размере до восьмидесяти тысяч рублей либо в размере заработной платы или иного дохода осужденного за период до шести месяцев, либо обязательными работами на срок до четырехсот восьмидесяти часов, либо исправительными работами на срок до двух лет, либо арестом на срок до трех месяцев [2].

Положения о недопустимости разглашения следственных данных установлены, в частности, Уголовно-процессуальным кодексом Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Так, в ст. 161–162 определено, что данные предварительного расследования не подлежат разглашению. Они могут быть преданы огласке лишь с разрешения прокурора, следователя, дознавателя и только в том объеме, в каком ими будет признано это допустимым, если разглашение не противоречит интересам предварительного расследования и не связано с нарушением прав и законных интересов участников уголовного судопроизводства [16].

Такая информация может касаться как характера производимых следственных действий, так и доказательной базы, перспектив расследования, круга лиц, участвующих в расследовании. Следователь или дознаватель должен предупредить участников уголовного судопроизводства о недопустимости разглашения без соответствующего разрешения ставшей им известной информации предварительного расследования, о чем у них берется подписка с предупреждением об ответственности. Разглашение сведений о частной жизни участников уголовного судопроизводства без их согласия не допускается, ибо они относятся к персональным данным [15, с. 38].

Федеральным законом Российской Федерации от 20 августа 2004 г. № 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства» определена необходимость обеспечения конфиденциальности сведений о защищаемом лице [15, с. 39].

Правовые нормы, регулирующие использование конфиденциальной информации в судебных разбирательствах установлены также Гражданско-процессуальным кодексом РФ от 14 ноября 2002 г. № 138-ФЗ. Статья 10 «Гласность судебного разбирательства» содержит правила защиты информации на закрытых судебных заседаниях [4].

Служебная тайна

Нормативно-правовые акты:

- *Налоговый кодекс Российской Федерации от 31 июля 1998 г. № 146-ФЗ;*
- *Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ;*
- *Основы законодательства Российской Федерации о нотариате от 11 февраля 1993 г. № 4462-1;*
- *Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера»;*
- *Постановление Правительства Российской Федерации от 3 ноября 1994 г. № 1233 «Об утверждении положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».*

Служебная тайна – это охраняемая законом информация ограниченного доступа о деятельности государственных и негосударственных структур, доступ к которой ограничен в силу служебной необходимости, за исключением информации, составляющей государственную тайну, а также информация ограниченного распространения, ставшая известной в государственных и негосударственных структурах на законном основании, для исполнения служебных обязанностей, имеющая действительную или потенциальную ценность в силу неизвестности ее третьим лицам [15, с. 47].

Служебные сведения ограниченного доступа (служебная тайна) составляют один из видов конфиденциальной информации. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 определяет служебную тайну как служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами.

Постановлением Правительства Российской Федерации от 3 ноября 1994 г. № 1233 «Об утверждении положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти» установлен порядок обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти и уполномоченном органе управления использованием атомной энергии, а также на подведомственных им предприятиях, в учреждениях и организациях.

Данное положение относит к **служебной информации ограниченного распространения** несекретную информацию, касающуюся деятельности организаций, ограничения на распространение которой диктуются служебной необходимостью. Положение также устанавливает порядок организации документооборота документов ограниченного распространения [16].

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

банке Российской Федерации (Банке России)», «Об основах муниципальной службы Российской Федерации», «О рынке ценных бумаг» и др. [15, с. 41]

Налоговая тайна. Примером служебной тайны является налоговая. В соответствии с Налоговым кодексом Российской Федерации налоговую тайну составляют любые полученные налоговым органом, а также органами внутренних дел, государственного внебюджетного фонда и таможенным органом сведения о налогоплательщике. Информация о налогоплательщике, если он является физическим лицом, – это одновременно его личная тайна, т. е. относится к персональным данным. Исключение составляет информация, которая не может быть налоговой тайной (см. приложение 1 учебника Н.Н. Куняева). Утрата документов, содержащих налоговую тайну, либо разглашение сведений, составляющих налоговую тайну, влечет ответственность, предусмотренную ст. 183 Уголовного кодекса Российской Федерации [15, с. 43].

Основами законодательства Российской Федерации о нотариате от 11 февраля 1993 г. № 4462-1 (ст. 5) установлено, что при исполнении служебных обязанностей нотариусу, а также лицам, работающим в нотариальной конторе, запрещается разглашать сведения, оглашать документы, которые стали им известны в связи с совершением нотариальных действий, в том числе и после сложения полномочий, или увольнения, за исключением случаев, предусмотренных в документе. Сведения (документы) о совершенных нотариальных действиях могут выдаваться только лицам, от имени или по поручению которых совершены эти действия [16].

Сведения, связанные с профессиональной деятельностью (профессиональная тайна)

Нормативно-правовые акты:

- *Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ;*
- *Федеральный закон Российской Федерации от 31 мая 2002 г. № 63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации»;*
- *Федеральный закон Российской Федерации от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;*
- *Федеральный закон Российской Федерации от 17 июля 1999 г. № 176-ФЗ «О почтовой связи»;*
- *Федеральный закон Российской Федерации от 07 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»;*
- *Федеральный закон Российской Федерации от 30 декабря 2008 г. № 307-ФЗ «Об аудиторской деятельности»;*
- *Закон Российской Федерации от 27 декабря 1991 г. № 2124-I «О средствах массовой информации».*

Профессиональная тайна – это охраняемая законом информация ограниченного доступа, за исключением информации, составляющей государственную тайну, доверенная или ставшая известной лицу исключительно в силу исполнения им своих профессиональных обязанностей, не связанных с государственной или муниципальной службой, незаконное получение или распространение которой может повлечь за собой вред правам и законным интересам другого лица, доверившего эту информацию [11, с. 52].

К конфиденциальной информации относятся сведения, связанные с профессиональной деятельностью: врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и др. [16]

Фактически получается, что профессиональная тайна – это персональные данные клиентов, пациентов и т. д., а также служебная и коммерческая тайны других организаций [11, с. 69].

Порядок обращения и порядок доступа к информации, составляющей различные виды профессиональной тайны, регламентируется рядом законодательных актов Российской Федерации. Как правило, это законодательные акты, регулирующие отношения в определенных сферах деятельности.

Адвокатская тайна. Например, Федеральный закон от 31 мая 2002 г. № 63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации» содержит ст. 8 «Адвокатская тайна», в которой установлено, что адвокатской тайной являются любые сведения, связанные с оказанием адвокатом юридической помощи своему доверителю. В связи с этим адвокат не может быть вызван и допрошен в качестве свидетеля об обстоятельствах, ставших ему известными в связи с обращением к нему за юридической помощью или в связи с ее оказанием [16].

Согласно ст. 7.1 «Права и обязанности иных лиц» Федерального закона от 07 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»

«Адвокат и адвокатская палата, нотариус и нотариальная палата, лица, осуществляющие предпринимательскую деятельность в сфере оказания юридических или бухгалтерских услуг, а также аудиторская организация, индивидуальный аудитор при оказании аудиторских услуг не вправе разглашать факт передачи в уполномоченный орган следующей информации:

1. При наличии у адвоката, нотариуса, лица, осуществляющего предпринимательскую деятельность в сфере оказания юридических или бухгалтерских услуг, любых оснований полагать, что сделки или финансовые операции, указанные в пункте 1 настоящей статьи, осуществляются или могут быть осуществлены в целях легализации (отмывания) доходов, полученных преступным путем, или финансирования терроризма, они обязаны уведомить об этом уполномоченный орган.

Адвокат и нотариус вправе передать такую информацию как самостоятельно, так и через соответственно адвокатскую и нотариальную палаты при наличии у этих палат соглашения о взаимодействии с уполномоченным органом.

2. Аудиторские организации, индивидуальные аудиторы при оказании аудиторских услуг при наличии любых оснований полагать, что сделки или финансовые операции аудируемого лица могли или могут быть осуществлены в целях легализации (отмывания) доходов, полученных преступным путем, или финансирования терроризма, обязаны уведомить об этом уполномоченный орган» [3].

Врачебная тайна. В ст. 13 «Соблюдение врачебной тайны» Федерального закона от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» установлено, что информация о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иные сведения, полученные при его медицинском обследовании и лечении, составляют врачебную тайну. Не допускается разглашение сведений, составляющих врачебную тайну, лицами, которым они стали известны при обучении, исполнении профессиональных, служебных и иных обязанностей, кроме случаев, установленных законом.

Тайна связи. Федеральный закон от 17 июля 1999 г. № 176-ФЗ «О почтовой связи» (ст. 15) содержит положения, направленные на защиту тайны связи: тайны переписки, почтовых, телеграфных и иных сообщений, входящих в сферу деятельности операторов поч-

товой связи. Тайна связи не подлежит разглашению без согласия пользователя услуг почтовой связи. Все операторы почтовой связи обязаны обеспечивать соблюдение тайны связи. Информация об адресных данных пользователей услуг почтовой связи, о почтовых отправлениях, почтовых переводах денежных средств, телеграфных и иных сообщениях, входящих в сферу деятельности операторов почтовой связи, а также сами эти почтовые отправления, переводимые денежные средства, телеграфные и иные сообщения являются тайной связи и могут выдаваться только отправителям (адресатам) или их представителям. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений в соответствии с Уголовным кодексом Российской Федерации (ст. 138) влечет уголовную ответственность [16].

В соответствии с Федеральным законом «Об оперативно-розыскной деятельности», проведение оперативно-розыскных мероприятий, которые ограничивают конституционные права человека и гражданина на тайну переписки и т. д., допускается на основании судебного решения [11, с. 50].

Аудиторская тайна. В соответствии с Федеральным законом «Об аудиторской деятельности» аудиторские организации и индивидуальные аудиторы обязаны хранить тайну об операциях аудируемых лиц и лиц, которым оказывались сопутствующие аудиту услуги.

Журналистская тайна (редакционная тайна). Не допускается использование средств массовой информации в целях совершения уголовно наказуемых деяний, для разглашения сведений, составляющих государственную или иную специально охраняемую законом тайну, для распространения материалов, содержащих публичные призывы к осуществлению террористической деятельности или публично оправдывающих терроризм, других экстремистских материалов, а также материалов, пропагандирующих порнографию, культ насилия и жестокости. Редакция не вправе разглашать в распространяемых сообщениях и материалах сведения, предоставленные гражданином, субъектом персональных сведений с условием сохранения их в тайне. Редакция также обязана сохранять в тайне источник информации и не вправе называть лицо, предоставившее сведения с условием неразглашения его имени, за исключением случая, когда соответствующее требование поступило от суда в связи с находящимся в его производстве делом [11, с. 51–52].

Предоставление информации организаторами торговли[1], клиринговыми организациями[2] и центральными контрагентами[3]. Согласно ст. 7.1.-1 Федерального закона от 07 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»:

«3. При наличии у организатора торговли, клиринговой организации или центрального контрагента достаточных оснований полагать, что соответствующие договоры (услуги) заключены (оказываются) или могут заключаться (оказываться) в целях легализации (отмывания) доходов, полученных преступным путем, или финансирования терроризма, они обязаны уведомить об этом уполномоченный орган в порядке, установленном Банком России по согласованию с уполномоченным органом.

4. Организатор торговли, клиринговая организация и центральный контрагент не вправе разглашать факт передачи в уполномоченный орган информации».

При этом ст. 10 гласит: «Органы государственной власти Российской Федерации, осуществляющие деятельность, связанную с противодействием легализации (отмыванию)

---

[1] *Организатор торговли ценными бумагами* – это профессиональный участник рынка, юридическое лицо, осуществляющее деятельность по организации торговли ценными бумагами.

[2] *Клиринговая организация* – это организация-посредник между покупателем и продавцом ценных бумаг, которая берет на себя функции по покупке бумаг, представляя интересы фирмы-заказчика или, наоборот, фирмы-продавца.

[3] *Центральный контрагент* – это организация, являющаяся посредником между сторонами сделки, т. е. продавцом для первоначального покупателя и покупателем для первоначального продавца, что гарантирует исполнение обязательств в рамках сделки.

доходов, полученных преступным путем, и финансированию терроризма, направившие запрос, обеспечивают конфиденциальность предоставленной информации и используют ее только в целях, указанных в запросе», ст. 8: «Работники уполномоченного органа при исполнении настоящего Федерального закона обеспечивают сохранность ставших им известными сведений, связанных с деятельностью уполномоченного органа, составляющих служебную, банковскую, налоговую, коммерческую тайну или тайну связи, и несут установленную законодательством Российской Федерации ответственность за разглашение этих сведений» [3].

Сведения, связанные с коммерческой деятельностью

Нормативно-правовые акты:

- *Гражданский кодекс Российской Федерации от 26 января 1996 г. № 51-ФЗ;*
- *Федеральный закон Российской Федерации от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне».*

Согласно Федеральному закону от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»

> **коммерческая тайна** – режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Указанным законом определены виды информации, которая не может составлять коммерческую тайну, данный список приведен в приложении (см. *Приложение 1*) [5].

Закон устанавливает меры организационного характера, обеспечивающие защиту документов, содержащих коммерческую тайну, от несанкционированного доступа. В том числе законом установлен гриф ограничения доступа к документам, содержащим коммерческую тайну: «Коммерческая тайна» [16].

Законодательством Российской Федерации предусмотрена возможность разглашения коммерческой тайны при найме подряда. В ст. 727 § 1 «Общие положения о подряде» главы 37 «Подряд» части 2 Гражданского кодекса Российской Федерации установлено, что если сторона благодаря исполнению своего обязательства по договору подряда получила от другой стороны информацию о новых решениях и технических знаниях, в том числе не защищаемых законом, а также сведения, в отношении которых их обладателем установлен режим коммерческой тайны, сторона, получившая такую информацию, не вправе сообщать ее третьим лицам без согласия другой стороны. Порядок и условия пользования такой информацией определяются соглашением сторон [1].

Банковская тайна. Возможны различные модификации конфиденциальной информации, составляющей коммерческую тайну. Одним из видов последней является банковская тайна, которая относится, как правило, к финансово-кредитной деятельности и едина для всех кредитных организаций (коммерческих банков).

Все служащие кредитной организации обязаны хранить тайну операций, счетов и вкладов ее клиентов и корреспондентов, а также иных сведений, устанавливаемых кредитной организацией, если это не противоречит федеральному закону.

Организация, осуществляющая функции по обязательному страхованию вкладов, не вправе раскрывать третьим лицам информацию, полученную в соответствии с Федеральным законом «О страховании вкладов физических лиц в банках Российской Федерации» [11, с. 55–56].

Секрет производства (ноу-хау)

Нормативно-правовые акты:

- *Гражданский кодекс Российской Федерации от 26 января 1996 г. № 51-ФЗ;*
- *Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне».*

Ст. 1465 Гражданского кодекса Российской Федерации определяет

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

Исключительное право на секрет производства, созданный работником в связи с выполнением своих трудовых обязанностей или конкретного задания работодателя (служебный секрет производства), принадлежит работодателю (ст. 1470) [1].

Существует **три вида договоров**, регулирующих конфиденциальность секрета производства:

1) договор об отчуждении исключительного права на секрет производства;

2) лицензионный договор о предоставлении права использования секрета производства;

3) секрет производства, полученный при выполнении работ по договору подряда [10, с. 59].

Вывод. Таким образом, в приведенных выше нормативных правовых актах содержатся отдельные положения, определяющие общие принципы учета, хранения и использования документов, содержащих конфиденциальные сведения. Однако законодательные акты РФ не регламентируют в полной мере порядок работы с документами, содержащими конфиденциальную информацию. Поэтому так важно создание на предприятии, работающем с конфиденциальной информацией, локальных нормативных документов по защите конфиденциальных сведений, а также правилам работы и хранения конфиденциальных документов.

Вопросы для самоконтроля

1. Что понимается под конфиденциальностью информации?
2. Кем является обладатель информации согласно Закону об информации?
3. В каком нормативном акте представлены определения понятий «документированная информация» и «документ»? Дайте определения этим понятиям.
4. Что такое конфиденциальная документированная информация? Назовите ее особенности. Чем она отличается от обычного документа?
5. С какого времени владелец объекта интеллектуальной собственности приобретает законодательную защиту от неправомерных действий третьих лиц и может требовать устранения нарушений своих интересов, взыскать компенсацию убытков?
6. Поможет ли защитить свою интеллектуальную собственность наличие национального патента при осуществлении деятельности на территории другого государства? Обоснуйте свой ответ.

7. Перечислите наиболее важные международные акты, которые направлены на охрану интеллектуальной собственности, и годы их учреждения.

8. Выделите общие принципы охраны интеллектуальных прав на международном уровне.

9. Назовите основные международные организации по охране интеллектуальной собственности.

10. Расшифруйте аббревиатуры ВОИС, ВТО и ЕС.

11. Как подразделяется информация в зависимости от порядка ее предоставления или распространения согласно Закону об информации?

12. Назовите виды конфиденциальной информации, установленные Указом Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

13. Что такое персональные данные?

14. Что понимается под секретом производства (ноу-хау)?

15. Чем отличается служебная тайна от профессиональной тайны?

Список использованных источников и литературы

Источники

1. Гражданский кодекс Российской Федерации от 26 января 1996 г. № 51-ФЗ. URL: http://www.consultant.ru/document/cons_doc_LAW_5142/ (дата обращения: 15.07.2019).

2. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ. URL: http://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 15.07.2019).

3. Федеральный конституционный закон от 25 декабря 2000 г. № 2-ФКЗ «О Государственном гербе Российской Федерации». URL: http://www.consultant.ru/document/cons_doc_LAW_29674/ (дата обращения: 16.12. 2019).

4. Федеральный закон Российской Федерации от 07 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма». URL: http://www.consultant.ru/document/cons_doc_LAW_32834/ (дата обращения: 15.07.2019).

5. Гражданско-процессуальный кодекс Российской Федерации от 14 ноября 2002 г. № 138-ФЗ. URL: http://www.consultant.ru/document/cons_doc_LAW_39570/ (дата обращения: 15.07.2019).

6. Федеральный закон Российской Федерации от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне». URL: http://www.consultant.ru/document/cons_doc_LAW_48699/ (дата обращения: 15.07.2019).

7. Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 15.07.2019).

8. Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации». URL: https://base.garant.ru/193875/ (дата обращения: 15.07.2019).

9. Постановление Правительства Российской Федерации от 03 февраля 2012 г. № 79 (ред. от 15 июня 2016 г.) «О лицензировании деятельности по технической защите конфиденциальной информации» (вместе с «Положением о лицензировании деятельности по технической защите конфиденциальной информации»). URL: http://www.consultant.ru/ document/cons_doc_LAW_125798/ (дата обращения: 15.07.2019).

10. ГОСТ Р 7.0.8-2013. Национальный стандарт Российской Федерации. «Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и ар-

хивное дело. Термины и определения» (утв. Приказом Росстандарта от 17 октября 2013 г. № 1185-ст). URL: http://www.consultant.ru/document/cons_doc_LAW_163800/ (дата обращения: 15.07.2019).

11. ГОСТ Р 7.0.97-2016. Национальный стандарт Российской Федерации. «Система стандартов по информации, библиотечному и издательскому делу. Организационно-распорядительная документация. Требования к оформлению документов» (утв. Приказом Росстандарта от 08 декабря 2016 г. № 2004-ст). URL: http://www.consultant.ru/ document/cons_doc_LAW_216461/ (дата обращения: 16.12. 2019).

Литература

12. Алексенцев А.И. Конфиденциальное делопроизводство [Электрон. ресурс] // Управление персоналом. М., 2003. 200 с. (pdf).

13. Егоров В.П. Конфиденциальное делопроизводство [Электрон. ресурс]: учеб. пособие. М.: Юридический институт МИИТа, 2015. 178 с. (pdf).

14. Законодательство и другие нормативные материалы по принятию конфиденциального режима [Электрон. ресурс] // Студенческая библиотека онлайн: [сайт]. URL: https://studbooks.net/859948/buhgalterskiy_uchet_i_audit/zakonodatelstva_podzakonnye_akty_reguliruyuschie_konfidentsialnoe_deloproizvodstvo (дата обращения: 15.07.2019).

15. Куняев Н.Н. Конфиденциальное делопроизводство и защищенный электронный документооборот [Электрон. ресурс]: учебник / Н.Н. Куняев, А.С. Демушкин, А.Г. Фабричнов; под общ. ред. Н.Н. Куняева. М.: Логос, 2011. 452 с. (Новая университетская библиотека). (pdf).

16. Маланыч И.Н. Международные правовые нормы в сфере защиты персональных данных [Электрон. ресурс] // ISO27000.ru. Искусство управления информационной безопасностью [сайт]. URL: http://www.iso27000.ru/chitalnyi-zai/zaschita-personalnyh-dannyh/mezhdunarodnye-pravovye-normy-v-sfere-zaschity-personalnyh-dannyh (дата обращения: 16.08.2019).

17. Международная охрана интеллектуальной собственности [Электрон. ресурс] // «Гардиум» – аккредитованный партнер Российского экспортного центра: [сайт]. URL: https://legal-support.ru/information/blog/zashita-prav/mezhdunarodnaya-ohrana-intellektualnoi-sobstvennosti/ (дата обращения: 15.08.2019).

18. Мэггс П.Б., Сергеев А.П. Интеллектуальная собственность [Электрон. ресурс]. М.: Юристъ, 2000. 400 с. URL: https://studfiles.net/preview/5251206/page:3/ (дата обращения: 15.08.2019).

19. Сотрудничество со Всемирной организацией интеллектуальной собственности (ВОИС) [Электрон. ресурс] // Роспатент. Федеральная служба по интеллектуальной собственности [официальный сайт]. URL: https://rupto.ru/ru/activities/inter/coop/wipo (дата обращения: 15.08.2019).

20. Фирсова А.Ю. Модуль 8. Работа с конфиденциальными документами. Курс повышения квалификации / профессиональной переподготовки «Основы делопроизводства и секретарское дело» [Электрон. ресурс] // Академия подготовки главных специалистов [сайт]. [2019]. URL: https://specialitet.ru (дата обращения: 03.11.2019).

21. Янковая В.Ф. Нормативная база для работы с конфиденциальными документами [Электрон. ресурс] // Журнал об электронном контенте, документах и бизнес-процессах «ECM-Journal»: [сайт]. 12 августа 2013 г. URL: https://ecm-journal.ru/card.aspx?ContentID=4694943 (дата обращения: 15.07.2019).

Глава 2
ДОКУМЕНТИРОВАНИЕ И УЧЕТ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

2.1. Разработка перечня конфиденциальной документированной информации

Конфиденциальная документированная информация должна создаваться только при действительной необходимости в письменном удостоверении наличия и содержания управленческих, коммерческих, производственных и иных действий, передаче информации, хранении и использовании ее в течение конкретного времени и в определенном количестве экземпляров.

При этом решение задач конфиденциальной деятельности должно обеспечиваться минимальным количеством конфиденциальных документов при сохранении полноты требуемой информации.

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

Целями разработки перечня конфиденциальной документированной информации должны являться не только определение состава конфиденциальной документированной информации, необходимой и достаточной для деятельности организации, но и установление конкретных лиц, имеющих право создавать, составлять, визировать и подписывать (утверждать) документы, а также предотвращение необоснованной рассылки этих документов [6, с. 70].

Примерный перечень информации, составляющей коммерческую, служебную тайны, секрет производства (ноу-хау) организации, приведен в приложении 2 к учебнику Н.Н. Куняева [6, с. 71].

Основные этапы разработки перечня конфиденциальной документированной информации

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

Второй этап. Определяется, **какая из установленной информации должна быть ограниченного доступа** и относиться к какому-либо виду тайн, за исключением государственной. Базовым критерием при этом является возможность получения преимуществ от использования информации за счет неизвестности ее третьим лицам [6, с. 73] .

Третий этап. После установления состава информации **определяется степень ее конфиденциальности**. Степень конфиденциальности – это показатель уровня закрытости информации. Уровень закрытости зависит от величины ущерба, который может наступить при утечке информации. Чем больше этот ущерб, тем выше должна быть и степень конфиденциальности информации.

Четвертый этап. Это этап **определения конкретных сроков конфиденциальности информации** либо обстоятельств и событий, при наступлении которых она снимается (табл. 1).

Специально созданная руководством организации постоянно действующая экспертная комиссия по защите конфиденциальной информации разрабатывает, согласовывает перечень конфиденциальной документированной информации, после чего он утверждается и вводится в действие приказом руководителя организации.

В приказе должны быть определены мероприятия по обеспечению функционирования перечня и контролю за его выполнением. С приказом и перечнем необходимо ознакомить под расписку всех сотрудников организации, работающих с информацией ограниченного доступа, за исключением той, которая представляет государственную тайну [6, с. 74].

Таблица 1

Форма перечня конфиденциальной документированной информации

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

Важно! В формах учета носителей не должны производиться подчистки и исправления с применением корректирующей жидкости. Ошибочная запись зачеркивается одной чертой.

Вносимые исправления заверяются подписью сотрудника подразделения конфиденциального делопроизводства с проставлением даты. Листы журналов учета носителей должны быть перед заведением пронумерованы, прошиты и опечатаны печатью подразделения конфиденциального делопроизводства. На обратной стороне последнего листа журнала проставляется заверительная надпись с указанием количества листов, подписываемая сотрудником, ответственным за ведение журнала. Заверительная надпись на картотеку учета носителей с указанием количества карточек в картотеке составляется по окончании года на отдельной карточке и помещается в конце картотеки. Если содержащиеся в учетных формах сведения по совокупности являются конфиденциальными, журналам и картотекам должен присваиваться гриф конфиденциальности.

На карточках учета гриф конфиденциальности не проставляется [5, с. 71].

Вопросы для самоконтроля

1. Назовите цели разработки перечня конфиденциальной документированной информации.
2. Перечислите основные этапы разработки перечня конфиденциальной документированной информации.
3. Назовите базовый критерий при определении, какая из установленной информации должна быть ограниченного доступа.

4. Можно ли в формах учета производить подчистки и исправления с применением корректирующей жидкости учета носителей?

5. Кто и как заверяет исправления в учетных формах?

2.2. Разработка и ведение перечня создаваемых конфиденциальных документов

Сразу же после заполнения перечня конфиденциальной документированной информации разрабатывается перечень создаваемых конфиденциальных документов (табл. 2) [6, с. 76].

Таблица 2

Форма перечня создаваемых конфиденциальных документов

Учетный номер и отметка конфиденциальности	Дата регистрации	Наименование документа	Срок конфиденциальности	Ф.И.О. лиц, имеющих право создавать документ	Ф.И.О. лиц, имеющих право подписывать документ	Количество составляемых экземпляров документа	Куда направляется	Примечание
1	2	3	4	5	6	7	8	9

Если документ подлежит утверждению, то в графе 6 сначала проставляются Ф.И.О. лица (лиц), подписывающего документ, затем, после слова «утв.» – Ф.И.О. лица, утверждающего документ. При значительном количестве утверждаемых документов графа 6 может быть разделена на две графы: «Ф.И.О. лиц, имеющих право подписывать документы» и «Ф.И.О. лиц, имеющих право утверждать документы» [6, с. 75].

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

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

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

При изменении перечня конфиденциальной документированной информации соответствующие изменения вносятся и в перечень создаваемой конфиденциальной документированной информации. О снятии грифа конфиденциальности информации с отправленных документов должны быть письменно оповещены организации и предприятия – адресаты [6, с. 77].

Вопросы для самоконтроля

1. Кто разрабатывает, подписывает и утверждает перечень конфиденциальной документированной информации?

2. Какие сведения должен содержать приказ, утверждающий перечень конфиденциальной документированной информации?

3. Каким образом извещаются организации и предприятия – адресаты о снятии грифа конфиденциальности информации с отправленных документов?

2.3. Документирование конфиденциальной информации

Согласно ГОСТ Р 7.0.8-2013 **документирование –** это запись информации на носителе по установленным правилам [2].

Документирование информации ограниченного доступа является важнейшей составной частью конфиденциального делопроизводства, поскольку от количества, состава и правильности оформления конфиденциальных документов зависят качество и эффективность управленческой и производственной деятельности, достоверность и юридическая сила документов, трудоемкость их обработки и качество организации делопроизводства и документооборота, включая защищенный электронный документооборот, обмен электронными сообщениями [6, с. 62].

Работа с созданными/изданными конфиденциальными документами включает четыре процедуры (схема 1):

1. процедура приема черновика документа от исполнителя;
2. процедура традиционной или автоматизированной регистрации черновика;
3. процедура подготовки и выдачи проекта документа исполнителю;
4. процедура снятия копий с документа, производства выписки и изготовления дополнительных экземпляров документа.

Схема 1. Последовательность и характеристика процедур изготовления конфиденциальных документов

1. Процедура приема черновика документа от исполнителя

получение делопроизводителем документов от исполнителя бумажного черновика или учтенного диска (с бумажным экземпляром учетной карточки — описи документов, записанных на носителе) с черновиком подготовленного документа или получение оформленного черновика по защищенной линии связи от компьютера исполнителя

проверка наличия на черновике письменного разрешения на изготовление проекта документа, подписанного полномочным руководителем

проверка реального наличия на магнитном носителе (диске) черновика одного документа и соответствия его данным, указанным в бумажном экземпляре учетной карточки носителя, заверение соответствия росписями исполнителя и сотрудника участка

проверка наличия всех реквизитов и частей документа, обозначения

подсчет количества листов черновика

внесение отметки о получении носителя (рабочей тетради, флэш-памяти и т. п.) во внутреннюю опись документов, находящихся у исполнителя

2. Процедура традиционной или автоматизированной регистрации черновика

внесение исходных сведений о черновике в журнал учета черновиков и проектов документов

резервирование машинописного номера (регистрационного номера этапа изготовления) проекта документа в контрольном журнале учета карточек подготовленных документов или определение этого номера по валовой картотеке учетных карточек (если на документ заполняется два экземпляра карточки)

при использовании единой нумерации документов на участке изготовления и участке учета подготовленных документов — одновременное резервирование аналогичного номера в контрольном журнале участка учета подготовленных (изданных) документов

проставление машинописного номера на титульном листе и (или) листах черновика (в электронный черновик документа учетный номер вносится с клавиатуры ПК или автоматически), на чистом бланке учетной карточки подготовленного документа и в журнале учета черновиков и проектов документов

изъятие листов черновика из спецблокнота и фиксирование изъятия каждого листа на корешке или в контрольном листе спецблокнота

возврат спецблокнота исполнителю

вкладывание в черновик или подкалывание к листам черновика пронумерованной учетной карточки подготовленного документа

передача черновика документа для печати машинистке (оператору ПК) под роспись в журнале учета черновиков и проектов документов

3. Процедура подготовки и выдачи проекта документа исполнителю

- заполнение необходимых граф пронумерованной учетной карточки подготовленного документа
- подготовка с помощью компьютера текста и реквизитов документа с учетом требований государственного стандарта
- обозначение на нижнем поле напечатанного комплекта экземпляров каждого листа документа учетного (машинописного) номера
- обозначение на оборотной стороне последнего листа всех экземпляров документа учетного (машинописного) номера, грифа конфиденциальности, количества отпечатанных (изготовленных) экземпляров, при необходимости их целевого назначения, фамилии исполнителя, индекса машинистки (оператора) и даты печатания (изготовления) документа
- передача отпечатанного проекта документа, черновика и учетной карточки руководителю участка изготовления документов
- проверка правильности и комплектности отпечатанного проекта документа, его соответствия черновику
- проверка исполнителем комплектности и правильности изготовления проекта документа, просмотр дискеты, если документ был изготовлен на этом носителе
- выдача исполнителю всех экземпляров проекта документа и черновика под роспись в учетной карточке подготовленного документа
- передача отпечатанного проекта документа и черновика для регистрации в «журнале учета проектов документов»
- выдача исполнителю отпечатанного проекта документа и черновика под роспись в журнале
- учет подготовленных документов

4. Процедура снятия копий с документа, производства выписки и изготовления дополнительных экземпляров документа

- получение документа от исполнителя
- проверка наличия на документе разрешения полномочного руководителя на снятие копии или производство выписки, изготовление дополнительных экземпляров документа
- внесение отметки о получении документа во внутреннюю опись документов, находящихся у исполнителя
- внесение отметки о снятии копии или производстве выписки в учетные формы основного документа
- внесение отметки о дополнительно размноженных экземплярах в учетные формы основного документа
- внесение соответствующих отметок в основной документ
- внесение дополнений и изменений в электронную опись документов, выданных конкретным исполнителям, допечатка необходимых сведений во внутреннюю опись документов, находящихся у исполнителя
- выдача копии, выписки или дополнительно размноженных экземпляров исполнителю под роспись в традиционной карточке или бумажном экземпляре электронной учетной карточки выписки, копии или основного документа
- возвращение исполнителю основного документа под роспись в учетной карточке документа или с уничтожением расписки
- возвращение сотруднику учетных форм документов, а также основного документа и его учетной формы, если документ был получен не от исполнителя
- уничтожение в базе данных компьютера всех материалов по изготовлению копий, выписок и дополнительных экземпляров документа, кроме записей в электронных описях

Использование отметки конфиденциальности при оформлении документов

Нанесение на документы, содержащие конфиденциальную информацию, отметки ограничения доступа – грифа ограничения доступа к документу – является одним из обязательных условий получения по отношению к данной информации статуса коммерческой или иной тайны [5, с. 15].

Гриф ограничения доступа к документу – реквизит, свидетельствующий об особом характере информации документа и ограничивающий доступ к нему [2].

Для служебной информации ограниченного распространения, в том числе для информации, составляющей служебную тайну, за исключением информации, относящейся к государственной тайне, установлена одна степень конфиденциальности – «Для служебного пользования». Наименование данной отметки и его сокращенное название определены Положением о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, утвержденным Постановлением Правительства Российской Федерации [6, с. 66].

В зависимости от возможной степени ущерба, наносимого организации в случае разглашения информации, применяются две степени конфиденциальности информации: «Конфиденциально» и «Строго конфиденциально» [6, с. 64].

На практике негосударственные структуры, обладающие информацией, составляющей служебную тайну или секрет производства, применяют наименование отметки конфиденциальности «Для служебного пользования» совместно со степенями конфиденциальности документов «Конфиденциально» и «Строго конфиденциально» [6, с. 66–67].

В Федеральном законе «О коммерческой тайне» установлена одна степень конфиденциальности – «Коммерческая тайна». Указывается обладатель этой информации (для юридических лиц – полное наименование и место нахождения, для индивидуальных предпринимателей – фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства) [6, с. 67–68].

Документированная информация, не подлежащая отправлению в другие организации, может иметь две степени и два наименования конфиденциальности – «Конфиденциально», «Строго конфиденциально», а отправляемая – одну степень и наименование «Коммерческая тайна». Для информации ограниченного доступа, составляющей коммерческую тайну, используется гриф «Коммерческая тайна». Гриф «Коммерческая тайна» можно дополнять соответствующим внутренним грифом степени конфиденциальности: «Конфиденциально» и «Строго конфиденциально» или грифом «Для служебного пользования» [6, с. 68].

Не допускается, в соответствии со ст. 8 закона Российской Федерации «О государственной тайне», использование грифов ограничения доступа, относящихся к государственной тайне: «Особой важности», «Совершенно секретно», «Секретно» [6, с. 64].

На документы, дела, издания, а также другие носители информации наносится отметка конфиденциальности, включающая следующие реквизиты:

- степень конфиденциальности информации со ссылкой на соответствующий пункт действующего в организации перечня конфиденциальной документированной информации;
- название организации, осуществившей ограничение доступа к конфиденциальной документированной информации;
- регистрационный номер;
- дату или условие снятия степени конфиденциальности или ограничение доступа [6, с. 64–65].

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

Строго конфиденциально
Экз. № 1

или

Для служебного пользования
Экз. № 3

Для нанесения регистрационного номера, который должен включать в обязательном порядке данные о конфиденциальности документа, на регистрационно-контрольных карточках, а также в электронных картотеках допускается сокращение написания отметки: «Строго конфиденциально» – СКФД, «Конфиденциально» – КФД, «Для служебного пользования» – ДСП, «Служебная тайна – СТ», «Профессиональная тайна – ПТ», «Персональные данные – ПД», «Коммерческая тайна – КТ» [6, с. 65]. Можно встретить также отметку «Строго конфиденциальная информация» – СКИ [7].

Гриф «Особый контроль» присваиваются документу лично руководителем организации, им изменяется или отменяется. Исполнение, использование и хранение документов с этим грифом также организуется руководителем с возможным привлечением руководителя службы конфиденциальных документов. Исполнителям документы с этим грифом не передаются [7].

Возможно проставление отметки о конфиденциальности в форме штампа и дополнение другими реквизитами, например, адресатом, как в нижеприведенном примере [6, с. 65].

Рис. 1. Примеры оформления штампа «Коммерческая тайна»

Некоторые специалисты не рекомендуют ставить гриф «КТ», объясняя это тем, что грифом обозначается не вид тайны, а характер ограничения доступа к документу [7].

На электронных документах и документах, записанных на любых машинных носителях, гриф обозначается на всех листах. Ниже грифа или ниже адресата могут обозначаться ограничительные пометы типа: «Лично», «Только в руки», «Только адресату», «Лично в руки» и др. При регистрации конфиденциальных документов к его номеру добавляется сокращенное обозначение грифа конфиденциальности, например,

№ 37 К, 89 СК, 97 ДСП.

Документы и информация, конфиденциальные в целом (например, документация службы персонала, службы безопасности, документы, отнесенные к профессиональной

тайне, и т. д.), как правило, не маркируются, потому что в полном объеме обладают строгим ограничением доступа к ним персонала.

На ценных, но не конфиденциальных документах может проставляться отметка, надпись, штамп, привлекающая особое внимание к сохранности таких документов, например:

«Собственная информация фирмы», «Информация особого внимания», «Копии не снимать», «Хранить в сейфе» [7].

Если созданный конфиденциальный документ подлежит отправлению с сопроводительным письмом, то оно регистрируется за самостоятельным номером, на нем проставляется отметка конфиденциальности, соответствующая отметке конфиденциальности приложения, независимо от того, содержит или нет сопроводительное письмо конфиденциальные данные [6, с. 65].

При наличии нескольких приложений с разными степенями конфиденциальности отметка конфиденциальности сопроводительного письма устанавливается по наивысшей степени конфиденциальности приложений. Необходимость проставления на сопроводительном письме отметки конфиденциальности вызвана также тем обстоятельством, что без соблюдения этого требования подавляющее большинство сопроводительных писем будут не конфиденциальными, а открытыми. Однако поскольку документы отправляются за номерами сопроводительных писем, то формально и конфиденциальные приложения окажутся открытыми [6, с. 66].

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

Определение степени ограничения доступа к документам

Степень конфиденциальности может быть **присвоена** документу:

- исполнителем на стадии подготовки документа;
- руководителем структурного подразделения или руководителем организации на стадии согласования или подписания документа;
- адресатом (получателем) документа на стадии его первичной обработки в службе делопроизводства или службе конфиденциального делопроизводства, если в организации существует такая отдельно выделенная служба [6, с. 64].

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

- соответствующая корректировка перечня конфиденциальной документированной информации;
- истечение установленного срока действия конфиденциальности информации в соответствии с перечнем конфиденциальной документированной информации;
- наличие события, при котором отметка конфиденциальности должна быть изменена или снята, например, окончание действия договора между организациями [6, с. 64].

После снятия отметки конфиденциальности документ передается в службу делопроизводства. Об изменении или снятии конфиденциальности на самом документе делается отметка, удостоверяемая визой руководителя, подписавшего этот документ. О внесении в документ такой отметки сообщается заинтересованным лицам, учреждениям, предприятиям и организациям [6, с. 64].

В целях своевременного изменения или снятия отметки конфиденциальности с документов необходимо регулярно просматривать учетные картотеки (перечни, журналы, списки и т. д.), в том числе электронные, и выявлять те документы, которые могут быть удалены из этих картотек [6, с. 65].

Основанием для снятия грифа может быть также изменение объективных обстоятельств, вследствие которых дальнейшая защита определенных конфиденциальных сведений организации является нецелесообразной:

- исключение информации, содержащейся в документе (носителе), из перечня конфиденциальной информации организации;
- истечение установленного срока действия режима ограничения доступа к информации;
- наличие события, при котором дальнейшая защита конфиденциальной информации становится нецелесообразной (например, патентование изобретения, разглашение информации и др.);
- установление факта неправильности присвоения грифа конфиденциальности документу (носителю).

Подготовка предложений о снятии грифа конфиденциальности возлагается, как правило, на экспертную комиссию, создаваемую по решению руководства организации.

Заключение комиссии оформляют актом, утверждаемым руководством организации. На документе (документе выделенного хранения, внешнем электронном носителе) гриф конфиденциальности зачеркивают одной чертой и рядом с ним с помощью специального штампа или от руки делают отметку о снятии грифа:

Гриф снят. Акт №____от____

(указать номер акта и дату его утверждения руководителем)

Гриф заверяется подписью лица, ответственного за ведение конфиденциального делопроизводства, и печатью организации (структурного подразделения). Аналогичные отметки вносятся в описи дел, журналы регистрации конфиденциальных документов (учета документов выделенного хранения, внешних электронных носителей).

О снятии грифа конфиденциальности с документов (документов выделенного хранения, внешних электронных носителей) необходимо письменно проинформировать всех адресатов, которым эти материалы направлялись.

Вопросы для самоконтроля

1. Дайте определения понятиям «документирование», «гриф ограничения доступа к документам».
2. Требуется ли отметка об ограничении доступа на приказе о приеме на работу, содержащем персональные данные?
3. Какие отметки об ограничении доступа будут иметь документы об аудиторской проверке?
4. Какую степень конфиденциальности приобретает сопроводительное письмо к документам с разными степенями конфиденциальности?
5. По какой причине не рекомендуется ставить гриф «Коммерческая тайна» на документах?
6. Что включает в себя работа с созданными/изданными конфиденциальными документами?

2.4. Учет и оформление бумажных и машинных носителей конфиденциальной информации

Учет – это установление наличия, количества путем подсчетов.

Создание конфиденциальных документов должно начинаться с учета, оформления и выдачи исполнителям бумажных носителей информации, на которых будут составляться черновики или проекты конфиденциальных документов. Эти технологии не всегда являются обязательными, поскольку они усложняют процесс документирования конфиденциальной информации и понижают оперативность подготовки документов.

Бумажными носителями могут быть: спецблокноты, отдельные листы бумаги, типовые формы документов, стенографические и рабочие тетради [6, с. 79].

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.

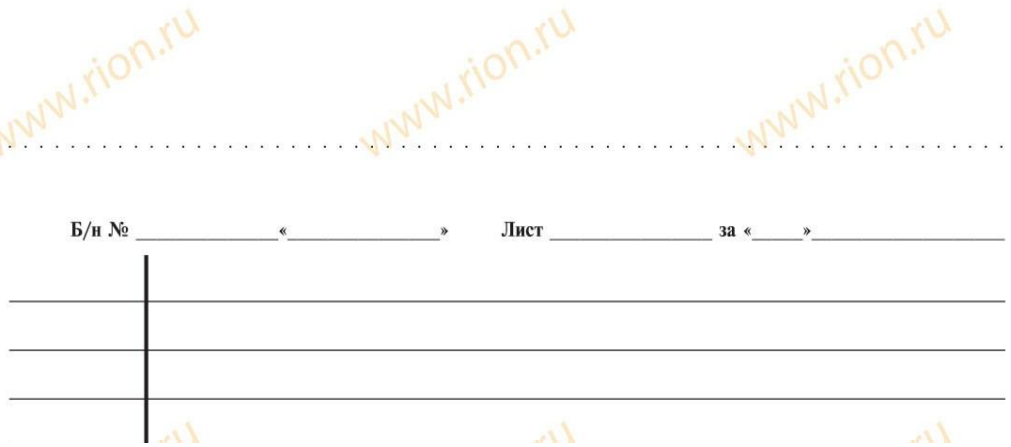


Рис. 2. Пример верхней части макета спецблокнота, отпечатанного в типографии РИОН

Рабочая тетрадь (сброшюрованные листы бумаги без линии отрыва) служит, 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.

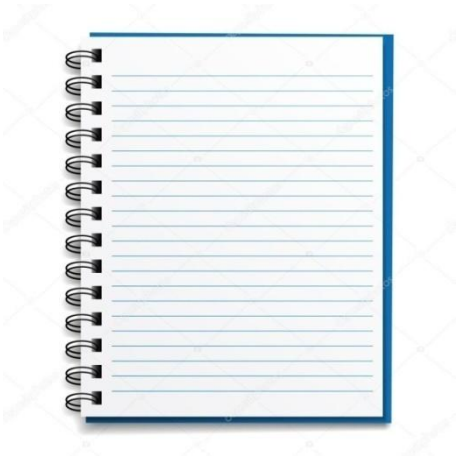


Рис. 3. Пример рабочей тетради

Схема 2. Последовательность и характеристика процедур оформления и учета носителей конфиденциальной информации

Перед взятием на учет носители должны быть соответствующим образом оформлены. На обложках спецблокнотов сотрудник службы делопроизводства пишет или проставляет штампом (если не проставлено типографским способом) слово «Спецблокнот» и в

правом верхнем углу гриф конфиденциальности. Если листы спецблокнота не пронумерованы типографским способом, то они нумеруются. На обложках рабочих и стенографических тетрадей указываются вид носителя, гриф конфиденциальности, инициалы и фамилия исполнителя. Листы тетрадей нумеруются, оборот последнего листа подписывается сотрудником службы делопроизводства с указанием количества листов в тетради. Листы типовых форм документов нумеруются исполнителем, на первом листе проставляется гриф конфиденциальности. Носители конфиденциальной информации учитываются в журналах или карточках (табл. 3) [6, с. 79–80].

В графе 2 арабскими цифрами проставляется дата: в карточке – с указанием числа, месяца и года, в журнале – числа и месяца (год проставляется перед началом регистрации носителей за этот год). В графе 3 пишется: спецблокнот, листы, типовая форма, рабочая тетрадь и др. В графе 4 указывается наименование носителя, если он предназначен для составления конкретного документа, или его назначение, если в него будет вноситься различная информация, например по спецблокноту – «для черновиков», по рабочей тетради – «для рабочих записей» [6, с. 80].

Таблица 3

Форма перечня бумажных носителей конфиденциальной информации

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

Одновременно на самих носителях проставляется:

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

- на рабочих тетрадях – в верхнем левом углу лицевой стороны обложки (а при невозможности в верхнем левом углу форзаца) такой же штамп с указанием учетного номера носителя и количества листов; на отдельных листах документа в верхней части левого поля первого листа проставляется такой же штамп с указанием учетного номера носителя и количества листов; на левом поле остальных листов – штамп «К носителю № __» или сокращенно «К Н № __» с указанием номера.

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

При необходимости постановки на учет дополнительных листов носителя (при нехватке ранее взятых листов для составления черновика документа или для замены испорченных листов) они нумеруются от последнего листа, ранее учтенного по этому номеру носителя, регистрируются в журнале учета носителей под тем же номером, что и ранее

взятые листы, отдельной строкой под ними (при этом заполняются графы 2, 5), на левом поле каждого листа проставляется штамп «К Н № __» с указанием номера, а на первом листе всего носителя прежнее количество листов зачеркивается и проставляется новое с учетом дополнительных листов. Исправление заверяется подписью сотрудника службы делопроизводства. Выдача дополнительных листов производится под отдельную подпись в графе 7 журнала учета носителей [6, с. 82].

Магнитные и оптические носители, предназначенные для отображения (фиксирования) конфиденциальной информации, должны учитываться подразделением конфиденциального делопроизводства до нанесения на них информации в журналах (карточках) учета машинных носителей конфиденциальной информации, в которые целесообразно включать следующие графы:

Таблица 4

Форма журнала учета машинных носителей

Учетный номер и отметка конфиденциальности носителя	**Дата регистрации**	**Вид носителя**	**Тип носителя**	**Наименование информации, наносимой на носитель**	**Отметка о переносе информации на другой носитель**	**Отметка об отправлении носителя**	**Отметка о возврате носителя**	**Отметка об уничтожении (стирании) информации**	**Отметка об уничтожении носителя**
1	2	3	4	5	6	7	8	9	10

Журнал учета машинных носителей, на которые заносится информация, составляющая коммерческую тайну, ведется отдельно от журнала учета машинных носителей, предназначенных для занесения информации, составляющей служебную тайну. Заполнение граф 1, 2 производится таким же образом, как и в журнале учета бумажных носителей. В графе 3 проставляется: магнитный диск, дискета, оптический диск и др. В графе 4 пишется название (марка) носителя. В графе 5 указывается наименование информации, которая будет заноситься на носитель, если она заранее известна, если неизвестна, то графа заполняется по мере нанесения информации. В графе 6 напротив наименования соответствующей информации проставляются типы носителей, на которые перенесена информация (распечатка, дискета и др.), и их учетные номера. В графе 7 проставляются наименование предприятия, на которое направлен носитель, наименование, номер и дата сопроводительного документа. В графе 8 указываются номер и дата сопроводительного письма, если носитель возвращен с сопроводительным письмом, или порядковый номер и дата поступления пакета с носителем, проставленные в журнале учета поступивших пакетов, если носитель возвращен без сопроводительного письма. Если предприятие не осуществляет отправление машинных носителей, то графы 7, 8 опускаются. В графе 9 производится запись «информация уничтожена путем стирания», заверяемая подписью работника, производившего стирание, с проставлением даты.

Такие записи должны осуществляться по мере стирания информации и проставляться напротив ее наименования, указанного в графе 5. Графа 10 заполняется в том случае, если носитель в силу различных причин уничтожается. При этом указывается способ уничтожения. Отметка об уничтожении носителя заверяется подписями двух сотрудников подразделения конфиденциального делопроизводства с проставлением даты уничтожения. На самих машинных носителях проставляются их учетные номера и грифы конфиденциальности (аббревиатурой). Учет бумажных и машинных носителей производится по каждому виду тайны раздельно. В зависимости от количества и продолжительности хранения носителей учет 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 (не уничтоженные) по предыдущему учету носители перерегистрируются по новому учету с отметкой о перерегистрации каждого носителя в предыдущей учетной форме, которая проставляется следующим образом: «Перерегистрирован в журнал (или картотеку) за _____ год под № _____» с указанием года журнала и номера носителя. Отметка проставляется в графе 9 журнала учета бумажных носителей и в графе 10 журнала учета машинных носителей [5, с. 70–71].

2.5. Изготовление и учет проектов конфиденциальных документов

Документы не рекомендуется диктовать, наговаривать на диктофон. Проекты других текстовых документов изготавливаются печатным способом под диктовку или со звуковоспроизводящих устройств либо в два этапа: составление на бумажном носителе черновика проекта документа рукописным способом и последующее печатание проекта документа с черновика. Также возможен вариант внесения переменной части текста в типовые формы документов, хранимые в памяти компьютера, и их дальнейшего распечатывания на принтере [6, с. 83].

Видами материальных носителей конфиденциальных документов могут быть:

- для традиционных текстовых документов – спецблокноты (специальные блокноты с отрывными листами и корешком, выполняющим функцию учета листов, нанесения отметок о целевом их использовании); рабочие тетради для больших по объему документов; отдельные пронумерованные листы бумаги, типографские формы и бланки документов;
- для чертежно-графических документов – пронумерованные листы ватмана, кальки, пленки, миллиметровки (координатной бумаги) и т. п.;
- для машиночитаемых документов – маркированные и пронумерованные магнитные ленты, диски, дискеты, карты и т. п.;
- для аудио- и видеодокументов – маркированные и пронумерованные кассеты с магнитной пленкой, лазерные диски, кассеты с кинопленкой и т. п.;
- для фотодокументов – маркированные и пронумерованные кассеты с фотопленкой, фотобумага, микрофиши, слайды, кассеты с микрофотопленкой [7].

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 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.

При любом способе изготовления (рукописном, печатном) проект документа должен иметь все необходимые и правильно оформленные реквизиты [4, с. 44].

В случае если документ печатается с черновика, на первом листе черновика должны быть проставлены количество необходимых экземпляров проекта документа и фамилия исполнителя, а если подлежащий изданию документ не предусмотрен перечнями издаваемых конфиденциальных документов, то на черновике дополнительно должна стоять виза-разрешение руководителей подразделения, которое издает документ, и подразделения конфиденциального делопроизводства (или службы безопасности).

При приеме черновика от исполнителя сотрудник подразделения конфиденциального делопроизводства обязан:

- при составлении черновика в спецблокноте – просчитать количество листов черновика и изъять их из блокнота;
- при составлении черновика на отдельных листах бумаги или в типовой форме документа – просчитать количество его листов;
- при составлении черновика в рабочей тетради – проверить наличие листов тетради и соответствие их количества заверительной надписи [5, с. 72].

После проведения этих операций данные о черновике вносятся в журнал или карточку учета проектов созданных/изданных конфиденциальных документов (табл. 5).

Таблица 5

Форма журнала или карточки учета проектов созданных/изданных конфиденциальных документов

Учетный номер и отметка конфиденциальности	Дата документа	Вид и заголовок документа	Ф.И.О. исполнителя	Номера носителя и листов черновика	Количество экземпляров документов	Количество листов в экземпляре	Подпись за получение черновика и проекта документа	Подпись за возврат, дата
1	2	3	4	5	6	7	8	9

Окончание

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

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

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

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

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

Форма расписки исполнителя за получение отдельных листов бумаги, типовой формы документа, стенографической или рабочей тетради

РАСПИСКА

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

После печатания проекта документа заполняются графы 6–7 журнала учета созданных/изданных документов, проект документа вместе с черновиком передается исполнителю под подпись в графе 8. Разовая расписка, выданная ранее исполнителю за получение носителя (черновика), возвращается сотруднику службы конфиденциального делопроизводства и уничтожается [6, с. 84].

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

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

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

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

Эти же графы заполняются при печатании проекта документа со звуковоспроизводящих устройств (в графе 5 проставляются вид и номер носителя речевой информации). Прием/возврат носителя осуществляется по разовой расписке [6, с. 86].

Если проект документа был отпечатан как открытый, а в процессе визирования или подписания было принято решение о переводе его в разряд конфиденциальных, то исполнителем должны быть представлены в службу делопроизводства все экземпляры отпечатанного проекта и черновик. На обороте последнего экземпляра проекта исполнитель указывает, сколько экземпляров отпечатано и сколько листов в черновике, заверяя это своей подписью. При отсутствии черновика или отдельных экземпляров проекта документа руководителем организации назначается комиссия для их поиска. Если они не будут найдены, то об этом делается отметка на обороте последнего экземпляра проекта за подписью председателя комиссии.

Об обстоятельствах утраты докладывается руководителю организации для принятия соответствующих решений [6, с. 86–87].

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

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

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

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

Сотрудник службы делопроизводства расписывается за получение конфиденциального документа (проекта) черновика в графе 9 журнала учета созданных/изданных документов, одновременно проставляя в графе 2 дату документа, которая должна соответствовать дате его подписания (утверждения) [6, с. 87].

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

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

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

ответствующий штамп, заверяемый подписью сотрудника службы делопроизводства с указанием даты.

Вопросы для самоконтроля

1. Для чего используется спецблокнот? Как он выглядит?
2. Что входит в оформление таких бумажных носителей конфиденциальной информации, как спецблокнот и рабочая тетрадь?
3. Какие сведения указывают в расписке за получение отдельных листов бумаги, типовой формы документа, рабочей тетради?
4. Какие операции проводит сотрудник подразделения конфиденциального делопроизводства при приеме черновика от исполнителя?
5. Каким способом изготавливаются проекты конфиденциальных документов? Возможна ли предварительная надиктовка на диктофон?

2.6. Учет использования и хранения печатей, штампов, бланков

Согласно ГОСТ Р 7.0.8-2013 **печать –** это устройство, используемое для заверения подлинности подписи должностного лица посредством нанесения его оттиска на документ [2].

Рис. 4. Примеры печатей организаций

Федеральные органы власти применяют печати с изображением Государственного герба Российской Федерации. Порядок применения гербовых печатей устанавливается российским законодательством. Порядок применения печатей с изображением Государственного герба регулируется Федеральным конституционным законом от 25 декабря 2000 г. № 2-ФКЗ «О Государственном гербе Российской Федерации» [1]. Негосударственные организации применяют печать с наименованием самой организации в соответствии с уставом организации [6, с. 93].

Печать заверяет подлинность подписи должностного лица на документах, удостоверяющих права лиц, фиксирующих факты, связанные с финансовыми средствами, а также на иных документах, предусматривающих заверение подписи печатью в соответствии с законодательством Российской Федерации.

Документы заверяют печатью организации. Печать проставляется, не захватывая собственноручной подписи лица, подписавшего документ, или в месте, обозначенном «МП» («Место печати») [3].

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

Печатью заверяются подписи руководителя, его заместителей, финансовой службы, главного бухгалтера, а также других должностных лиц, которым доверенностью или распорядительным документом руководителя предоставлены соответствующие полномочия.

Передача печатей посторонним лицам и вынос их за пределы территории организации не допускаются.

Служба делопроизводства ведет общий учет имеющихся в организации печатей и штампов в специальном журнале с проставлением их оттисков (табл. 6). Выдача печатей и штампов осуществляется под расписку работникам, персонально ответственным за их использование и хранение. Листы журнала учета печатей и штампов нумеруются, прошнуровываются и опечатываются.

Печати хранятся в надежно запираемых шкафах. Ответственность за законность использования и хранение главной печати организации возлагается на руководителя. Ответственность за хранение, законность использования других печатей возлагается на руководителей соответствующих подразделений. Порядок хранения печатей и штампов, правильность их использования в структурных подразделениях проверяется подразделением, ответственным за учет печатей. В случае служебной необходимости по решению руководителя организации допускается изготовление дополнительных экземпляров печати [6, с. 94].

Для проставления отметки о заверении копии может использоваться штамп. С помощью штампа также может проставляться отметка о поступлении документа.

Еще один пример использования штампа: отметка о контроле, свидетельствующая о постановке документа на контроль, проставляется штампом «Контроль» на верхнем поле документа [3].

Штамп – это устройство прямоугольной формы для проставления отметок справочного характера о получении, регистрации, прохождении, исполнении документов и др. [6, с. 94]

Таблица 6

Форма журнала учета печатей и штампов

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

Окончание

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

Пришедшие в негодность и утратившие значение печати и штампы подлежат возврату по месту выдачи, где они уничтожаются по акту с соответствующей отметкой в журнале учета [6, с. 96].

Бланки

Бланк документа – это лист бумаги или электронный шаблон с реквизитами, идентифицирующими автора официального документа [2].

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

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

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

Организация работы по изготовлению бланков возлагается на административно-хозяйственную службу, которая получает от службы делопроизводства заявки на изготовление бланков документов, а также, при необходимости, их образцы (макеты); оформляет заказы на изготовление в типографии печатно-бланочной продукции; получает и ведет учет и выдачу в службу делопроизводства изготовленных бланков документов.

Изготовленные бланки документов нумеруются типографским способом или нумератором в службе делопроизводства. Порядковый номер проставляется в нижней части оборотной стороны бланка. Учет бланков ведется раздельно по их видам в журнале [6, с. 96].

Журнал учета бланков

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

Бланки выдаются работникам, ответственным за делопроизводство в подразделениях, под роспись в журнале учета выдачи бланков [6, с. 96].

Журнал учета выдачи бланков в структурные подразделения

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

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

Контроль за изготовлением, использованием и хранением бланков возлагается на службу делопроизводства. Лица, персонально ответственные за учет, использование и хранение бланков, назначаются распорядительным документом руководителя организации. Регистрационно-учетные формы необходимо включать в номенклатуру дел.

Проверку наличия, использования и хранения бланков проводят не реже одного раза в год экспертной комиссией, назначаемой распорядительным документом руководителя организации. О проведенных проверках делают отметки в учетно-регистрационных формах после последней записи. В случае обнаружения нарушений при изготовлении, учете, хранении и использовании бланков комиссия проводит служебное расследование, результаты которого оформляют актом и доводят до сведения руководства организации [6, с. 98].

Вопросы для самоконтроля

1. Дайте определение понятиям «печать», «штамп», «дата документа». В каком нормативном документе приведены названные термины?
2. Каковы правила проставления оттиска печати?
3. Какой локальной документ организации устанавливает применение печатей?
4. Чьи подписи заверяются печатью?
5. Приведите примеры использования штампов.

2.7. Особенности печатания, тиражирования и размножения конфиденциальных документов

Рис. 5. Ризограф – техническое средство тиражирования документов

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

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

Черновики и варианты уничтожаются с подтверждением факта уничтожения записью на копии отправляемого (исходящего) письма или подлиннике организационно-распорядительного документа: «Черновик (и варианты) уничтожены. Дата. Подпись». Запись производится непосредственно исполнителем или сотрудником структурного подразделения в зависимости от того, где были уничтожены черновики и варианты документа [6, с. 90].

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

В службе делопроизводства должны храниться регулярно обновляемые копии используемых исполнителями электронных носителей. Работа с электронными конфиденциальными документами разрешается только при наличии в организации сертифицированной системы защиты компьютеров и локальной сети [6, с. 91].

Допускается копирование (тиражирование) исполнителем непосредственно в подразделениях, имеющих копировальную технику, небольших по объему конфиденциальных документов. Порядок использования имеющейся копировальной техники в подразделениях устанавливается их руководителями. Учет выполненных копировальных работ ведется в журналах, которые выдаются службой делопроизводства сотрудникам, принявшим копировальную технику на ответственное хранение. Дополнительно размноженные экземпляры учитываются в службе делопроизводства за номером подлинника и в той же учетной форме. Выписки из документов делаются также с разрешения руководителя подразделения и учитываются за новыми номерами на карточках регистрации созданных/изданных документов.

Целевое использование сотрудниками копировальной техники следует строго контролировать.

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

О выполнении заказа делается соответствующая отметка. Учет выполненных работ по копированию конфиденциальных документов ведется на основании заказов.

Форма заказа на копирование документов

сшить
с обложкой
с оборотом
уменьшить
увеличить
(необходимое подчеркнуть)

ЗАКАЗ
на копирование документов

Индекс или наименование
подразделения _____
Исполнитель _____
Телефон _____
Наименование документа (полностью) _____
_____
Стр. _____ Экз. _____
Дата _____ Время _____
Подпись _____
Оператор _____ Дата _____ Время _____
Подпись исполнителя, получившего заказ _____
Дата _____ Время _____

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

Тиражирование и размножение конфиденциальных документов и изданий в типографии производится с разрешения службы делопроизводства (если такая служба существует в организации) и под контролем службы безопасности. В типографиях учет тиражируемых документов и изданий может осуществляться с учетом других открытых материалов [6, с. 93].

Вопросы для самоконтроля

1. В каком месте на документе указываются количество отпечатанных экземпляров, фамилия исполнителя, фамилия ответственного за распечатку и дату печатания документа?
2. Каким образом подтверждается факт уничтожения черновиков и вариантов документа?
3. Разрешается ли копирование (тиражирование) бланков документов, используемых в организации?
4. Каким образом ведется учет выполненных работ по копированию конфиденциальных документов?
5. Какие сведения указываются в заказе на копирование документов?

Список использованных источников и литературы

Источники

1. Федеральный конституционный закон от 25 декабря 2000 г. № 2-ФКЗ «О Государственном гербе Российской Федерации». URL: http://www.consultant.ru/document/cons_doc_LAW_29674/ (дата обращения: 16.12. 2019).

2. ГОСТ Р 7.0.8-2013. Национальный стандарт Российской Федерации. «Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения» (утв. Приказом Росстандарта от 17 октября 2013 г. № 1185-ст). URL: http://www.consultant.ru/document/cons_doc_LAW_163800/ (дата обращения: 15.07.2019).

3. ГОСТ Р 7.0.97-2016. Национальный стандарт Российской Федерации. «Система стандартов по информации, библиотечному и издательскому делу. Организационно-распорядительная документация. Требования к оформлению документов» (утв. Приказом Росстандарта от 08 декабря 2016 г. № 2004-ст). URL: http://www.consultant.ru/ document/cons_doc_LAW_216461/ (дата обращения: 16.12. 2019).

Литература

4. Алексенцев А.И. Конфиденциальное делопроизводство [Электрон. ресурс] // Управление персоналом. М., 2003. 200 с. (pdf).

5. Егоров В.П. Конфиденциальное делопроизводство [Электрон. ресурс]: учеб. пособие / В.П. Егоров, А.В. Слиньков. М.: Юридический институт МИИТа, 2015. 178 с. (pdf).

6. Куняев Н.Н. Конфиденциальное делопроизводство и защищенный электронный документооборот [Электрон. ресурс]: учебник / Н.Н. Куняев, А.С. Демушкин, А.Г. Фабричнов; под общ. ред. Н.Н. Куняева. М.: Логос, 2011. 452 с. (Новая университетская библиотека). (pdf).

7. Фирсова А.Ю. Модуль 8. Работа с конфиденциальными документами. Курс повышения квалификации/профессиональной переподготовки «Основы делопроизводства и секретарское дело» [Электрон. ресурс] // Академия подготовки главных специалистов [сайт]. [2019]. URL: https://specialitet.ru (дата обращения: 03.11.2019).

Глава 3
ОРГАНИЗАЦИЯ КОНФИДЕНЦИАЛЬНОГО ДОКУМЕНТООБОРОТА

Документооборот – это движение документов в организации с момента их создания или получения до завершения исполнения или отправки [7].

Основной целью организации конфиденциального документооборота является учет и регистрация конфиденциальных документов с целью формирования контрольной и справочно-информационной базы для оперативного нахождения, контроля исполнения, представления необходимых справок о конфиденциальных документах, а также для проверки их наличия, обеспечивающей постоянный мониторинг сохранности и защиты каждого документа и своевременное фиксирование его местонахождения [9, с. 99].

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

Учет, регистрация и хранение конфиденциальных документов, как правило, осуществляются централизованно в службе делопроизводства [9, с. 102].

Регистрация документа – присвоение документу регистрационного номера и внесение данных о документе в регистрационно-учетную форму [7].

3.1. Обработка поступающих конфиденциальных документов, их учет и регистрация

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

Конфиденциальные документы должны пересылаться (доставляться) между организациями в запечатанных пакетах, оформленных соответствующим образом [9, с. 107].

Важно! Следует учитывать ту особенность, что на пакетах, а часто на самих конфиденциальных документах не ставится гриф ограничения доступа. Это объясняется нежеланием отправителя обращать внимание посторонних лиц на отметку о конфиденциальности. Поэтому предварительное рассмотрение и распределение всей поступающей документированной информации должно выполняться квалифицированным сотрудником службы делопроизводства, обладающим знаниями структуры организации, функций структурных подразделений и обязанностей работников, состава и перечня конфиденциальной документированной информации и таких же перечней структурных подразделений организаций [9, с. 108].

Прием, первичная обработка, предварительное рассмотрение и распределение делопроизводителем поступивших документов включают следующие процедуры (схема 3) [11].

Схема 3. Последовательность и характеристика процедур приема, первичной обработки, предварительного рассмотрения и распределения документов

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

При нарушении оформления пакетов, несоответствии данных на пакете и в сопроводительном документе, а также повреждении упаковки составляется акт в двух экземплярах, который подписывается сотрудником службы делопроизводства и лицом, доставившим пакеты. Второй экземпляр акта направляется отделению связи, доставившему пакет, или организации – отправителю пакета, если он доставлен, минуя отделение связи. Если повреждение пакета позволяет изъять документ или прочесть его, то об этом сообщается руководству организации и службы делопроизводства, а пакет не принимается до принятия решения [9, с. 109].

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

Таблица 7

Журнал учета поступивших конфиденциальных пакетов

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

Окончание

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

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

Ошибочно присланные документы могут по согласованию с организацией-отправителем пересылаться по назначению, под их учетными номерами, в новых пакетах с вложением в них лицевой стороны пакета организации-отправителя. В этом случае в графе 9 журнала учета поступивших пакетов делается отметка о пересылке с указанием организации, которой направлен документ, номера и даты сопроводительного письма [9, с. 111].

3.1.2. Учет и регистрация поступивших (входящих) конфиденциальных документов

Учет и регистрация поступивших конфиденциальных документов осуществляются одновременно в единой форме (табл. 8), как правило, в день поступления.

Таблица 8

Форма журнала или карточки учета поступивших документов

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

Окончание

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

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

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

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

Если в организацию возвращены отправленные ранее без сопроводительного письма все или часть экземпляров документа, то производится отметка об их возвращении без присвоения входящего номера. Эта отметка проставляется в графе 8 журнала учета поступивших пакетов напротив возвращенного номера вложенного в пакет документа, например: № 12 (при возврате документа), № 2 (при возврате документа выделенного хранения), вх. № 15 (при возврате документа, зарегистрированного по входящему номеру).

Одновременно в графе 15 журнала учета созданных/изданных документов или в графе 11 журнала (карточки) учета документов инвентарного (выделенного) хранения (см. разд. 3.6) делается запись: «Экз. № __ возвращены, п/ж № __ за __» с проставлением номеров экземпляров, порядкового номера и даты поступления пакета, в котором находились возвращенные экземпляры. В графе 14 журнала учета поступивших документов (под отметкой об отправлении) производится запись: «Возвращен, п/ж № __ за __» с проставлением порядкового номера и даты поступления пакета с возвращаемым документом (п/ж означает «журнал поступивших пакетов») [9, с. 112–113].

При карточном способе учета конфиденциальной документированной информации (как и ее носителей) необходимо вести контрольный журнал, предназначенный для учета, обеспечения последовательности проставления номеров и контроля за местонахождением этой информации, находящейся в обращении, ускорения ее поиска, а также для проставления отметок о проверках на ее наличие. Контрольный журнал заводится по каждому виду карточного учета и регистрации документов (поступающие, внутренние, отправляемые) и отдельно для носителей (табл. 9) [9, с. 103].

Таблица 9

Форма контрольного журнала

Учетный и регистрационный номер документа (носителя), дата учета и регистрации	**Вид и наименование носителя, номера экземпляров, количество листов в экземпляре**	**Местонахождение документа (носителя)**	**Отметки о проведении проверки наличия документов (носителей)**
1	2	4	5

Вопросы для самоконтроля

1. Как вы понимаете, что такое конфиденциальный документооборот?
2. Приведите определение понятия «регистрация документа». Зачем нужна регистрация конфиденциальных документов?
3. Что включает в себя учет конфиденциальных документов?
4. Для чего нужен Перечень поступивших документов, направляемых на исполнение без доклада руководителю организации?
5. Что включает в себя экспедиционная обработка и учет поступающих пакетов с конфиденциальными документами?

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

Процедура передачи изданных внутренних документов на рассмотрение или исполнение включает две составляющие (схема 4).

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

Для регистрации внутренних конфиденциальных документов исполнитель сдает сотруднику службы делопроизводства:

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

Схема 4. Процедура передачи изданных внутренних документов на рассмотрение или исполнение

О сдаче и уничтожении указанных материалов сотрудник службы делопроизводства делает отметку в учетной карточке документов, находящихся у исполнителя. Отметка заверяется подписями сотрудника службы и исполнителя. Факт уничтожения черновика и других материалов подтверждается также отметкой на копии документа, остающейся в деле службы делопроизводства, например: «Черновик уничтожен. Дата. Подпись сотрудника делопроизводства». Черновики и другие материалы уничтожаются путем измельчения, исключающего возможность восстановления текста. Попытки исполнителей оставить в своем распоряжении какие-либо неучтенные материалы по исполненному документу должны рассматриваться руководством организации как грубое нарушение работы с конфиденциальными документами и трудовой дисциплины.

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

Регистрация конфиденциальных распорядительных документов ведется отдельно от их учета. Для обеспечения последовательности проставления таких номеров, ускорения их поиска журналы учета или карточки (электронные карточки в АИС) созданных конфиденциальных документов необходимо вести по каждому их виду отдельно (табл. 10).

Таблица 10

Форма журнала/карточки регистрации распорядительных конфиденциальных документов

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

В графе 3 проставляется учетный номер документа, присвоенный ему на стадии учета его проекта до основной регистрации по журналу учета созданных/изданных документов (см. разд. 2.5).

Графы 1–4 обязательны, целесообразность включения граф 5–7 должна определяться главным образом объемом и характером справочной работы по конфиденциальным распорядительным документам.

Приложения к созданным/изданным документам являются самостоятельными документами и имеют свои номера по соответствующим видам учета [9, с. 113–114].

3.3. Технологии исполнения и контроля за исполнением конфиденциальных документов

При большом объеме поступающих документов целесообразно их предварительно рассмотреть и распределить по уровням принятия решений по ним. С этой целью разрабатывается перечень поступивших документов, направляемых на исполнение без доклада руководителю организации. В перечень включаются конкретные наименования поступающих документов, которые имеют, как правило, типовой и повторяющийся характер и адресуются заместителям руководителя организации, руководителям структурных подразделений или непосредственным исполнителям без рассмотрения их руководителем организации. Перечень подписывается председателем и членами экспертной комиссии и вводится в действие приказом руководителя организации. В приказе определяется должностное лицо, которому предоставляется право адресования документов, включенных в перечень [9, с. 116].

Перечень позволяет сократить путь и время движения документов до непосредственных исполнителей и, следовательно, ускорить процесс их исполнения, освободить руководство от рассмотрения вопросов, которые могут быть решены непосредственными исполнителями документов, уменьшить трудозатраты на рассмотрение, исполнение и обработку документов, обеспечить выполнение требований разрешительной системы доступа к поступившим конфиденциальным документам (табл. 11).

Таблица 11

Форма переченя поступивших документов, направляемых на исполнение без доклада руководителю организации

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

Не включенные в перечень документы, подлежащие рассмотрению непосредственно руководителем организации, передаются ему (его помощнику, секретарю) под подпись в журнале передачи конфиденциальных документов, если они не рассматриваются в присутствии сотрудника службы делопроизводства, ответственного за их учет (табл. 12).

Таблица 12

Форма журнала передачи конфиденциальных документов

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

Если документ одновременно выдается по частям нескольким исполнителям, то при карточном учете подписи за получение документа проставляются на основной карточке, которая ставится в ячейку картотеки по фамилии одного из исполнителей, в ячейки остальных исполнителей помещаются сигнальные карточки, которые могут быть либо дубликатом основной карточки с указанием количества листов (экземпляров), выданных исполнителю, либо содержать лишь сведения об учетном номере документа, фамилию соответствующего исполнителя, количестве полученных им листов (экземпляров). Применение автоматизированных электронных картотек контроля исполнения упрощает данный процесс [9, с. 118].

При работе с конфиденциальными документами руководители и исполнители обязаны:

- знакомиться только с теми конфиденциальными документами, к которым они получили разрешение на доступ в силу должностных обязанностей;
- предъявлять работнику службы делопроизводства числящиеся за ними документы для проверки их наличия и комплектности;
- вести учет находящейся у них конфиденциальной документации;
- ежедневно по окончании рабочего дня проверять наличие документов и сдавать их на хранение в службу делопроизводства;
- немедленно сообщать непосредственному руководителю и в службу делопроизводства об утере или недодаче документов, обнаружении лишних или неучтенных документов, отдельных листов;
- сдавать по описи в службу делопроизводства все числящиеся за ними документы при увольнении, уходе в отпуск, отъезде в командировку [9, с. 120–121].

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

- предотвратить выдачу документов лицу, не имеющему права доступа к нему;
- зафиксировать факт передачи документа исполнителю;
- обеспечить физическую сохранность документа, приложений, листов и других частей документа;
- ознакомить исполнителя только с той частью документа, которая ему адресована;
- предотвратить возможность ознакомления с документом постороннего лица при выдаче документа исполнителю и его возврате;
- обеспечить учет документов, находящихся у исполнителей [9, с. 121].

Вопросы для самоконтроля

1. Что включает в себя процедура передачи изданных внутренних документов на рассмотрение или исполнение?
2. Какие обязанности возлагаются на руководителей и исполнителей при работе с конфиденциальными документами?
3. Какие действия требуется выполнить сотруднику службы делопроизводства, выдавая документы исполнителям для работы?
4. На какой стадии работы с документами начинается учет и регистрация внутренних (созданных/изданных) конфиденциальных документов?
5. Какие поступившие документы отправляются без доклада руководителю и какие сведения включает форма журнала об этой процедуре?

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

3.4.1. Учет и регистрация отправляемых конфиденциальных документов

При отправлении документов заполняется журнал изданнных/отправляемых конфиденциальных документов (табл. 13) [9, с. 122].

Таблица 13

Форма журнала изданнных/отправляемых конфиденциальных документов

№ п/п	Издано или поступило			
	Наименование документа	Откуда поступил, где отпечатан	Входящий номер сопроводительного письма и дата	Количество и номера экземпляров
1	2	3	4	5

Окончание

Распределение			Возврат	Уничтожение
Куда и кому отправлен или выдан	Номер исходящего документа или расписка в получении и дата	Количество и номера экземпляров	Дата, номера экземпляров	Дата, номер акта
6	7	8	9	10

При отправлении документов также производятся соответствующие отметки, а именно:

- в журнале или карточке учета проектов внутренних (созданных/изданных) конфиденциальных документов в графах 12–14 (см. разд. 2.5);
- в журнале или карточке учета и распределения внутренних (созданных/изданных) конфиденциальных документов (табл. 14);
- в журнале инвентарного (выделенного) учета в графах 8–10 (см. разд. 3.5) [9, с. 122].

Таблица 14

Форма журнала/карточки учета и распределения внутренних (созданных/изданных) конфиденциальных документов

Регистрационный номер и отметка конфиденциальности отправляемого документа	Дата отправления	Вид и заголовок документа	Адресат получателя отправляемого документа	Количество листов приложений
1	2	3	4	5

Окончание

Количество листов документа	Индекс (номер) дела, номера листов дела	Номер по инвентарному (выделенному) учету	Примечание
6	7	8	9

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

Если по каким-либо причинам отправлен документ (или часть его), зарегистрированный в журнале (карточке) учета проектов созданных документов, то в журнале проставляется отметка об отправлении (см. разд. 3.1.2). В ней указываются: количество отправленных листов, куда они отправлены, наименование, номер и дата сопроводительного документа, например: «3 листа отправлены в АОО «Межрегионсервис» по реестру № 7 от 21.01.2010 г.» [9, с. 123].

3.4.2. Экспедиционные технологии обработки и рассылки отправляемой конфиденциальной документированной информации

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

- исключить возможность тайного вскрытия этих документов и несанкционированного ознакомления с ними в процессе их пересылки (передачи) адресату, подмены документов и листов;
- ограничить возможность утери, кражи или подмены пакета с конфиденциальными документами;
- подтвердить факт отправки конфиденциальной документированной информации и правильность оформления этого факта в учетных формах;
- исключить ошибочную отправку документов другому адресату, необоснованную рассылку ряду адресатов [9, с. 124].

Разрешением на отправку конфиденциальной документированной информации является подписание руководством организации сопроводительного письма к ней или разрешительная отметка в учетном журнале отправляемых пакетов (табл. 15), если документы отправляются без сопроводительного письма [9, с. 125].

Таблица 15

Форма журнала отправляемых пакетов

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

Варианты упаковки конфиденциальных документов

Первый вариант. Конфиденциальная документированная информация упаковывается в два пакета (двойное пакетирование). На внутреннем пакете проставляются: отметка конфиденциальности (в правом верхнем углу пакета), соответствующая наивысшей степени конфиденциальности документов, подлежащих вложению в пакет; фамилия лица, которому документ адресуется; номера вложенных документов, при необходимости ставится пометка «Лично».

Внутренний пакет опечатывается бумажными наклейками, на которые ставится печать «Для пакетов» или службы делопроизводства. Внешний пакет оформляется в

соответствии с почтовыми правилами, указанные сведения о конфиденциальности информации на него не выносятся. Пакеты с конфиденциальными документами пересылаются ценными отправлениями.

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

Второй вариант. На одном светонепроницаемом пакете пишутся адрес и наименование организации-получателя (открытые или условные), под которыми перечисляются учетные номера конфиденциальных документов, вкладываемых в пакет. Если конфиденциальная документированная информация отправляется с сопроводительным письмом, то на пакете проставляется только номер сопроводительного письма без указания номеров приложений. При направлении документов в двух и более экземплярах на пакете рядом с номером документа в скобках указываются номера экземпляров. Ниже проставляются адрес и наименование организации-отправителя [9, с. 125]. Например:

1. *Получатель:* 301264, Садовая ул., д. 5, г. Люберцы, Московская обл., ЗАО «Энерго». № 543/ДСП, 456/ДСП

Отправитель: 117393, г. Москва, д. 82, ВНИИДАД.

2. *Получатель:* 301264, Садовая ул., д. 5, г. Люберцы, Московская обл., ЗАО «Энерго». № 148 (пять экз.)

Отправитель: 117393, г. Москва, д. 82, ВНИИДАД.

На упаковке конфиденциальных документов и изданий не рекомендуется указывать фамилии и должности руководителей и сотрудников, а также наименования структурных подразделений [9, с. 127].

Вопросы для самоконтроля

1. Какие сведения включает журнал изданных/отправляемых конфиденциальных документов?
2. Какие отметки производятся при отправлении документов?
3. Чем отличается регистрация документов, поступивших с сопроводительным письмом и без него?
4. Назовите варианты упаковки конфиденциальных документов.
5. Какие изменения технических носителей информации сигнализируют об их несанкционированном вскрытии?
6. По какой причине при отправке на пакетах, а часто на самих конфиденциальных документах не ставится гриф ограничения доступа?

3.5. Учет конфиденциальной документированной информации инвентарного (выделенного) хранения

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

- не подлежащие подшивке в дела, например: сброшюрованные, документы большого формата, чертежно-графические, научно-технические, в том числе являющиеся приложениями к основным, фотографии, рисунки, электронные документы на соответствующих носителях (дискеты, флеш-памяти);
- изъятые по какой-либо причине из дела и переведенные на выделенное хранение (образовавшие самостоятельное дело), например, документы, доступ к которым имеет более узкий круг лиц;

- технические носители информации (чистые или с записанной информацией), например, дискеты, видео- и аудиокассеты, кассеты с фотопленкой и др.;
- бумажные носители информации для составления черновиков, оригиналов и подлинников документов, например, рабочие тетради, отдельные листы бумаги, тетради с отрывными листами и др.;
- журналы (картотеки) учета документов, картотеки учета выдачи дел и документов, законченные дела.

Журнал (картотека) инвентарного учета (табл. 16) ведется непрерывно, номера каждого года продолжают номера предыдущих лет. Вызвано это тем, что выделенному хранению подлежат, как правило, документы постоянного и долговременного хранения, и их ежегодная перерегистрация привела бы к увеличению трудоемкости обработки конфиденциальной документированной информации и созданию сложностей для пользователей.

Таблица 16

Форма журнала (картотеки) инвентарного учета

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

Продолжение

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

Окончание

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

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

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

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

При поступлении конфиденциальной документированной информации, созданной другой организацией и подлежащей инвентарному учету, ей сразу (без оформления в журнале учета и регистрации поступивших конфиденциальных документов) присваивается очередной порядковый номер по журналу (карточке) инвентарного учета. Этот номер проставляется на документе, в графе 8 журнала учета поступивших пакетов и в графе 1 журнала (карточки) инвентарного учета с одновременным заполнением граф 2–7 этого журнала. При этом в графе 5 указывается: «п/ж № __ за __» (где «п/ж» – журнал учета пакетов), с проставлением номера и даты поступления пакета, в котором находился конфиденциальный документ [9, с. 132].

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

На каждый конфиденциальный документ заводится карточка учета выдачи по следующей форме [9, с. 133].

Форма карточки учета выдачи конфиденциальных документов инвентарного хранения

КАРТОЧКА
выдачи конфиденциального документа инвентарного учета

_____
(учетный номер и наименование документа)

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

Вопросы для самоконтроля

1. Что вы понимаете под инвентарным учетом?
2. Какие конфиденциальные документы берутся на инвентарный (выделенный или списочный) учет?
3. Какие сведения вносятся в журнал (картотеку) инвентарного учета?

3.6. Корпоративный конфиденциальный электронный документооборот

Организация работы с конфиденциальными электронными документами должна включать следующие взаимосвязанные системы:

- системы электронного конфиденциального документооборота;
- системы защиты информации, циркулирующей в системе электронного конфиденциального документооборота;
- системы электронного конфиденциального информационного хранилища;
- системы сопряжения конфиденциального электронного и бумажного документооборота.

Система электронного конфиденциального документооборота должна предусматривать следующие возможности:

- создания электронных документов с помощью текстовых редакторов, включая создание электронных документов по типовым формам;

- создания составных электронных документов, состоящих из нескольких разных по формату файлов;
- создания электронных документов с помощью сканирования документа на бумажном носителе;
- создания электронных документов с помощью иных электронных данных, полученных с помощью:

1. электронной почты;
2. корпоративной компьютерной сети;
3. устройств ввода компьютерной информации (дисководы и т.д.);

- работы с электронными документами различных форматов (текстовых, графических и т.д.);
- создания регистрационной карточки электронного документа, связки регистрационной карточки с электронным документом и присвоение необходимых реквизитов, среди которых:

1. дата создания, получения, исполнения;
2. регистрационный номер;
3. фамилия, имя, отчество исполнителя, адресата;
4. права доступа;
5. степень конфиденциальности;
6. количество листов и т. д.;

- разделения документов по степени конфиденциальности, присвоения каждому документу грифа конфиденциальности и разграничения права пользователей работы с конфиденциальными документами по мандатному принципу;
- получения и отправления электронных документов (документооборот) по корпоративной компьютерной сети, а также по электронной почте;
- работы с взаимосвязанными документами, поддержания возможности установления ссылок между учетными карточками или документами, связанных тематически, отменяющих или дополняющих друг друга (например, с помощью гиперссылок с возможностью просмотра цепочки взаимосвязанных документов);
- контроля передвижения электронных документов по сети и контроля ознакомления с электронными документами, а также контроля за копированием, редактированием и размножением электронных документов;
- осуществления контрольных функций (контроля исполнения резолюций, поручений, сроков исполнения и т.д.), а также возможность сигнального режима, как составной части контроля;
- поиска электронных документов по:

1. реквизитам;
2. ключевым словам;
3. содержанию;
4. дате создания;
5. контрольным срокам;
6. исполнителю и т. д.;

- анализа электронных документов по:

1. тематике;
2. проблематике;
3. исполнителям;
4. резолюциям;
5. дате создания и т. д.;

- дублирования (архивирования) электронных документов с заданной периодичностью, а также ведения систематизированных электронных архивов документов, их образов, учетных карточек с возможностью поиска и анализа;
- разделения конфиденциального и открытого электронного делопроизводства [10].

Вопросы для самоконтроля

1. Дайте определение термина «документооборот».
2. Что вы понимаете под корпоративным конфиденциальным электронным документооборотом?
3. Что включает в себя организация работы с конфиденциальными электронными документами?
4. Какие возможности должна предусматривать система электронного конфиденциального документооборота?

3.7. Создание отдела конфиденциального делопроизводства

Численный состав сотрудников подразделения конфиденциального делопроизводства должен определяться объемом выполняемой работы с учетом норм времени на ее выполнение. Поскольку государственных нормативов времени на работы, связанные с конфиденциальным делопроизводством, нет, следует использовать государственные нормативы времени, установленные для открытого делопроизводства [8, с. 46], например:

- Нормы времени на работы по документационному обеспечению управленческих структур федеральных органов исполнительной власти, утвержденные постановлением Министерства труда и социального развития РФ от 26 марта 2002 г. № 23;
- Межотраслевые укрупненные нормативы времени на работы по документационному обеспечению управления, утвержденные постановлением Министерства труда РФ от 25 ноября 1994 г. № 72;
- Нормы времени на работы по автоматизированной архивной технологии и документационному обеспечению органов управления, утвержденные постановлением Министерства труда РФ от 10 сентября 1993 г. № 152;
- Укрупненные нормы времени на работы, выполняемые в объединенных архивах, хранящих документы по личному составу учреждений, организаций, предприятий, утвержденные постановлением Министерства труда России от 18 декабря 1992 г. № 57.

Как показывает практика, содержащиеся в названных и других документах нормативы применительно к конфиденциальному делопроизводству должны быть увеличены в среднем примерно на 20–25%, что вызывается большим количеством и большей сложностью операций с конфиденциальными документами [8, с. 46].

При определении должностей следует руководствоваться «Общероссийским классификатором профессий рабочих, должностей служащих и тарифных разрядов» (ОК 01694), регламентирующим наименования должностей, а также использовать «Квалификационный справочник должностей руководителей, специалистов и других служащих», утвержденный постановлением Министерства труда и социального развития РФ, в котором содержатся квалификационные требования к должностям [8, с. 47].

Основные задачи и функции подразделения конфиденциального делопроизводства, а также права и ответственность его руководителя должны быть закреплены в положении о подразделении, а обязанности, права, ответственность сотрудников подразделения конфиденциального делопроизводства или специально назначенных для ведения конфиденциального делопроизводства лиц – в должностных инструкциях, разрабатываемых на конкретные должности [8, с. 48].

3.8. Постоянно действующая экспертная комиссия и ее задачи

В постоянно действующую экспертную комиссию по защите конфиденциальной информации (ПДЭК) входят следующие подразделения: служба безопасности, служба делопроизводства, служба кадров и подразделение информационных технологий и автоматизированной информационной системы (информационно-технологический центр, главный вычислительный центр и др.).

Основными функциями ПДЭК являются:

- организация работы по формированию Перечня (номенклатуры) должностных лиц, имеющих полномочия в отношении отнесения информации к конфиденциальной. Перечень утверждается приказом организации;
- организация работы по формированию и созданию Перечня конфиденциальной документированной информации организации;
- организация работы по формированию и созданию Реестра конфиденциальной информации и автоматизированной информационной системы;
- подготовка предложений по организации разработки и выполнению программ, планов, нормативных и методических документов, обеспечивающих реализацию доступа к конфиденциальной информации, ее защиту и охрану, и представление их в установленном порядке руководству организации;
- рассмотрение и представление руководству организации предложений по нормативному регулированию вопросов режима конфиденциальности информации, доступа к ней и совершенствованию системы защиты и охраны конфиденциальной информации в организации;
- подготовка и предоставление руководству организации предложений по отнесению информации к конфиденциальной, к различным степеням конфиденциальности [9, с. 146–147].

Учитывая важность задач ПДЭК, в ее состав следует включать высококвалифицированных сотрудников, в первую очередь руководителей подразделений, имеющих доступ к конфиденциальной информации. Кроме того, в состав комиссии должны входить руководитель службы безопасности предприятия и руководитель подразделения конфиденциального делопроизводства, а также руководитель архива предприятия (при наличии архива). Председателем комиссии необходимо назначать одного из заместителей руководителя предприятия, допущенного ко всем конфиденциальным документам.

ПДЭК создается приказом руководителя предприятия и должна работать на постоянной основе с заменой в необходимых случаях отдельных ее членов. Задачи, функции и порядок работы комиссии определяются положением о ней. На ПДЭК может быть возложено и проведение экспертизы ценности открытых документов с тем, чтобы она могла оценивать значение документов, образующихся в деятельности предприятия, в их совокупности и таким образом более правильно определять сроки их хранения. Сотрудники, работающие с конфиденциальными документами, должны иметь допуск к соответствующим видам тайны.

Допуск сотрудников предприятия к коммерческой и служебной тайне осуществляется с их согласия и предусматривает принятие сотрудниками обязательств по соблюдению установленного на предприятии режима соответствующего вида тайны, которые закрепляются в трудовом договоре (контракте) или специальном соглашении:

- ознакомление сотрудников с положениями законодательства, предусматривающими ответственность за нарушение конфиденциальности;
- ознакомление сотрудников с перечнями сведений, составляющих коммерческую и служебную тайну предприятия, и к которым сотрудники имеют право доступа [8, с. 51–52].

Вопросы для самоконтроля

1. Какими нормативными документами следует руководствоваться при определении должностей отдела конфиденциального делопроизводства?
2. Чем определяется численный состав сотрудников подразделения конфиденциального делопроизводства?
3. Каковы основные функции постоянно действующей экспертной комисси?
4. В каких документах в организации фиксируется допуск сотрудников предприятия к коммерческой и служебной тайне?

Список использованных источников и литературы

Источники

1. Укрупненные нормы времени на работы, выполняемые в объединенных архивах, хранящих документы по личному составу учреждений, организаций, предприятий (утв. Постановлением Минтруда РФ от 18 декабря 1992 г. № 57). URL: http://www.consultant.ru/document/cons_doc_LAW_90905/ (дата обращения: 30.12.2019).
2. Постановление Минтруда РФ от 10 сентября 1993 г. № 152 «Об утверждении Норм времени на работы по автоматизированной архивной технологии и документационному обеспечению органов управления». URL: http://www.consultant.ru/document/cons_doc_LAW_91031/ (дата обращения: 30.12.2019).
3. Постановление Министерства труда РФ от 25 ноября 1994 г. № 72 «Об утверждении Межотраслевых укрупненных нормативов времени на работы по документационному обеспечению управления». URL: http://www.consultant.ru/document/cons_doc_LAW_98813/ (дата обращения: 30.12.2019).
4. Постановление Госстандарта РФ от 26 декабря 1994 г. № 367 (ред. от 19 июня 2012 г.) «О принятии и введении в действие Общероссийского классификатора профессий рабочих, должностей служащих и тарифных разрядов ОК 016-94» (вместе с «ОК 016-94. Общероссийский классификатор профессий рабочих, должностей служащих и тарифных разрядов») (дата введения 01.01.1996). URL: http://www.consultant.ru/document/Cons_doc_LAW_58964/ (дата обращения: 30.12.2019).
5. Квалификационный справочник должностей руководителей, специалистов и других служащих (утв. Постановлением Минтруда России от 21 августа 1998 г. № 37) (ред. от 27 марта 2018 г.). URL: http://www.consultant.ru/document/cons_doc_LAW_58804/ (дата обращения: 30.12.2019).
6. Постановление Минтруда РФ от 26 марта 2002 г. № 23 «Об утверждении норм времени на работы по документационному обеспечению управленческих структур федеральных органов исполнительной власти». URL: http://www.consultant.ru/document/cons_doc_LAW_91156/ (дата обращения: 30.12.2019).
7. ГОСТ Р 7.0.8-2013. Национальный стандарт Российской Федерации. «Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения» (утв. Приказом Росстандарта от 17 октября 2013 г. № 1185-ст). URL: http://www.consultant.ru/document/cons_doc_LAW_163800/ (дата обращения: 15.07.2019).

Литература

8. Егоров В.П. Конфиденциальное делопроизводство [Электрон. ресурс]: учеб. пособие / В.П. Егоров, А.В. Слиньков. М.: Юридический институт МИИТа, 2015. 178 с. (pdf).
9. Куняев Н.Н. Конфиденциальное делопроизводство и защищенный электронный документооборот [Электрон. ресурс]: учебник / Н.Н. Куняев, А.С. Демушкин, А.Г. Фаб-

ричнов; под общ. ред. Н.Н. Куняева. М.: Логос, 2011. 452 с. (Новая университетская библиотека). (pdf).

10. Панкратьев В.В. Организация конфиденциального делопроизводства [Электрон. ресурс] // Техника для спецслужб [сайт]. [2007]. URL: http://www.bnti.ru/showart.asp?aid=808&lvl=04 (дата обращения: 14.10.2017).

11. Фирсова А.Ю. Модуль 8. Работа с конфиденциальными документами. Курс повышения квалификации/профессиональной переподготовки «Основы делопроизводства и секретарское дело» [Электрон. ресурс] // Академия подготовки главных специалистов [сайт]. [2019]. URL: https://specialitet.ru (дата обращения: 03.11.2019).

Глава 4
НОМЕНКЛАТУРА КОНФИДЕНЦИАЛЬНЫХ ДЕЛ И ОРГАНИЗАЦИЯ АРХИВНОГО ХРАНЕНИЯ КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ

4.1. Составление и ведение номенклатуры конфиденциальных дел

В соответствии с ГОСТ Р 7.0.8-2013 **номенклатура дел** – систематизированный перечень заголовков дел, создаваемых в организации, с указанием сроков их хранения.

Дело – документ или совокупность документов, относящихся к одному вопросу или участку деятельности, помещенных в отдельную обложку [3].

Номенклатура дел организации составляется на основе номенклатур дел структурных подразделений. После ее согласования с экспертной проверочной комиссией (ЭПК) утверждается руководителем организации не позднее конца текущего года и вводится в действие с 1 января следующего года. Один раз в 5 лет она согласовывается с Экспертно-проверочной комиссией федерального государственного архива, куда на постоянное хранение передаются образующиеся в процессе деятельности организации документы Архивного фонда Российской Федерации. В случае изменения функций и структуры организации номенклатура также подлежит согласованию с Экспертно-проверочной комиссией федерального государственного архива. Согласования проводятся при первоначальной разработке номенклатуры конфиденциальных дел и в случае ее значительной переработки (существенное изменение заголовков дел, включение большого количества новых дел, расширение списка лиц, допущенных к делам) [6, с. 174–177].

Номенклатура конфиденциальных дел разрабатывается постоянно действующей экспертной комиссией (ПДЭК). Так как в состав ПДЭК входят ответственные за делопроизводство и архивное хранение документов в организации лица, которые одновременно являются членами ЭПК, то номенклатура конфиденциальных дел может не представляться на проверку ЭПК в целях экономии времени.

Наименованиями разделов номенклатуры дел организации являются наименования структурных подразделений [6, с. 174].

Номенклатура конфиденциальных дел, определяя наименования (заголовки) дел и выступая тем самым в роли плана распределения исполненных документов по делам, одновременно устанавливает индексы и сроки хранения дел и является составной частью разрешительной системы доступа к конфиденциальной информации. Кроме того, номенклатура позволяет проверить наличие конфиденциальных дел и может быть использована в качестве схем построения справочной картотеки по конфиденциальным документам и со-

ставления описей дел постоянного и долговременного хранения (свыше 10 лет), передаваемых в архив организации [6, с. 176].

В случаях, когда образуется большое количество одних и тех же видов документов и дел (распоряжения, постановления, приказы, инструкции, отчеты, сводки и т. д.) с отметкой конфиденциальности и без этой отметки, но являющихся конфиденциальной документированной информацией, например, кадровая документация – персональные данные, целесообразно предусматривать их обособленное формирование в дела. При этом в графе номенклатуры дел «Индекс дела» к номеру дела добавляется отметка конфиденциальности [6, с. 177]. Например:

Индексы дел	*Заголовки дел*
01-1	Приказы по основной деятельности
01-1/ДСП	То же
08-98	Переписка об аренде помещений
08-98/КФД	То же

Если в деятельности структурного подразделения организации образуется небольшое количество конфиденциальной документированной информации, номенклатурой дел может быть предусмотрено заведение одного дела, которое именуется, например, «Материалы для служебного пользования» или «Конфиденциальные материалы». Срок хранения одного такого дела не устанавливается, а в соответствующей графе номенклатуры дел проставляется отметка ЭК (экспертная комиссия).

Номенклатура должна иметь соответствующую отметку конфиденциальности, издаваться в двух экземплярах и регистрироваться в журнале регистрации созданных/изданных внутренних конфиденциальных документов. Первый экземпляр номенклатуры хранится в службе делопроизводства и по окончании года подшивается в специальное дело, второй передается в качестве рабочего в архив организации.

После утверждения номенклатуры дел возможные в течение года изменения вносятся в нее руководителем службы делопроизводства (с проставлением подписи) на основании служебных записок руководителей структурных подразделений.

В номенклатуру не включаются документы, зарегистрированные по журналу инвентарного (выделенного) учета конфиденциальных документов [6, с. 178].

Таким образом, **номенклатурой конфиденциальных дел** можно считать оформленный в установленном порядке систематизированный перечень наименований дел, заводимых в организации, с указанием их индексов (номеров), сроков хранения и лиц, которым предоставлено право пользования этими делами [6, с. 176].

Форма номенклатуры конфиденциальных дел приведена в приложении (см. *Приложение 2*).

При значительном количестве дел целесообразно группировать их в номенклатуре по разделам, соответствующим наименованиям структурных подразделений или основным направлениям (вопросам) деятельности предприятия.

Каждому разделу присваивается номер, например:

02 – Плановый отдел (при структурной схеме);

14 – Финансирование (при производственно-отраслевой схеме) [7].

В графе 1 указываются индекс или номер дела и отметка конфиденциальности. Переходящие дела сохраняют одни и те же индексы (номера) на весь период ведения дела. Графа заполняется при составлении номенклатуры дел.

В графу 2 вносится заголовок дела. Переходящие дела сохраняют одни и те же заголовки до их закрытия. Графа заполняется при составлении номенклатуры дел. При закрытии дела заголовок может корректироваться, все изменения переносятся в номенклатуру дел [6, с. 181].

Полнота и сочетание в заголовках других компонентов могут быть различными. Указывать их следует тогда, когда они несут в себе необходимую информацию и без их наличия теряются индивидуальные особенности заголовка или возникает его двоякое понимание. При этом:

- в заголовках дел с планово-отчетной документацией указывается периодичность этой документации, например: «Месячные планы…», «Отчет о выполнении плана … за __г.»;
- если в деле объединяется переписка с несколькими однородными предприятиями, то в заголовке указывается их обобщенное название, например: «Переписка с приборостроительными заводами…»;
- в конце заголовков дел с копийными распорядительными документами пишется слово «копии».

При составлении заголовков дел необходимо предусматривать:

- группировку документов в дело по одному вопросу (за исключением распорядительных документов и протоколов);
- раздельную группировку документов постоянного, долговременного (свыше 10 лет) и временного (до 10 лет) сроков хранения;
- группировку документов с учетом распределения обязанностей между сотрудниками предприятия, что позволяет в значительной мере предотвращать ознакомление пользователей с документами, не имеющими к ним отношения по роду выполняемой работы;
- группировку распорядительных документов по видам документов (приказы, указания, постановления, распоряжения, решения);
- группировку приказов по предприятию по трем делам: по основной деятельности, личному составу (при наличии конфиденциальных приказов) и оперативным вопросам;
- группировку приказов по основной деятельности в два дела: с подлинниками и копиями;
- группировку документов коллегий и других коллегиальных органов в два дела: протоколы и решения; документы к заседаниям (повестка дня, доклады, справки, заключения, проекты решений и др.);
- группировку приложений к документам вместе с документами, к которым они относятся (исключение допускается для больших по объему приложений, для которых могут предусматриваться отдельные дела) [7].

В графе 3 перечисляются инициалы и фамилии всех лиц, которым предоставляется право пользования соответствующим делом. Состав лиц, допускаемых к каждому конкретному делу, должен определяться в соответствии с принципами и требованиями разрешительной системы доступа к конфиденциальной информации и регламента доступа к конфиденциальной информации и исключать необоснованный доступ пользователей к де-

лам. Графа заполняется при составлении номенклатуры дел. В течение года в список могут вноситься изменения.

В графах 4 и 5 арабскими цифрами проставляются номер каждого тома и дата его заведения. Графы заполняются в день подшивки первого документа тома дела (заполнения первой позиции журнала (карточки) учета и регистрации). Если дело переходящее, то в графе 5 при составлении номенклатуры указывается: «Переходящее с 20__ г.» с проставлением года заведения дела.

В графе 6 арабскими цифрами проставляется дата закрытия каждого тома. Графа заполняется в день закрытия тома. Если дело переходит на следующий год, то в графе указывается: «Переходит на 20__ г.».

В графе 7 указывается количество листов в томе (без учета листов описи документов дела). Графа заполняется при заведении журнала учета и при закрытии тома дела, картотеки.

Графы 4–7 заполняются по каждому тому отдельной строкой. Не допускается открывать очередной том до закрытия предыдущего.

В графе 8 проставляются срок хранения и номера статей (их может быть несколько) по определенному перечню документов со сроками хранения. Графа заполняется при составлении номенклатуры дел. При закрытии дела и проведении экспертизы ценности имеющихся документов срок хранения и номера статей могут корректироваться. Изменения должны быть перенесены в номенклатуру дел.

В графе 9 указываются архивный шифр дела (номера фонда, описи, единицы хранения), если дело передано в архив; номер и дата акта об уничтожении дела или, если дело направлено в другую организацию, наименование организации, номер и дата сопроводительного документа (письма, реестра, расписки, квитанции).

Если предусмотренное номенклатурой дело не было заведено, то по окончании года в графе 9 проставляется отметка: «Дело не заводилось» [6, с. 183–184].

Конфиденциальные документы в обычной номенклатуре дел

Данный способ систематизации и учета конфиденциальных документов вполне допустим, если их немного в составе документального фонда. Это могут быть, например:

- документы по личному составу, которые образуются в деятельности бухгалтерии (сведения о заработной плате, других выплатах) и
- документы отдела кадров (анкетные данные, имущественное положение, состав семьи, размер заработной платы, копии персональных документов, результаты психологических тестов, аттестации и другие сведения и документы, необходимые для формирования личного дела сотрудника), которым может быть присвоен гриф ограничения доступа – «Персональные данные».

В номенклатуре может быть одновременно несколько дел с одинаковым заголовком, но разными индексами под каждый имеющийся вариант доступа (в зависимости от грифа ограничения доступа).

Пример.

После снятия грифа ограничения доступа «Коммерческая тайна документы из дела № 06-17/кт перемещаются в аналогичное «открытое» дело с индексом № 06-17. Отметка «ЭК» в графе «Примечание» говорит о порядке снятия грифа – экспертной комиссией по защите конфиденциальной информации.

Если в дело с «обычными» документами включается несколько документов с грифом ограничения доступа, то всему делу присваивается соответствующий гриф ограничения доступа. Если степень ограничения доступа к включенным в дело документам разная, то делу присваивается максимальная из них.

Если конфиденциальных документов немного, то допускается их формирование в дела по видам тайны с обобщенными заголовками дел:

- «Документы для служебного пользования»;
- «Документы с грифом “Конфиденциально”» и т. п. по видам тайны.

Конкретный срок хранения таких конфиденциальных дел, включенных в обычную номенклатуру дел, не фиксируется. Вместо этого в графе «Срок хранения и номера статей по перечню» оформляется отметка «ЭК», свидетельствующая, что срок хранения документов дела установит экспертная комиссия по защите конфиденциальной информации [5].

4.2. Формирование конфиденциальных дел

Формирование дела – группировка исполненных документов в дело в соответствии с номенклатурой дел и их систематизация внутри дела [3].

Дела формируются в соответствии с номенклатурой дел, а также с соблюдением принципов систематизации документов и их распределения (группировки) на дела постоянного и долговременного (свыше 10 лет) хранения, в том числе дела по личному составу, и дела временного (до 10 лет включительно) хранения [6, с. 174].

В дела помещаются исполненные документы (подлинники или заверенные копии), оформленные в установленном порядке. Вторые экземпляры могут помещаться в дело лишь в случаях, когда на них имеются какие-либо резолюции, пометки, дополняющие содержание основного экземпляра. При необходимости допускается помещать в дела временного (до 10 лет) хранения проекты документов. В исключительных случаях с разрешения руководителя службы делопроизводства допускается помещать в конфиденциальные дела отдельные открытые документы, имеющие прямое отношение к содержанию конфиденциальных документов дела.

Перед помещением документа в дело сотрудник подразделения конфиденциального делопроизводства обязан проверить наличие отметки об исполнении, соответствие вида и содержания документа заголовку дела, наличие отметки о переводе приложения на учет конфиденциальных документов выделенного хранения, если оно не подшивается в дело. В дела не должны помещаться документы, подлежащие возврату. В деле группируются, как правило, документы одного календарного года [4].

В зависимости от вида и содержания документы систематизируются внутри дел в вопросно-логической или хронологической последовательности, а также их сочетании [6, с. 184].

Созданные/изданные распорядительные документы (приказы, протоколы, акты) систематизируются в делах хронологически в порядке возрастания номеров. В делах с перепиской поступившие (входящие) документы помещаются вместе с копиями отправленных (исходящих) документов, которыми они исполнены. Копии созданных инициативных документов, направляемых в другие учреждения, организации, предприятия, в целях обеспечения их сохранности подшиваются, как правило, в дело сразу, до получения на них ответов [6, с. 185].

4.3. Оформление конфиденциальных дел

Оформление дела – подготовка дела к передаче на архивное хранение [3].

Оформление конфиденциального дела включает описание дела на обложке, проставление на внутренней стороне обложки инициалов и фамилий лиц, допущенных к делу, заведение карточки учета выдачи дела, заполнение описи документов дела, нумерацию лис-

тов, составление заверительной надписи, прошивку и опечатывание дела. Форма обложки дела представлена в приложении (см. *Приложение 3*) [6, с. 187].

При заведении дела на обложке указываются (сверху вниз):

1. гриф конфиденциальности дела;
2. название предприятия;
3. название структурного подразделения (если в дело помещаются документы одного структурного подразделения);
4. индекс (номер) дела;
5. заголовок дела;
6. год заведения дела на обложках дел с планами и отчетами (вместо крайних дат документов в деле);
7. срок хранения и номера статей по перечню документов с указанием сроков хранения [4].

При закрытии дела на обложке проставляются крайние даты документов в деле, которые должны соответствовать датам создания/издания (подписания, утверждения) или поступления самого раннего и самого позднего документов, вне зависимости от расположения этих документов в деле. Расхождение между датами, указанными в номенклатуре дел и на обложках дел, обусловлено тем, что даты, проставляемые в номенклатуре, диктуются режимом конфиденциальности (в случае утраты дела для обеспечения его поиска необходимо знать, когда оно было заведено или когда закрыто), а даты, проставляемые на обложке, показывают, к какому периоду относятся документы, находящиеся в деле. Эти даты ускоряют поиск необходимых документов и переносятся в опись дел, подлежащих передаче на архивное хранение. На обложке также указывается количество листов (без листов описи документов дела) [6, с. 187–188].

Перед заведением каждого конфиденциального дела любого срока хранения в него подшивается приблизительно необходимое количество листов описи документов дела (табл. 17) [6, с. 188].

Таблица 17

Форма описи дела

№ п/п	Дата документа	Номер и отметка конфиденциальности поступившего документа	Номер и отметка конфиденциальности созданного/ изданного документа	Откуда поступил или куда адресован документ	№ листа дел	Отметка о местонахождении изъятого из дела документа
1	2	3	4	5	6	7

Данные о документах вносятся в опись в момент подшивки документов. При подшивке в конфиденциальные дела открытых документов в графах 3 или 4 производится отметка «н/к» – неконфиденциальный. Если в дело подшивается документ, имеющий приложения, в том числе открытые, то запись в графах 3 или 4 производится одной позицией за номером основного документа без отметок о наличии приложений, с проставлением в графе 6 номеров общего количества листов, включая листы приложений. Если документ внутренний, то в графе 5 указывается только его краткое содержание. В описи документов дел временного хранения при небольшом объеме справочной работы по документам графа 5 может не заполняться.

При заведении дела на внутреннюю сторону обложки дела переносятся из номенклатуры инициалы и фамилии лиц, которым предоставлено право пользования делом. Список заверяется подписью сотрудника службы делопроизводства. Это позволяет при определе-

нии правомерности выдачи дела пользователю не обращаться к номенклатуре дел. Одновременно заводится карточка учета выдачи дела [6, с. 188].

Форма карточки учета выдачи дела

КАРТОЧКА УЧЕТА ВЫДАЧИ ДЕЛА

_____

(индекс (номер) и гриф конфиденциальности дела, номер тома, заголовок дела)

Дата выдачи	Количество листов	Кому выдано	Подпись за получение	Подпись за возврат
1	2	3	4	5

Графа 2 необходима потому, что в процессе формирования дела меняется количество его листов [6, с. 188].

Карточка помещается в бумажный карман, приклеенный к внутренней стороне обложки дела. По заполнении одной карточки заводится следующая, а заполненная вносится в опись документов дела после последней записи. Карточки не нумеруются и листами дела не считаются. Карточки, заводимые после закрытия дела, также вносятся в опись документов дела. Необходимость сохранения всех карточек вызвана тем, что в случае разглашения конфиденциальной информации, содержащейся в документах дела, по карточкам можно установить, кто пользовался делом, и тем самым определить круг лиц, которые могли разгласить информацию [6, с. 190].

4.4. Экспертиза ценности конфиденциальных документов

Экспертиза ценности документов – изучение документов на основании критериев их ценности для определения сроков хранения документов.

Критерии экспертизы ценности документов – признаки, определяющие значимость происхождения, содержания и внешних особенностей документов [3].

Проведение такой экспертизы целесообразно возлагать на постоянно действующую экспертную комиссию организации.

Экспертиза ценности конфиденциальных документов проводится ежегодно или при небольшом объеме документов один раз в несколько лет, однако подвергать экспертизе целесообразно документы, изданные 3–5 лет назад, когда одновременно с подготовкой документов для архивного хранения возможны отбор их для уничтожения (значительное количество документов имеет срок хранения 3–5 лет) и снятие отметки конфиденциальности с существенной части документов.

Экспертиза ценности документов дела проводится путем изучения содержания каждого подшитого в дело вида документа и установления его соответствия сроку хранения и номерам статей Перечня документов со сроками хранения, указанными на обложке дела. Одновременно проверяется правильность формирования дела: соответствие видов и содержания документов заголовку дела, отсутствие в делах постоянного срока хранения документов временного срока хранения, а также определяется возможность снятия отметки конфиденциальности с отдельных документов или с дела в целом [6, с. 195].

Нормативным актом, регламентирующим хранение и отбор на хранение, а также уничтожение типовых документов, служит Перечень типовых управленческих докумен-

тов, образующихся в деятельности организаций, с указанием сроков хранения, утвержденный руководителем Росархива от 26 августа 2010 г. № 63 [1].

4.5. Подготовка конфиденциальных документов и дел для архивного хранения

Хранение документов – организация рационального размещения и обеспечение сохранности документов [3].

Согласно протоколу заседания ПДЭК производится частичное переформирование и дооформление соответствующих дел и документов, в том числе:

- изъятие из дел документов, подлежащих перешивке в другие дела, и подшивка их в эти дела с проставлением в описях документов дел, из которых изъяты документы, их нового местонахождения и помещением в дела справок-заместителей, а также с перенумерацией листов, перешитых документов в делах, в которые они помещены, внесением их в описи документов дел и исправлением количества листов в заверительной надписи дел, на обложках дел и в номенклатуре дел;
- изъятие из дел документов, подлежащих уничтожению;
- зачеркивание отметки конфиденциальности с проставлением даты и номера протокола заседания ПДЭК, подписи на документах, подшитых в дела, обложках дел и документов, подлежащих снятию ограничения доступа (в описях документов дела, номенклатуре дел и журнале учета документов выделенного хранения отметка конфиденциальности зачеркивается без ссылки на протокол заседания ПДЭК);
- изъятие из дел (по решению ПДЭК) документов, с которых снята отметка конфиденциальности с отметкой в описях документов дел и помещением в дела справок-заместителей;
- передача снятых с ограничения доступа дел и документов выделенного хранения по акту в службу делопроизводства с отметкой в графе 9 номенклатуры дел;
- корректировка заголовков, сроков хранения и номеров статей по перечням отраслевых, ведомственных документов со сроками хранения, на обложках дел и в номенклатуре дел;
- проставление сроков хранения и номеров статей Перечня типовых управленческих документов, образующихся в деятельности организаций, с указанием сроков хранения на обложках дел.

На дела и документы инвентарного (выделенного) хранения, которые отобраны для постоянного хранения, составляется опись по установленной форме (см. *Приложение 4*) [6, с. 198].

На дела и документы долговременного хранения (свыше 10 лет) составляется аналогичная опись с добавлением перед графой «Примечание» графы «Срок хранения и номера статей по Перечню». На научно-техническую, проектную, конструкторскую и иную специальную документацию составляются отдельные описи документов [6, с. 200].

4.6. Хранение и правила выдачи конфиденциальных документов

Дела до передачи в архив организации или на уничтожение хранятся в структурных подразделениях по месту их формирования. Дела выдаются во временное пользование сотрудникам структурных подразделений на срок, определяемый руководителем организации. После истечения этого срока они подлежат возврату.

Выдача дел другим организациям производится на основании их письменных запросов с разрешения руководителя организации или его заместителя, курирующего вопросы делопроизводства.

Изъятие документов из дел постоянного хранения допускается в исключительных случаях с разрешения руководителя организации. При этом в деле оставляется копия документа, заверенная в установленном порядке, и акт о причинах выдачи подлинника [6, с. 174].

Вместо изъятых документов в дело помещается справка-заместитель следующей формы [6, с. 185].

СПРАВКА-ЗАМЕСТИТЕЛЬ

Документ № _____ от_____ на _____л. из дела изъят и ____

_____

(указывается новое местонахождение документа: при подшивке в другое дело – индекс дела, номера тома и листов; при отправлении – куда направлен, постоянно или временно, наименование, номер и дата сопроводительного документа; при уничтожении – номер и дата акта об уничтожении)

Основание: _____

(подпись, инициалы, фамилия лица, производившего изъятие, дата)

О документах, изъятых из дела безвозвратно, делается соответствующая отметка в описи документов дела (см. форму в разд. 4.4). При необходимости вместо изъятых документов в дело могут быть подшиты их копии. В этом случае справка-заместитель не требуется. Отметки о снятии копий и местонахождении подлинников производятся в соответствующих регистрационных и учетных формах [6, с. 186].

4.7. Подготовка конфиденциальных документов и дел к уничтожению

Уничтожение документов – исключение документов из документального или архивного фонда по истечении срока их хранения с последующим уничтожением (утилизацией) в установленном порядке [3].

Уничтожение конфиденциальных документов и дел организуется службой конфиденциального делопроизводства, если таковая имеется, либо службой делопроизводства.

После утверждения описей дел и конфиденциальных документов постоянного срока хранения составляется акт по тем делам и конфиденциальным документам за соответствующий период, которые подлежат уничтожению. В акт включаются дела, отдельные документы из дел и документы инвентарного (выделенного) хранения, отобранные экспертной комиссией. Форма акта содержится в приложении № 21 к «Правилам организации хранения, комплектования, учета и использования документов Архивного фонда Российской Федерации и других архивных документов в органах государственной власти, органах местного самоуправления и организациях» от 31 марта 2015 г. № 526 (см. *Приложение 5*) [2].

У отдельных категорий документов есть своя специфика уничтожения. Так, бухгалтерские документы не могут быть уничтожены до проведения ревизии по ним. Факт уничтожения черновика конфиденциального документа и других материалов данной группы подтверждается пометкой на копии документа, оставшейся в деле службы делопроизводства: «Черновик уничтожен. Дата. Подпись» [6, с. 210].

При уничтожении конфиденциальных материалов должен быть установлен порядок, исключающий возможность ознакомления с ними посторонних лиц.

Неполное уничтожение документов позволяет восстановить их текст и исключает возможность уничтожения материалов, не подлежащих включению в эту категорию. В ходе уничтожения подобных материалов угрозы их безопасности реализуются за счет:

- подмены документов, выделенных для уничтожения или изъятия из документов и дел отдельных частей (листов, фотографий, образцов печатей, росписей);
- ошибочного или умышленного выделения документов для уничтожения или фиктивное «уничтожение» ценных документов и дел;
- неполного уничтожения документов, дел и носителей, дающего возможность восстановить их текст;
- утраты (утери, кражи) документов и дел, выделенных для уничтожения.

Перечисленные факторы возникновения угроз могут стать контролируемыми, если соблюдаются следующие условия уничтожения документов, дел и носителей информации:

- коллегиальность принятия решения об уничтожении документов, дел и самого процесса уничтожения;
- документирование (актирование) подготовки к уничтожению и уничтожение документов и дел;
- внесение комиссией отметок об уничтожении в акт и учетные формы только после фактического уничтожения документов и дел.

С оформлением акта уничтожаются любые электронные документы, описи и учетные формы, находящиеся как в рабочем или архивном массивах компьютера, так и на магнитных носителях, хранимых вне ЭВМ.

Подписывать акт и вносить отметки об уничтожении в учетные формы до фактического уничтожения конфиденциальных материалов не допускается.

Бумажные документы уничтожаются путем сожжения, дробления, превращения в бесформенную массу. Магнитные и фотографические носители уничтожаются сожжением, дроблением, расплавлением и другими способами, исключающими возможность их восстановления.

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

При уничтожении использованного спецблокнота в контрольном листе проверяются наличие отметок и подписей о номерах документов или об уничтожении испорченных листов, обложка спецблокнота с корешками изъятых листов и с испорченными листами, если они не были уничтожены ранее, а в графе 9 журнала учета носителей пишется слово или проставляется штамп «Уничтожен», заверяемый подписью сотрудника службы делопроизводства с указанием даты [6, с. 88].

Уничтожение, как правило, должно производиться по окончании квартала после проведения проверки наличия конфиденциальных документов за истекший квартал, что позволяет в случае недостачи каких-либо документов проверить содержимое урны на предмет случайного помещения в нее недостающих документов [5, с. 78].

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

Форма акта об уничтожении бумажных носителей

Наименование организации

АКТ
_____ № _____
об уничтожении макулатуры

УТВЕРЖДАЮ
Руководитель организации
_____
Подпись Расшифровка подписи

Дата

_____

(должности, инициалы, фамилии сотрудников службы делопроизводства)

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

Наименование должности	**Подпись**	**Расшифровка подписи**
Наименование должности	**Подпись**	**Расшифровка подписи**

Бумажные носители могут уничтожаться и с помощью бумагорезательной машины, как правило, также после проведения квартальной проверки наличия документов. При уничтожении таким способом тоже может составляться акт об уничтожении с заменой в тексте слова «Сжигание» на слова «Измельчение машиной» [6, с. 89].

Участие в подготовке к уничтожению документов, дел и носителей информации включает следующие процедуры.

Схема 5. Последовательность и характеристика процедур подготовки к уничтожению документов, дел и носителей информации

Без составления акта уничтожаются испорченные бумажные и технические носители, черновики и проекты документов, внутренние описи документов, находящихся у исполнителя, и другие материалы, образовавшиеся при исполнении конфиденциальных документов.

В *Приложении 6* приведены примеры величины бумажных обрезков, полученных при применении различных вариантов измельчения документов в зависимости от степени конфиденциальности, которые предлагаются специальными фирмами, занимающимися списанием, уничтожением и утилизацией документов [8].

Вопросы для самоконтроля

1. Какие задачи выполняет номенклатура конфиденциальных дел?
2. Когда и при каких изменениях проводится согласование номенклатуры конфиденциальных дел с Экспертно-проверочной комиссией федерального государственного архива?
3. Когда в номенклатуре конфиденциальных дел проводится корректировка номеров статей по перечню документов со сроками хранения?
4. Сведения какого документа позволяют установить, кто пользовался делом, и тем самым определить круг лиц, которые могли разгласить информацию?
5. Какой документ помещается в дело вместо изъятых документов?
6. Чем отличается обложка конфиденциального дела от дела с документами с открытым доступом?
7. Назовите методы уничтожения различных видов носителей информации?
8. Какие документы можно уничтожить без составления акта?
9. В чем отличие формы описи дела конфиденциальных документов от описи дела документов открытого доступа?
10. Возможно ли совместное архивное хранение конфиденциальных дел и дел открытого доступа в одном помещении?
11. Можно ли оставлять на столе конфиденциальные документы после рабочего дня или отлучаясь в другой кабинет?

Список использованных источников и литературы

Источники

1. Перечень типовых управленческих документов, образующихся в деятельности организаций, с указанием сроков хранения, утвержденный руководителем Росархива от 26 августа 2010 г. № 63. URL: http://www.consultant.ru/document/cons_doc_LAW_104953/ (дата обращения: 13.01.2020).

2. Правила организации хранения, комплектования, учета и использования документов Архивного фонда Российской Федерации и других архивных документов в органах государственной власти, органах местного самоуправления и организациях от 31 марта 2015 г. № 526. URL: http://www.consultant.ru/document/cons_doc_LAW_185738/ (дата обращения: 16.01.2020).

3. ГОСТ Р 7.0.8-2013. Национальный стандарт Российской Федерации. «Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения» (утв. Приказом Росстандарта от 17 октября 2013 г. № 1185-ст). URL: http://www.consultant.ru/document/cons_doc_LAW_163800/ (дата обращения: 15.07.2019).

Литература

4. Алексенцев А.И. Конфиденциальное делопроизводство // Управление персоналом. [Электрон. ресурс]. М., 2003. 200 с. (pdf).

5. Иритикова В. Конфиденциальные документы в номенклатуре дел [Электрон. ресурс] // Делопресс [сайт]. [2014]. URL: http://www.delo-press.ru/articles.php?n=17357 (дата обращения: 06.01.2020).

6. Куняев Н.Н. Конфиденциальное делопроизводство и защищенный электронный документооборот [Электрон. ресурс]: учебник / Н.Н. Куняев, А.С. Демушкин, А.Г. Фабричнов; под общ. ред. Н.Н. Куняева. М.: Логос, 2011. 452 с. (Новая университетская библиотека). (pdf).

7. Стенюков М.В. Документы. Делопроизводство. М.: Приор-издат, 2010. 9-е изд., перераб. и доп. 160 с.

8. Утилизация документов [Электрон. ресурс]: Списание, уничтожение и утилизация документов // Уральская казна [сайт]. [2013]. URL: http://ural-kazna.ru/?yclid=18365138943844847826 (дата обращения: 16.01.2020).

Глава 5
РАЗРЕШИТЕЛЬНАЯ СИСТЕМА ДОСТУПА И МЕТОДЫ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В ОРГАНИЗАЦИЯХ

5.1. Разрешительная система доступа к конфиденциальной информации

Ключевым звеном в защите конфиденциальной информации, в том числе информации, циркулирующей в системах конфиденциального электронного документооборота, является организация санкционированного (разрешенного) доступа к ней [7, с. 141].

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

- на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
- на соблюдение конфиденциальности информации ограниченного доступа;
- на реализацию права на доступ к информации [2].

Доступ к информации – это возможность получения информации и ее использования [2].

Доступ к конфиденциальной информации – это санкционированное полномочным должностным лицом ознакомление с данной информацией, ее получение и использование конкретным физическим или юридическим лицом.

Допуск к конфиденциальной информации – это процедура оформления права граждан на доступ к такой информации, а для организаций, предприятий, учреждений – права на проведение работ с использованием такой информации [7, с. 141].

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

- надежность – исключение возможности несанкционированного доступа посторонних лиц к конфиденциальной информации в обычных и экстремальных условиях (чрезвычайные ситуации, пожары, наводнения и др.);
- полнота охвата всех категорий исполнителей и всех категорий конфиденциальной информации;
- конкретность и однозначность решения о доступе (да/нет);
- производственная и служебная необходимость – единственный критерий доступа к конфиденциальной информации;

- определенность состава должностных лиц, дающих санкцию на доступ к конфиденциальной информации, исключение возможности бесконтрольной и несанкционированной выдачи таких санкций;
- регламентация и организация работы всех категорий персонала с конфиденциальной информацией;
- соответствие функциональных обязанностей работника передаваемой ему конфиденциальной документированной информации;
- наличие нормативно-методических документов и положений по защите и охране конфиденциальной информации, режиму конфиденциальности информации и доступа к ней, в том числе утвержденного перечня конфиденциальной документированной информации, реестра конфиденциальной информации автоматизированной информационной системы;
- наличие необходимых условий в зданиях, помещениях, кабинетах для работы с конфиденциальной документированной информацией;
- оформление разрешения на ознакомление с конфиденциальной информацией;
- ознакомление пользователя, при необходимости, только с частью конфиденциального документа, при этом в разрешении на ознакомление должны быть указаны разделы, пункты или страницы, с которыми можно знакомить пользователя, если конфиденциальная документированная информация находится на бумажном носителе [7, с. 143].

Регламент доступа к конфиденциальной информации (далее – Регламент) или Положение о режиме конфиденциальности информации разрабатывается экспертной комиссией по защите конфиденциальной информации и содержит следующие разделы.

1. Общие положения. В этом разделе указываются:

- цель разработки Регламента;
- основные задачи и принципы системы допуска и доступа;
- нормативные документы, на которых базируется Регламент организации, а также лица, на которых возлагается ответственность за невыполнение его требований;
- руководство организации, руководители службы безопасности, службы делопроизводства, структурных подразделений, осуществляющих контроль за соблюдением норм Регламента в пределах их компетенции [7, с. 143].

2. Круг лиц, имеющих право давать разрешение на допуск и доступ к конфиденциальной информации. В данном разделе должны быть перечислены все должности лиц, которые могут давать разрешение на доступ к конфиденциальной информации, с указанием категории пользователей, состава информации и ее носителей. Право давать разрешение на доступ к соответствующей конфиденциальной информации имеют:

- руководитель организации – всем категориям пользователей;
- заместители руководителя по отдельным направлениям – всем пользователям, но в пределах своей сферы деятельности;
- руководители структурных подразделений – всем сотрудникам подразделений.

3. Порядок оформления разрешений на доступ к конфиденциальной информации и предоставление ее пользователям. В данном разделе определяется порядок оформления разрешений на доступ к различным носителям конфиденциальной информации и выдачи носителей пользователям. Разрешение на ознакомление должно оформляться: по поступившим и созданным/изданным документам – в форме резолюции на конфиденциальном документе; по документам, зарегистрированным по учету инвентарного (выделенного) хранения, – в форме резолюции на документе или подписанного соответствующими руководителями списка пользователей на внутренней стороне обложки документа, титульном листе либо в карточке учета выдачи конфиденциального документа. При этом следует оговорить, что исполнители и лица, которые визировали, согласовывали, подписывали и утверждали конфиденциальные документы, допускаются к соответствую-

щей конфиденциальной информации, в том числе циркулирующей в АИС, без оформления дополнительных разрешений, если они продолжают выполнять те же функциональные обязанности. Без специального разрешения могут допускаться также лица, указанные в тексте распорядительных документов организации (приказов, распоряжений) [7, с. 144].

4. Порядок учета работников и должностных лиц организации, а также работников должностных лиц других организаций, получивших доступ к конфиденциальной информации.

5. Порядок учета выдачи конфиденциальной документированной информации.

Регламент подписывается членами экспертной комиссии по защите конфиденциальной информации, визируется всеми лицами, имеющими право давать разрешение на доступ, и вводится в действие приказом руководителя организации. В приказе определяются также и мероприятия по введению Регламента в действие (порядок изучения Регламента пользователями, технология осуществления контроля за его выполнением и др.). После утверждения с Регламентом должны быть ознакомлены под расписку все сотрудники и работники организации, работающие с конфиденциальной информацией [7, с. 145].

5.2. Особенности доступа к конфиденциальной документированной информации, составляющей служебную, коммерческую, профессиональную тайны, секрет производства (ноу-хау) и служебный секрет производства

Доступ к информации, составляющей коммерческую тайну, – это ознакомление определенных лиц с информацией, составляющей коммерческую тайну, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации [1].

Существуют три вида договоров, регулирующих ограничение доступа к секрету производства и служебному секрету производства:

- договор об отчуждении исключительного права на секрет производства;
- лицензионный договор о предоставлении права использования секрета производства;
- секрет производства, полученный при выполнении работ по договору подряда [6, с. 148].

Контрагент – это сторона гражданско-правового договора, которой обладатель информации, составляющей коммерческую тайну, передал эту информацию.

Разглашение информации, составляющей коммерческую тайну, – это действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору [1].

В договорах должны быть определены условия защиты и охраны конфиденциальности информации и доступа к ней, в том числе в случае реорганизации или ликвидации одной из сторон договора в соответствии с гражданским законодательством, а также обязан-

ность контрагента по возмещению убытков при разглашении им этой информации вопреки договорам, в соответствии со следующим типовым текстом пункта договора [7, с. 149].

Контрагент – это сторона гражданско-правового договора, которой обладатель информации, составляющей коммерческую тайну, передал эту информацию.

Разглашение информации, составляющей коммерческую тайну, – это действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору [1].

Пункт договора (государственного контракта) о неразглашении информации

Контрагент (лицензиат) обязан:

- не разглашать конфиденциальную информацию организации, которая будет доверена или станет известной по условиям договора;
- не передавать третьим лицам и не раскрывать публично конфиденциальную информацию организации без ее согласия;
- выполнять по договору требования инструкций и положений по обеспечению сохранности конфиденциальной информации организации и доступу к ней;
- сохранять конфиденциальную информацию тех организаций, с которыми у организации имеются служебные и деловые отношения;
- не использовать знание конфиденциальной информации организации для занятий любой деятельностью, которая может нанести ей ущерб;
- в случае расторжения договора все носители конфиденциальной информации организации (рукописи, черновики, чертежи, магнитные ленты, диски, дискеты, распечатки на принтерах, кино-, фотонегативы и позитивы, модели, материалы, изделия и др.), которые находились в распоряжении в связи с выполнением договорных обязанностей, передать организации;
- незамедлительно сообщить организации о допущенном контрагентом либо ставшем ему известным факте разглашения или угрозы разглашения, незаконном получении или незаконном использовании конфиденциальной информации третьими лицами, об утрате или недостаче носителей конфиденциальной информации и о других фактах, которые могут привести к разглашению конфиденциальной информации организации, а также о причинах и условиях возможной утечки информации [7, с. 149].

Передача информации, составляющей коммерческую тайну, – это передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем контрагенту на основании договора в объеме и на условиях, которые предусмотрены договором, включая условие о принятии контрагентом установленных договором мер по охране ее конфиденциальности [1].

В целях охраны конфиденциальности информации организации работодатель (обладатель конфиденциальной информации) должен:

- ознакомить под расписку работника, доступ которого к конфиденциальной информации необходим для выполнения им своих трудовых обязанностей, с перечнем конфиденциальной документированной информации организации;
- ознакомить под расписку работника с установленным режимом конфиденциальности информации и с мерами ответственности за его нарушение в соответствии с Регламентом доступа к информации по типовой форме (см. *Приложение 7*) [7, с. 150].

Основными требованиями доступа к конфиденциальной информации являются:

- наличие приказа о приеме на работу, переводе, временном замещении, изменении должностных обязанностей и другом или назначении на должность, которая предусматривает работу с конфиденциальной информацией;
- наличие подписанного сторонами трудового договора (служебного контракта для государственных служащих), имеющего пункт о неразглашении конфиденциальной информации, составляющей какую-либо тайну организации, например, секрет производства, кроме государственной тайны, или подписанного обязательства о неразглашении информации и обеспечении защиты и охраны конфиденциальности информации, обладателем которой являются организация и ее контрагенты [7, с. 152–153].

5.3. Обработка персональных данных на предприятии

Многие юридические лица и индивидуальные предприниматели в ходе осуществления своей деятельности работают с физическими лицами. При предоставлении различных документов физические лица сообщают свои персональные данные (ПД), такие как фамилия, имя, отчество, дата рождения и др. Эти сведения в соответствии с законодательством РФ подлежат особому режиму хранения и обращения с ними.

Обработка ПД представляет собой действия с ПД, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение. Федеральным законом № 152-ФЗ «О персональных данных» устанавливаются принципы обработки ПД.

Хранение ПД должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении [12, с. 25].

Правительство РФ постановлением от 01 ноября 2012 г. № 1119 утвердило Требования к защите персональных данных при их обработке в информационных системах персональных данных. При обработке персональных данных в информационных системах устанавливаются 4 уровня защищенности персональных данных. В требованиях подробно описываются условия обеспечения защиты информации для каждого из указанных уровней защищенности [4].

К документам, содержащим персональные данные работника, относятся:

- анкета, которую соискатель заполняет при приеме на работу;
- копия паспорта;
- копии свидетельств о заключении брака, рождении детей;
- документы воинского учета;
- справка о доходах и суммах налога физлица с предыдущего места работы;
- документы об образовании и квалификации сотрудника;
- СНИЛС;
- трудовой договор;
- приказ о приеме на работу;
- приказы об изменении условий труда;

- приказ о прекращении трудового договора;
- приказы о поощрениях и дисциплинарных взысканиях, применяемых к работнику;
- трудовая книжка.

Более того, к персональным данным работника относится информация медицинского характера. Все персональные данные работника работодатель может получать только от него самого. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом и от него должно быть получено письменное согласие (см. *Приложение 8*) [8, с. 81]. Согласие действует со дня его подписания до дня отзыва в письменной форме [11].

5.4. Режим хранения конфиденциальных документов

Хранение конфиденциальных документов требует особого режима, так как информация, содержащаяся в данных документах, является объектом защиты. Специальный режим хранения конфиденциальных документов предусматривает обязательное соблюдение следующих правил.

- Помещение, где хранятся конфиденциальные документы, не должно находиться на первом или последнем этажах здания, потому что данные этажи потенциально наиболее доступны для проникновения.
- Вход в помещение разрешается только лицам, имеющим доступ к работе с документами.
- Уборка помещений, ремонт находящегося в них оборудования и технических средств, связанных с привлечением лиц, не имеющих доступа к хранящимся в помещении документам, должны проходить только в присутствии сотрудников службы защиты информации.
- Входные двери помещений должны быть обиты металлом и оборудованы надежными замками.
- По окончании рабочего дня двери не только закрываются, но и опечатываются печатью службы защиты информации. Печать проставляется на тонкий слой пластилина или специальной мастики таким образом, чтобы оттиск невозможно было снять и восстановить.
- Перед открытием двери в начале рабочего дня проверяется сохранность оттиска печати и целостность запоров. При обнаружении попыток проникновения в помещение необходимо немедленно поставить в известность службу безопасности и доложить первому руководителю. До принятия решения первым руководителем помещение не открывается и обеспечивается физической охраной.
- Для предотвращения несанкционированного входа в помещение в течение рабочего дня на двери устанавливаются электромеханические или электронные замки.
- Входные двери, окна, сейфы, шкафы, стеллажи следует оснастить охранной сигнализацией.
- Ключи от сейфов, шкафов, стеллажей, решеток, дверей в нерабочее время должны храниться в опечатанном пенале (конверте) в службе безопасности или в бюро контроля защиты информации. Факт передачи ключа регистрируется в специальном журнале приема-передачи помещений и ключей под охрану (табл. 18) [9].

Все сейфы, шкафы и стеллажи, установленные в помещениях службы делопроизводства и в служебных комнатах исполнителей, в которых круглосуточно или в рабочее время хранятся конфиденциальные документы, а также ключи от них должны учитываться службой охраны по журналу учета хранилищ и ключей от них (табл. 19) [7, с. 219].

Таблица 18

Форма журнала приема-передачи помещений и ключей под охрану

№ помещения, передаваемого под охрану	№ печатей, которыми опечатаны помещения и пеналы с ключами	Дата и время передачи под охрану	Подпись и фамилия лица, передавшего помещения и ключи под охрану
1	2	3	4

Окончание

Отметка о включении сигнализации	Подпись и фамилия лица, принявшего объекты под охрану	Дата и время получения пеналов	Подпись и фамилия лица, получившего пеналы	Отметка о выключении сигнализации
5	6	7	8	9

Таблица 19

Форма журнала учета хранилищ и ключей от них

№ п/п	Наименование хранилища (сейф, металлический шкаф, металлический стеллаж)	Инвентарный номер хранилища	Местонахождение хранилища (подразделение, номер комнаты)
1	2	3	4

Окончание

Инициалы и фамилия ответственного за хранилище	Количество экземпляров ключей и их номера	Подпись ответственного за хранилище, за получение ключей, дата	Подпись сотрудника	Службы охраны за прием ключей
5	6	7	8	9

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

При командировании работников в другие организации-контрагенты для проведения совместных работ им выдаются справки, удостоверяющие наличие у них доступа к конфиденциальной информации другой организации (далее – справка).

Справка выдается службой безопасности организации, в которой работает командированный, под расписку командированного в журнале (карточке) учета выдачи справок о доступе на срок разовой командировки или на срок выполнения задания, но не более чем на год. Справка подписывается руководителем службы безопасности или службы кадров и заверяется печатью организации. Делать в справке отметки, содержащие конфиденциальную информацию, запрещается.

На обороте справки о допуске указываются степень конфиденциальности информации, с которой ознакомилось командированное лицо, и дата. Запись заверяется подписью руководителя службы безопасности организации или службы кадров, куда было командировано должностное лицо, и печатью организации.

Справка возвращается ее владельцу для сдачи в службу безопасности или службу кадров по месту его постоянной работы, после чего уничтожается, о чем делается отметка в журнале (карточке), которая заверяется подписями двух сотрудников службы безопасности. При этом акт на уничтожение не оформляется [7, с. 166].

Кроме справки, командировочному выдается предписание на выполнение задания. Предписание – это документ на выполнение задания, связанного с информацией конфиденциального характера, который подписывается руководителем организации или структурного подразделения организации и заверяется печатью организации.

В предписании кратко излагается основание командирования (номер и дата приказа, договора, совместный план научно-исследовательских и опытно-конструкторских работ и т. д.), а также определяется, с какой информацией необходимо ознакомить командируемое лицо для выполнения им задания.

Предписание, в котором содержится информация всех степеней конфиденциальности («Конфиденциально», «Совершенно конфиденциально»), пересылается почтой в порядке, установленном для конфиденциальных документов. Предписание выдается для посещения только одной организации. Командированное лицо может иметь доступ только к той информации, которая ему необходима в рамках выполняемого задания, указанного в предписании.

Доступ для ознакомления с данной информацией осуществляется с письменного разрешения руководителя принимающей организации или структурного подразделения.

Предписание на выполнение задания с разрешением руководителя принимающей организации ознакомить командированное лицо с конфиденциальной информацией вместе со справками о допуске регистрируется в журнале (картотеке) учета командированных.

Предписание с визой соответствующего руководителя подразделения и отметкой о доступе командированного лица передается принимающим его должностным лицам. Те, в свою очередь, производят на обороте предписания отметки о степени конфиденциальности информации, с которой фактически ознакомилось командированное лицо. Отметки подтверждаются подписью командированного лица, после чего один экземпляр предписания передается для хранения в службу безопасности организации, а также другой организации, в которую прибыл командированный.

Предписание хранится в специальном деле в службе безопасности или службе кадров организации, а также в принимающей организации в течение не менее 5 лет.

Доступ к конфиденциальной информации командируемых работников и должностных лиц в принимающей организации осуществляется после предъявления ими документов, удостоверяющих личность, справок о доступе, предписаний на выполнение заданий [7, с. 167].

5.6. Учет персонала, получившего доступ к конфиденциальной документированной информации, и/или лиц, которым она была передана или предоставлена

Технологии ограничения доступа предполагают создание в организации номенклатуры должностей работников, подлежащих оформлению на допуск к конфиденциальной документированной информации по форме, представленной в приложении (см. *Приложение 9*) [7, с. 168].

Номенклатура должностей работников, подлежащих оформлению на допуск к конфиденциальной документированной информации, составляется службой безопасности совместно со службой кадров, согласовывается с экспертной комиссией по защите конфиденциальной информации и подписывается руководителем организации. Номенклатура хранится в службе безопасности, второй экземпляр – в службе кадров организации, третий – в службе делопроизводства.

Технология доступа к конфиденциальной информации также включает учет должностных лиц других организаций, получивших доступ, и/или лиц, которым такая информация была предоставлена или передана. Учет производится по следующей форме. Журнал (картотека) может вестись в автоматизированном режиме.

ЖУРНАЛ (КАРТОТЕКА)

учета работников, включая работников других организаций, получающих в пользование конфиденциальную документированную информацию

Дата выдачи документа	Номер записи	Наименование документа	Номер и дата документа	Наименование структурного подразделения или иной организации	Должность, фамилия, имя, отчество
1	2	3	4	5	6

Окончание

Цель получения	Основание получения	Расписка в получении	Дата возврата	Подтверждение возврата (подпись лица, ответственного за выдачу документов)	Примечание
7	8	9	10	11	12

При обнаружении факта утраты конфиденциальной документированной информации или факта разглашения информации должно вводиться ограничение на доступ или прекращение доступа к любой информации до окончания служебного расследования, которое оформляется актом по следующей типовой форме, представленной в приложении (см. *Приложение 10*) [7, с. 170–171].

5.7. Режим обмена конфиденциальной документированной информацией

Если сотрудники работают с конфиденциальными документами в своих служебных кабинетах, то документы (кроме дел) разрешается выдавать им как на один рабочий день, так и на все время, необходимое для работы с ними. В последних случаях, помимо сейфа и номерной печати, сотруднику выдаются под подпись в лицевом счете специальный портфель (кейс), имеющий устройство для опечатывания, и типовая форма «Опись конфиденциальных документов, находящихся у исполнителя». В опись сотрудник должен вносить каждый документ в момент его получения и вычеркивать его после исполнения и передачи в службу делопроизводства. Опись предназначена для проведения самоконтроля за наличием конфиденциальных документов (табл. 20) [7, с. 211].

Таблица 20

Форма описи конфиденциальных документов, находящихся у исполнителя

№ п/п	Номер и отметка конфиденциальности				Количество листов
	созданного (изданного) документа	поступившего документа	инвентарного (выделенного) хранения	носителя	
1	2	3	4	5	6

Сотрудникам, работающим с конфиденциальной документированной информацией, запрещается (это должно быть отражено в разделе инструкции по конфиденциальному делопроизводству):

- использовать конфиденциальные сведения в публикациях, открытых документах, докладах и переписке, рекламных материалах, выставочных проспектах и информационных сообщениях;

- передавать кому-либо, в том числе работникам организации, устно или письменно конфиденциальную информацию, документы, если это не связано со служебной необходимостью и не разрешено непосредственным руководителем;
- вести переговоры, содержащие конфиденциальные данные, по незащищенным линиям связи, в неприспособленных помещениях, в присутствии посторонних лиц;
- снимать копии с документов и делать из них выписки без письменного разрешения непосредственного руководителя;
- знакомиться с конфиденциальными документами, делами и базами данных других сотрудников, работать за их компьютерами;
- переписывать сведения из документов в личные записные книжки, дневники, календари, карточки учета работы;
- вносить в помещения организации личные фото-, видеокамеры, компьютеры (ноутбуки), аудиотехнику, магнитофоны, плееры, переговорные устройства, технические носители информации (дискеты и др.), мобильные телефоны, копировальные аппараты и пользоваться ими;
- выносить конфиденциальные документы из здания без разрешения руководства организации, работать с конфиденциальной документированной информацией в непредназначенных для этого помещениях;
- оставлять конфиденциальные документы на рабочем столе без контроля, хранить эти документы вместе с открытыми документами и материалами, оставлять без контроля компьютер с загруженной конфиденциальной информацией;
- разглашать сведения о характере автоматизированной обработки конфиденциальной информации на компьютере в АИС и о личных идентифицирующих паролях;
- разглашать сведения о составе находящейся у сотрудника конфиденциальной документированной информации, системе ее защиты и месте хранения, а также об известных ему элементах обеспечения информационной безопасности организации [7, с. 213–214].

Нарушения порядка обмена конфиденциальными документами целесообразно учитывать в целях последующего анализа и принятия мер по их предотвращению. Учет нарушений может осуществляться в карточке (журнале) (табл. 21) [7, с. 215].

Таблица 21

Форма журнала (карточки) учета нарушений обмена конфиденциальными документами

Дата нарушения	Инициалы, фамилия лица, допустившего нарушение	Краткое изложение характера нарушения	Причины нарушения	Принятые меры
1	2	3	4	5

5.8. Режим конфиденциальности при проведении совещаний и переговоров

Все документы, составляемые в процессе подготовки конфиденциального совещания, должны иметь гриф конфиденциальности. Документы (в том числе договоры, контракты и др.), предназначенные для раздачи участникам совещания, не должны содержать конфиденциальной информации. Эта информация сообщается участникам совещания устно при обсуждении конкретного вопроса. Цифровые значения конфиденциальной документированной информации (технические и технологические параметры, суммы, проценты, сроки, объемы и т. д.) в проектах решений и других документов не указываются или фиксируются в качестве общепринятой стартовой величины при обсуждении. В проектах не должно быть развернутых обоснований для предоставления льгот и скидок тем или иным партнерам, клиентам или лишения их льгот. Проекты документов, раздаваемые участникам совещания, не должны иметь грифа конфиденциальности.

Список участников совещания составляется отдельно по каждому обсуждаемому вопросу. К участию в обсуждении вопроса привлекаются только те работники организации,

которые имеют непосредственное отношение к этому вопросу. В списке участников указываются фамилии, имена и отчества лиц, занимаемые должности, представляемые ими организации и наименования документов, подтверждающих их полномочия вести переговоры и принимать решения. Наименование представляемой организации может при необходимости заменяться ее условным обозначением.

Документом, подтверждающим полномочия лица (если это не руководитель сторонней организации) при ведении переговоров и принятии решения по конкретному вопросу, может служить письмо, доверенность представляемой лицом организации, рекомендательное письмо юридического или физического лица, письменный ответ сторонней организации на запрос о полномочиях представителя, в отдельных случаях телефонное, факсимильное или электронное послание – подтверждение полномочий руководителем сторонней организации [7, с. 223].

Помещение, где будет проводиться конфиденциальное совещание, должно быть оборудовано средствами технической защиты информации, иметь кондиционер, так как открытие окон, дверей в ходе проведения совещания не допускается. Окна должны быть закрыты шторами, входная дверь оборудована сигналом, оповещающим о ее неплотном закрытии. В целях звукоизоляции целесообразно иметь двойную дверь (тамбур) или зашторивать двери звукопоглощающей тканью.

В помещении для проведения совещаний не должны находиться приборы, оборудование и технические средства, которые непосредственно не используются для обеспечения хода совещания, например, мобильные телефоны, компьютеры (ноутбуки), теле-, радиоприемники и др.

Перед началом совещания сотрудник службы безопасности обязан убедиться в отсутствии в помещении аудио- и видеозаписывающих или передающих устройств и качественной работе средств технической защиты на всех возможных каналах утечки информации. Аудио- и видеозапись конфиденциальных совещаний, фотографирование ведутся только по письменному указанию руководителя организации и осуществляются одним из работников, готовивших совещание [7, с. 224].

Участникам конфиденциального совещания независимо от занимаемой должности и статуса на совещании не разрешается:

- вносить в помещение, в котором проводится совещание, фото-, кино-, видеоаппаратуру, компьютеры, магнитофоны, радиоприемники, радиотелефоны, мобильные телефоны и другую аппаратуру, пользоваться ею;
- делать выписки из документов, используемых при решении вопросов на совещании и имеющих гриф конфиденциальности;
- обсуждать вопросы, вынесенные на совещание, в местах общего пользования (буфет, туалет, курительная комната);
- информировать о совещании (вопросах повестки дня, составе участников, времени и месте проведения, ходе обсуждения вопросов, содержании решения и т. д.) любых лиц, не связанных с проведением данного совещания, в том числе сотрудников организации [7, с. 225].

5.9. Проверка наличия носителей конфиденциальной информации

Необходимо проводить комплексные плановые проверки фактического наличия документов, дел и носителей, и правильности отметок об их учете, регистрации и движении.

Оптимальными видами проверок и сроками их проведения являются:

- проверка правильности учета и регистрации носителей, документов, дел, учетных и регистрационных журналов (картотек), в том числе электронных – сразу после учета и регистрации;

- проверка правильности проставления отметок о движении конфиденциальных носителей, документов и дел, независимо от времени их учета и регистрации, – сразу после проставления отметок или, при невозможности проведения их сразу после проставления отметок, по истечении каждого квартала;
- проверка фактического наличия всех носителей и всех не подшитых в дела и не переведенных на учет инвентарного (выделенного) хранения созданных/изданных (внутренних) и поступивших документов, независимо от времени их регистрации, – один раз в квартал по истечении квартала;
- проверка фактического наличия всех дел, а также документов выделенного хранения и журналов (картотек) учета, в том числе электронных, зарегистрированных в истекшем и предыдущих годах, – один раз в год по истечении года [7, с. 227].

Отметки о проверках правильности учета и регистрации носителей, документов, дел и учетных и регистрационных журналов (картотек), в том числе электронных, а также правильности записей о возврате документов проставляются условным обозначением, например, «+» или «*».

Отметки о проверках фактического наличия носителей, документов, дел и учетных и регистрационных журналов (картотек) целесообразно проставлять датами проверок, поскольку, как уже отмечалось, такие проверки частично повторяются и по дате можно отличить одну проверку от другой [7, с. 228].

По результатам проверок составляется акт (см. *Приложение 11*).

5.10. Классификация угроз информационной безопасности

Угрозами безопасности информации являются:
- хищение (копирование) информации;
- уничтожение информации;
- модификация (искажение) информации;
- нарушение доступности (блокирование) информации;
- отрицание подлинности информации;
- навязывание ложной информации.

Все источники угроз безопасности информации можно разделить на три основные группы:
- обусловленные действиями субъекта (антропогенные источники угроз);
- обусловленные техническими средствами (техногенные источники угрозы);
- обусловленные стихийными источниками.

Антропогенные источники угроз

Внешние источники могут быть случайными или преднамеренными и иметь разный уровень квалификации. К ним относятся:
- криминальные структуры;
- потенциальные преступники и хакеры;
- недобросовестные партнеры;
- технический персонал поставщиков телематических услуг (вид связи, основанный на удаленном доступе к информации. Исключением является телефония, так как она требует промежуточной обработки данных);
- представители надзорных организаций и аварийных служб;
- представители силовых структур.

Внутренние субъекты (источники), как правило, представляют собой высококвалифицированных специалистов в области разработки и эксплуатации программного обеспечения и технических средств, знакомы со спецификой решаемых задач, структурой и основными функциями и принципами работы программно-аппаратных средств защиты ин-

формации, имеют возможность использования штатного оборудования и технических средств сети. К ним относятся:

- основной персонал (пользователи, программисты, разработчики);
- представители службы защиты информации;
- вспомогательный персонал (уборщики, охрана);
- технический персонал (жизнеобеспечение, эксплуатация).

Техногенные источники угроз

Технические средства, являющиеся источниками потенциальных угроз безопасности информации, также могут быть внешними:

- средства связи;
- сети инженерных коммуникаций (водоснабжения, канализации);
- транспорт;

и внутренними:

- некачественные технические средства обработки информации;
- некачественные программные средства обработки информации;
- вспомогательные средства (охраны, сигнализации, телефонии);
- другие технические средства, применяемые в учреждении.

Стихийные источники угроз

Стихийные источники потенциальных угроз информационной безопасности, как правило, являются внешними по отношению к защищаемому объекту и под ними понимаются прежде всего природные катаклизмы:

- пожары;
- землетрясения;
- наводнения;
- ураганы;
- различные непредвиденные обстоятельства;
- необъяснимые явления;
- другие форс-мажорные обстоятельства.

При определении актуальных угроз экспертно-аналитическим методом определяются объекты защиты, подверженные воздействию той или иной угрозы, характерные источники этих угроз и уязвимости, способствующие реализации угроз. Один из возможных используемых методов представлен в *Приложении 8* [5].

5.11. Средства защиты информационных систем

Для предотвращения потери и утечки конфиденциальных сведений используются следующие средства:

Рис. 6. Способы и средства защиты информации

Вопросы для самоконтроля

1. Что представляет собой защита информации?
2. Что понимается под доступом к информации?
3. Чем отличаются понятия «доступ» и «допуск» к конфиденциальной информации?
4. Какой нормативный акт федерального значения включает основные принципы защиты информации?
5. Какой локальный нормативный документ содержит основные принципы разграничения доступа к информации в организации?
6. Для чего создается экспертная комиссия по защите конфиденциальной информации и какие подразделения организации в нее входят?
7. Назовите основные функции экспертной комиссии по защите конфиденциальной информации.
8. Назовите основные требования доступа к конфиденциальной информации.
9. В каком случае работодатель может использовать персональные данные работника, полученные у третьей стороны?
10. Для чего предназначена опись конфиденциальных документов, находящихся у исполнителя?
11. Разрешается ли аудио- и видеозапись конфиденциальных совещаний?
12. Назовите угрозы безопасности информации.
13. Перечислите виды антропогенных источников угроз.

Список использованных источников и литературы

Источники

1. Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне». URL: http://www.consultant.ru/document/cons_doc_LAW_48699/ (дата обращения: 17.01.2020).

2. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 17.01.2020).

3. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных». URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 19.01.2020).

4. Постановление Правительства РФ от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». URL: http://www.consultant.ru/document/cons_doc_LAW_137356/ (дата обращения: 17.01.2020).

Литература

5. Вихорев С.В. Классификация угроз информационной безопасности [Электрон. ресурс] // Cnews.ru. Интернет-издание о высоких технологиях [сайт]. [2001]. URL: https://cnews.ru/reviews/free/oldcom/security/elvis_class.shtml (дата обращения: 20.01.2020).

6. Егоров В.П. Конфиденциальное делопроизводство [Электрон. ресурс]: учеб. пособие / В.П. Егоров, А.В. Слиньков. М.: Юридический институт МИИТа, 2015. 178 с. (pdf).

7. Куняев Н.Н. Конфиденциальное делопроизводство и защищенный электронный документооборот [Электрон. ресурс]: учебник / Н.Н. Куняев, А.С. Демушкин, А.Г. Фабричнов; под общ. ред. Н.Н. Куняева. М.: Логос, 2011. 452 с. (Новая университетская библиотека). (pdf).

8. Мазурова В.В. Защита персональных данных работника // Сибирский торгово-экономический журнал. 2008. № 7. С. 80–82.

9. Режим хранения конфиденциальных документов [Электрон. ресурс] // «Lawneed». Сущность права [сайт]. [2019]. URL: http://www.lawneed.ru/psens-271-1.html (дата обращения: 17.01.2020).

10. Современные методы защиты информации [Электрон. ресурс] // Camafon.ru [сайт]. [2019]. URL: https://camafon.ru/informatsionnaya-bezopasnost/metodyi-zashhityi (дата обращения: 20.01.2020).

11. Согласие работника на обработку персональных данных: бланк на 2020 год [Электрон. ресурс] // Гуру бухгалтерии [сайт]. [2019]. URL: https://buhguru.com/kadrovaya-rabota/soglasie-rabotnika-na-obrabotku-personalnyh-dannyh-skachajte-obrazets.html#__2019-2020 (дата обращения: 19.01.2020).

12. Трубачева С.И. Основные аспекты защиты персональных данных на предприятии // Вестн. Волжск. ун-та им. В.Н. Татищева. Сер. Информатика. Вып. 16. Тольятти: Изд-во Волжск. ун-та им. В.Н. Татищева, 2010. С. 25–32.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

Подготовка доклада с презентацией

Цель самостоятельной работы: расширение научного кругозора, овладение методами теоретического исследования, развитие самостоятельности мышления студента.

Доклад – публичное сообщение или документ, которые содержат информацию и отражают суть вопроса или исследования применительно к данной ситуации.

Этапы работы над сообщением:

1. Подбор и изучение основных источников по теме (как и при написании реферата, рекомендуется использовать не менее 8–10 источников).
2. Подбор, анализ и систематизация материала.
3. Разработка плана сообщения.
4. Подготовка выводов и обобщений.
5. Написание.
6. Составление библиографического списка.
7. Публичное выступление с результатами исследования.

Сообщение должно занимать от 5 до 10 минут.

Сообщение демонстрирует такие качества исследователя, как умение провести исследование, умение преподнести результаты слушателям и квалифицированно ответить на вопросы.

Отличительной чертой сообщения является научный, академический стиль. Академический стиль предполагает следующие нормы: предложения могут быть длинными и сложными; часто употребляются слова иностранного происхождения, различные термины; употребляются вводные конструкции типа «по всей видимости», «на наш взгляд». При этом должны отсутствовать местоимения «я», «моя (точка зрения)»; в тексте могут встречаться клише – унифицированные фразы.

Планируемые результаты самостоятельной работы:

– способность студентов анализировать результаты научных исследований и применять их при решении конкретных образовательных и исследовательских задач;

– готовность использовать индивидуальные креативные способности для оригинального решения исследовательских задач;

– способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

Разработка мультимедийной презентации

Цели самостоятельной работы (варианты):

– освоение (закрепление, обобщение, систематизация) учебного материала;

– обеспечение контроля качества знаний;

– формирование специальных компетенций, обеспечивающих возможность работы с информационными технологиями;

– становление общекультурных компетенций.

Общие требования. Электронная презентация должна быть выполнена на основе материала подготовленного реферата и должна использоваться как визуальная иллюстрация устного доклада по теме реферата.

Презентация должна быть выполнена в приложении MS Power Point и сдана в электронном виде лично или отправлена по электронной почте в сроки, определенные преподавателем.

Требования к оформлению. Электронная презентация должна содержать не менее 6 слайдов, содержащих текстовую и графическую информацию по соответствующей теме.

На первом слайде необходимо указать тему, Ф.И.О. студента, курс обучения.

Разрешается использовать встроенные шаблоны слайдов и стили оформления презентации, а также эффекты мультипликации.

Желательно избегать вставок в презентацию больших по объему графических файлов.

Оригинальные шрифтовые и оформительские решения приветствуются.

Планируемые результаты самостоятельной работы:

– повышение информационной культуры студентов и обеспечение их готовности к интеграции в современное информационное пространство;

– способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

– способность к критическому восприятию, обобщению, анализу профессиональной информации, постановке цели и выбору путей ее достижения;

– способность применять современные методики и технологии организации и реализации образовательного процесса на различных образовательных ступенях в различных образовательных учреждениях;

– готовность использовать индивидуальные креативные способности для оригинального решения исследовательских задач.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

Источники

1. Укрупненные нормы времени на работы, выполняемые в объединенных архивах, хранящих документы по личному составу учреждений, организаций, предприятий (утв. Постановлением Минтруда РФ от 18 декабря 1992 г. № 57). URL: http://www.consultant.ru/document/cons_doc_LAW_90905/ (дата обращения: 30.12.2019).
2. Постановление Минтруда РФ от 10 сентября 1993 г. № 152 «Об утверждении Норм времени на работы по автоматизированной архивной технологии и документационному обеспечению органов управления». URL: http://www.consultant.ru/document/cons_doc_LAW_91031/ (дата обращения: 30.12.2019).
3. Постановление Минтруда РФ от 25 ноября 1994 г. № 72 «Об утверждении Межотраслевых укрупненных нормативов времени на работы по документационному обеспечению управления». URL: http://www.consultant.ru/document/cons_doc_LAW_98813/ (дата обращения: 30.12.2019).
4. Постановление Госстандарта РФ от 26 декабря 1994 г. № 367 (ред. от 19 июня 2012 г.) «О принятии и введении в действие Общероссийского классификатора профессий рабочих, должностей служащих и тарифных разрядов ОК 016-94» (вместе с «ОК 016-94. Общероссийский классификатор профессий рабочих, должностей служащих и тарифных разрядов») (дата введения 01.01.1996). URL: http://www.consultant.ru/document/Cons_doc_LAW_58964/ (дата обращения: 30.12.2019).
5. Гражданский кодекс Российской Федерации от 26 января 1996 г. № 51-ФЗ. URL: http://www.consultant.ru/document/cons_doc_LAW_5142/ (дата обращения: 15.07.2019).
6. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ. URL: http://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 15.07.2019).
7. Квалификационный справочник должностей руководителей, специалистов и других служащих (утв. Постановлением Минтруда России от 21 августа 1998 г. № 37) (ред. от 27 марта 2018 г.). URL: http://www.consultant.ru/document/cons_doc_LAW_58804/ (дата обращения: 30.12.2019).
8. Федеральный конституционный закон от 25 декабря 2000 г. № 2-ФКЗ «О Государственном гербе Российской Федерации». URL: http://www.consultant.ru/document/cons_doc_LAW_29674/ (дата обращения: 16.12. 2019).
9. Федеральный закон Российской Федерации от 07 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма». URL: http://www.consultant.ru/document/cons_doc_LAW_32834/ (дата обращения: 15.07.2019).
10. Постановление Минтруда РФ от 26 марта 2002 г. № 23 «Об утверждении норм времени на работы по документационному обеспечению управленческих структур федеральных органов исполнительной власти». URL: http://www.consultant.ru/document/cons_doc_LAW_91156/ (дата обращения: 30.12.2019).
11. Гражданско-процессуальный кодекс Российской Федерации от 14 ноября 2002 г. № 138-ФЗ. http://www.consultant.ru/document/cons_doc_LAW_39570/ (дата обращения: 15.07.2019).
12. Федеральный закон Российской Федерации от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне». URL: http://www.consultant.ru/document/cons_doc_LAW_48699/ (дата обращения: 15.07.2019).
13. Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 15.07.2019).

14. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 19.01.2020).

15. Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации». URL: https://base.garant.ru/193875/ (дата обращения: 15.07.2019).

16. Перечень типовых управленческих документов, образующихся в деятельности организаций, с указанием сроков хранения, утвержденный руководителем Росархива от 26 августа 2010 г. № 63. URL: http://www.consultant.ru/document/cons_doc_LAW_104953/ (дата обращения: 13.01.2020).

17. Постановление Правительства Российской Федерации от 03 февраля 2012 г. № 79 (ред. от 15 июня 2016 г.) «О лицензировании деятельности по технической защите конфиденциальной информации» (вместе с «Положением о лицензировании деятельности по технической защите конфиденциальной информации»). URL: http://www.consultant.ru/ document/cons_doc_LAW_125798/(дата обращения: 15.07.2019).

18. Постановление Правительства РФ от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». URL: http://www.consultant.ru/document/cons_doc_LAW_137356/ (дата обращения: 17.01.2020).

19. Правила организации хранения, комплектования, учета и использования документов Архивного фонда Российской Федерации и других архивных документов в органах государственной власти, органах местного самоуправления и организациях от 31 марта 2015 г. № 526. URL: http://www.consultant.ru/document/cons_doc_LAW_185738/ (дата обращения: 16.01.2020).

20. ГОСТ Р 7.0.8-2013. Национальный стандарт Российской Федерации. «Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения» (утв. Приказом Росстандарта от 17 октября 2013 г. № 1185-ст). URL: http://www.consultant.ru/document/cons_doc_LAW_163800/ (дата обращения: 15.07.2019).

21. ГОСТ Р 7.0.97-2016. Национальный стандарт Российской Федерации. «Система стандартов по информации, библиотечному и издательскому делу. Организационно-распорядительная документация. Требования к оформлению документов» (утв. Приказом Росстандарта от 08 декабря 2016 г. № 2004-ст). URL: http://www.consultant.ru/document/cons_doc_LAW_216461/ (дата обращения: 16.12. 2019).

Литература

22. Алексенцев А.И. Конфиденциальное делопроизводство // Управление персоналом [Электрон. ресурс]. М., 2003. 200 с. (pdf).

23. Вихорев С.В. Классификация угроз информационной безопасности [Электрон. ресурс] // Cnews.ru. Интернет-издание о высоких технологиях [сайт]. [2001]. URL: https://cnews.ru/reviews/free/oldcom/security/elvis_class.shtml (дата обращения: 20.01.2020).

24. Егоров В.П. Конфиденциальное делопроизводство [Электрон. ресурс]: учеб. пособие / В.П. Егоров, А.В. Слиньков. М.: Юридический институт МИИТа, 2015. 178 с. (pdf).

25. Законодательство и другие нормативные материалы по принятию конфиденциального режима [Электрон. ресурс] // Студенческая библиотека онлайн: [сайт]. URL: https://studbooks.net/859948/buhgalterskiy_uchet_i_audit/zakonodatelstva_podzakonnye_akty_reguliruyuschie_konfidentsialnoe_deloproizvodstvo (дата обращения: 15.07.2019).

26. Куняев Н.Н. Конфиденциальное делопроизводство и защищенный электронный документооборот [Электрон. ресурс]: учебник / Н.Н. Куняев, А.С. Демушкин, А.Г. Фаб-

ричнов; под общ. ред. Н.Н. Куняева. М.: Логос, 2011. 452 с. (Новая университетская библиотека). (pdf).

27. Мазурова В.В. Защита персональных данных работника // Сибирский торгово-экономический журнал. 2008. № 7. С. 80–82.

28. Маланыч И.Н. Международные правовые нормы в сфере защиты персональных данных [Электрон. ресурс] // ISO27000.ru. Искусство управления информационной безопасностью [сайт]. URL: http://www.iso27000.ru/chitalnyi-zai/zaschita-personalnyh-dannyh/mezhdunarodnye-pravovye-normy-v-sfere-zaschity-personalnyh-dannyh (дата обращения: 16.08.2019).

29. Международная охрана интеллектуальной собственности [Электрон. ресурс] // «Гардиум» – аккредитованный партнер Российского экспорного центра: [сайт]. URL: https://legal-support.ru/information/blog/zashita-prav/mezhdunarodnaya-ohrana-intellektualnoi-sobstvennosti/ (дата обращения: 15.08.2019).

30. Мэггс П.Б., Сергеев А.П. Интеллектуальная собственность [Электрон. ресурс]. М.: Юристъ, 2000. 400 с. URL: https://studfiles.net/preview/5251206/page:3/ (дата обращения: 15.08.2019).

31. Панкратьев В.В. Организация конфиденциального делопроизводства [Электрон. ресурс] // Техника для спецслужб [сайт]. [2007]. URL: http://www.bnti.ru/showart.asp?aid=808&lvl=04 (дата обращения: 14.10.2017).

32. Режим хранения конфиденциальных документов [Электрон. ресурс] // «Lawneed». Сущность права [сайт]. [2019]. URL: http://www.lawneed.ru/psens-271-1.html (дата обращения: 17.01.2020).

33. Современные методы защиты информации [Электрон. ресурс] // Camafon.ru [сайт]. [2019]. URL: https://camafon.ru/informatsionnaya-bezopasnost/metodyi-zashhityi (дата обращения: 20.01.2020).

34. Согласие работника на обработку персональных данных: бланк на 2020 год [Электрон. ресурс] // Гуру бухгалтерии [сайт]. [2019]. URL: https://buhguru.com/kadrovaya-rabota/soglasie-rabotnika-na-obrabotku-personalnyh-dannyh-skachajte-obrazets.html#__2019-2020 (дата обращения: 19.01.2020).

35. Сотрудничество со Всемирной организацией интеллектуальной собственности (ВОИС) [Электрон. ресурс] // Роспатент. Федеральная служба по интеллектуальной собственности [официальный сайт]. URL: https://rupto.ru/ru/activities/inter/coop/wipo (дата обращения: 15.08.2019).

36. Трубачева С.И. Основные аспекты защиты персональных данных на предприятии // Вестн. Волжск. ун-та им. В.Н. Татищева. Сер. Информатика. Вып. 16. Тольятти: Изд-во Волжск. ун-та им. В.Н. Татищева, 2010. С. 25–32.

37. Фирсова А.Ю. Модуль 8. Работа с конфиденциальными документами. Курс повышения квалификации/профессиональной переподготовки «Основы делопроизводства и секретарское дело» [Электрон. ресурс] // Академия подготовки главных специалистов [сайт]. [2019]. URL: https://specialitet.ru (дата обращения: 03.11.2019).

38. Янковая В.Ф. Нормативная база для работы с конфиденциальными документами [Электрон. ресурс] // Журнал об электронном контенте, документах и бизнес-процессах «ECM-Journal»: [сайт]. 12 августа 2013 г. URL: https://ecm-journal.ru/card.aspx?ContentID=4694943 (дата обращения: 15.07.2019).

ПРИЛОЖЕНИЯ

Приложение 1

Виды информации, которая не может составлять коммерческую тайну

Коммерческую тайну не могут составлять сведения:

1) содержащиеся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры;

2) содержащиеся в документах, дающих право на осуществление предпринимательской деятельности;

3) о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов;

4) о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и безопасности населения в целом;

5) о численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости, о наличии свободных рабочих мест;

6) о задолженности работодателей по выплате заработной платы и по иным социальным выплатам;

7) о нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений;

8) об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности;

9) о размерах и структуре доходов некоммерческих организаций, о размерах и составе их имущества, об их расходах, о численности и об оплате труда их работников, об использовании безвозмездного труда граждан в деятельности некоммерческой организации;

10) о перечне лиц, имеющих право действовать без доверенности от имени юридического лица;

11) а также сведения, обязательность раскрытия которых или недопустимость ограничения доступа к которым установлена иными федеральными законами.

Приложение 2

Форма номенклатуры конфиденциальных дел

Наименование предприятия

«УТВЕРЖДАЮ»
Руководитель предприятия
_____
(подпись, инициалы, фамилия)
«__» _____ _____ г.

НОМЕНКЛАТУРА КОНФИДЕНЦИАЛЬНЫХ ДЕЛ
на _____ год

Индекс (номер) дела, отметка конфиденциальности	**Заголовок дела**	**Ф.И.О. лиц, которым предоставлено право пользования делом**	**№ тома**
1	2	3	4

Окончание

Дата		**Количество листов в томе**	**Срок хранения и номера статей по Перечню**	**Архивный шифр; номер и дата акта об уничтожении; номер и дата сопроводительного документа**
заведения тома	**закрытия тома**			
5	6	7	8	9

Руководитель подразделения КД
_____
(подпись, инициалы, фамилия, дата)

Рассмотрена и одобрена на заседании
ПДЭК предприятия
Протокол от _____ №_____

СОГЛАСОВАНО
Руководитель архива
предприятия
_____
(подпись, инициалы, фамилия, дата)

Приложение 3

Форма обложки конфиденциального дела

_____
(отметка конфиденциальности)

_____
(название организации)

_____
(название структурного подразделения)

Д Е Л О №___ Т О М №___

_____
_____
_____
(заголовок дела)

«____» _____ 20___ г.
«____» _____ 20___ г.
(крайние даты документов)

На _____ листах
Хранить _____ ст. ___
Перечня документов со сроками хранения

Приложение 4

Форма описи документов инвентарного (выделенного) хранения, которые отобраны для постоянного хранения

УТВЕРЖДАЮ
Наименование должности
руководителя организации
_____
(подпись, расшифровка подписи)
«__» _____ _____ г.

ФОНД № _____
ОПИСЬ № _____
конфиденциальных дел _____
и документов инвентарного (выделенного)
хранения за _____год

№ п/п	Индекс (номер) дела или номер документа и отметка конфиденциальности	Заголовок дела или документа	Количество листов	Примечание
1	2	3	4	5

В данную опись внесено _____дел и документов
(цифрами и прописью)
№ _____ по № _____ , в том числе:
литерные номера: _____
пропущенные номера: _____
Наименование должности
сотрудника, составившего опись _____
(подпись, расшифровка подписи)

Дата _____
Одобрено _____
Протокол ЭК _____
от _____ № _____
Включенные в настоящую опись дела и документы принял:
Наименование должности
сотрудника Архива организации _____
(подпись, расшифровка подписи)

Дата_____

Приложение 5

Форма акта о выделении к уничтожению архивных документов, не подлежащих хранению

Наименование организации

АКТ
_____ № _____
о выделении к уничтожению
архивных документов,
не подлежащих хранению

УТВЕРЖДАЮ
Руководитель организации

Подпись Расшифровка подписи

Дата

На основании _____
(название и выходные данные перечня документов с указанием
_____
сроков их хранения)
отобраны к уничтожению как не имеющие научно-исторической ценности и утратившие практическое значение документы фонда № _____
(название фонда)

№ п/п	Заголовок дела (групповой заголовок документов)	Годы	Номер описи[1]	Номер ед. хр. по описи	Количество ед. хр.	Сроки хранения и номера статей по перечню	Примечание
1	2	3	4	5	6	7	8

Итого _____ ед. хр. за _____ годы
(цифрами и прописью)
Описи дел постоянного хранения за _____ годы утверждены ЭПК
_____
(наименование архивного учреждения)
(протокол от _____ № _____)

Наименование должности
руководителя архива (лица,
ответственного за архив) Подпись Расшифровка подписи

СОГЛАСОВАНО
Протокол ЦЭК (ЭК) организации
от _____ № _____

[1] При выделении к уничтожению документов при подготовке дел к передаче в архив организации графы 4, 5 не заполняются.

Документы в количестве _____ ед. хр.:
– на бумажном носителе весом __ _____ кг
сданы на уничтожение;
– на электронном носителе сданы на уничтожение _____
_____
(способ уничтожения)

Наименование должности работника,
сдавшего документы Подпись Расшифровка подписи

Дата

Изменения в учетные документы внесены

Наименование должности работника
архива, внесшего изменения
в учетные документы Подпись Расшифровка подписи

Дата

Примеры величины бумажных обрезков, полученных при применении различных вариантов измельчения документов в зависимости от степени конфиденциальности

Приложение 7

Форма обязательства о неразглашении конфиденциальной информации

ОБЯЗАТЕЛЬСТВО
о неразглашении конфиденциальной информации

Я, _____,
(фамилия, имя, отчество, должность)
в качестве работника
_____
(наименование структурного подразделения)
(именуемого в дальнейшем «Организация») в период трудовых (служебных) отношений с Организацией (ее правопреемником) и в течение _____ лет после их окончания, в соответствии с п. __ трудового договора, заключенного между мной и Организацией, а также соответствующими положениями по обеспечению защиты и охраны конфиденциальной информации, действующими в Организации, обязуюсь:

1) не разглашать конфиденциальную информацию Организации, которая мне будет доверена или станет известна по работе (службе);

2) не передавать третьим лицам и не раскрывать публично конфиденциальную информацию Организации без согласия Организации;

3) выполнять относящиеся ко мне требования приказов, инструкций и положений по обеспечению сохранности конфиденциальной информации Организации;

4) в случае попытки посторонних лиц получить от меня конфиденциальную информацию Организации немедленно сообщить
_____;
(должностное лицо или подразделение Организации)

5) сохранять конфиденциальную информацию тех организаций, с которыми у Организации имеются деловые отношения;

6) не использовать знание конфиденциальной информации Организации для занятий любой деятельностью, которая может нанести ущерб Организации;

7) в случае моего увольнения все носители конфиденциальной информации Организации (рукописи, черновики, чертежи, магнитные ленты, диски, дискеты, распечатки на принтерах, кино-, фотонегативы и позитивы, модели, материалы, изделия и пр.), которые находились в моем распоряжении в связи с выполнением мною служебных обязанностей во время работы в Организации, передать
_____
(должностное лицо или подразделение Организации)

8) об утрате или недостаче носителей конфиденциальной информации, удостоверений, пропусков, ключей от режимных помещений, хранилищ, сейфов (металлических шкафов), личных печатей и о других фактах, которые могут привести к разглашению конфиденциальной информации Организации, а также о причинах и условиях возможной утечки сведений немедленно сообщать
_____
(должностное лицо или подразделение Организации)

Я предупрежден, что в случае невыполнения любого из пп. 1, 2, 3, 4, 5, 6, 8 настоящего обязательства могу быть уволен из Организации в соответствии с п. «в» ч. 6 ст. 81 ТК РФ.

До моего сведения также доведены с разъяснениями соответствующие положения по обеспечению сохранности конфиденциальной информации Организации, и я получил один экземпляр этих положений.

Мне известно, что нарушение этих положений может повлечь уголовную, административную, гражданско-правовую или иную ответственность, предусмотренную ст. 13.11, 13.14 КоАП РФ, ст. 183 УК РФ, иными нормативными правовыми актами Российской Федерации, в виде лишения свободы, денежного штрафа, обязанности по возмещению ущерба Организации (убытков, упущенной выгоды и морального ущерба) и других наказаний.

С Перечнем конфиденциальной документированной информации Организации и Регламентом по доступу к конфиденциальной информации ознакомлен.

_____ _____ _____

(подпись) (расшифровка подписи) (дата подписания)

Руководство Организации подтверждает, что данные Вами обязательства не ограничивают Ваших прав на интеллектуальную собственность. Об окончании срока действия обязательства руководство Организации уведомит Вас заблаговременно в письменной форме.

«____» _____ _____ г.

_____ _____ _____

(должность) (подпись) (расшифровка подписи)

Обязательства составлены в двух экземплярах. Один экземпляр находится у работника, второй хранится в Организации в качестве приложения к трудовому договору или личному делу работника.

Один экземпляр обязательств получил.

_____ _____ _____

(подпись) (расшифровка подписи) (дата подписания)

Приложение 8

Форма согласия на обработку персональных данных

СОГЛАСИЕ
на обработку персональных данных

Я,_____,
(фамилия, имя, отчество субъекта персональных данных)
в соответствии с п. 4 ст. 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», зарегистрирован___ по адресу: _____,
документ, удостоверяющий личность: _____,
_____
(наименование документа, серия и №, сведения о дате выдачи документа и выдавшем его органе)
(Вариант: _____,
(фамилия, имя, отчество представителя субъекта персональных данных)
зарегистрирован___ по адресу: _____,
документ, удостоверяющий личность: _____
_____,
(наименование документа, серия и №, сведения о дате выдачи документа и выдавшем его органе)
Доверенность от «__» _____ ____ г. № ___
(или реквизиты иного документа, подтверждающего полномочия представителя)
в целях _____
(указать цель обработки данных)
даю согласие _____,
(указать наименование или Ф.И.О. оператора, получающего согласие субъекта персональных данных)
находящемуся по адресу: _____,
(Вариант: _____,
(указать наименование или Ф.И.О. лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу)
находящемуся по адресу: _____,)
на обработку моих персональных данных, а именно: _____
_____,
(указать перечень персональных данных, на обработку которых дается согласие субъекта персональных данных)
то есть на совершение действий, предусмотренных п. 3 ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

Настоящее согласие действует со дня его подписания до дня отзыва в письменной форме[1].

«___»_____ ____ г.

Субъект персональных данных:

_____/_____
(подпись) (Ф.И.О.)

[1] Согласно п. 8 ч. 4 ст. 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности, срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом.

Приложение 9

Форма номенклатуры должностей работников, подлежащих оформлению на допуск к конфиденциальной документированной информации

УТВЕРЖДАЮ

_____

(руководитель организации или зам. руководителя по вопросам защиты КДИ)

_____

Подпись И.О. Фамилия

«___»_____20___ г.

Номенклатура должностей работников, подлежащих оформлению на допуск к КДИ

(по заполнении конфиденциально)

№ п/п	Подразделение	Количество работающих	Должность	Обоснование необходимости допуска	Количество лиц, подлежащих оформлению на доступ к КДИ			Количество лиц, оформленных на доступ к КДИ	Примечание
					вид конфиденциальной информации	степень «Конфиденциально»	Степень «Строго конфиденциально»		
1	2	3	4	5	6	7	8	9	10

«___» _____ 20__ г.

Руководитель Службы безопасности _____

(подпись)

Примечания.

1. Должности в номенклатуре указываются по каждому структурному подразделению с подведением итогов.
2. Порядковые номера указываются в возрастающей последовательности независимо от структурных подразделений.
3. В графе 5 кратко отражаются характер документов или выполняемых работ и степень их конфиденциальности со ссылкой на конкретный пункт Перечня конфиденциальной документированной информации.
4. В графе 9 указывается только общее количество лиц, подлежащих оформлению на допуск к конфиденциальной документированной информации, без обоснования необходимости допуска.
5. В графах 6–9 подводится итог по организации.

Приложение 10

Форма акта проведения внутреннего расследования по факту разглашения информации и (или) утраты, хищения, порчи документов

АКТ
проведения внутреннего расследования по факту разглашения информации и (или) утраты, хищения, порчи документов

*(дата)*_____

Комиссия в составе:
председатель комиссии _____
(должность, фамилия, имя, отчество)
члены комиссии:
1. _____
(должность, фамилия, имя, отчество)
2. _____
(должность, фамилия, имя, отчество)
3. _____
(должность, фамилия, имя, отчество)
по факту _____
(хищение, разглашение, порча документов, другое)
на основании _____
(докладная записка, акт проверки, другое)
провели расследование и выяснили следующее: _____
Прилагаются документы:
1. Объяснительная записка
_____
(структурное подразделение, должность, фамилия, имя, отчество работника)
2. _____
3. _____
На основании полученной информации и прилагаемых документов комиссия сделала вывод: _____
Акт составлен в 3-х экземплярах:
1-й экз. подшит в дело № __.
2-й экз. передан работнику.
Председатель комиссии: _____
(подпись) (расшифровка подписи)
Члены комиссии: _____
(подпись) (расшифровка подписи)
_____
(подпись) (расшифровка подписи)
_____
(подпись) (расшифровка подписи)
3-й экз. подшит в личное дело.

Приложение 11

Форма акта о проверке наличия конфиденциальных документов

УТВЕРЖДАЮ
Наименование должности
руководителя организации

_____ _____
(подпись, инициалы, фамилия)
«_ _»_____ ___ ___ г.

АКТ

_____№ _____

О проверке наличия конфиденциальных документов за_____

Составлен: _____
(инициалы, фамилии лиц, проводивших проверку)
В период с _____по _____201_ г. проведена проверка:
1) правильности проставления учетных данных носителей, документов, дел и журналов (картотек) учета;
2) правильности произведения отметок о движении носителей, документов и дел, независимо от времени их регистрации;
3) фактического наличия всех дел и документов выделенного хранения (без просчета листов);
4) фактического наличия всех носителей, внутренних (созданных/изданных) и поступивших документов с просчетом количества листов, независимо от времени их регистрации *(если рабочие и стенографические тетради проверялись без просчета количества листов, то это фиксируется в скобках или примечаниях)*;
5) фактического наличия журналов (картотек) учета (без просчета количества листов, карточек);
6) закрытия всех учетных номеров в журналах (картотеках) учета внутренних (созданных/изданных) поступивших документов и носителей.
В результате проверки установлено, что:
1. Все подлежащие проверке дела, документы инвентарного (выделенного) хранения и журналы (картотеки) учета находятся в наличии. *(Если в наличии не все, то пишется слово «кроме», с указанием учетных номеров документов или индексов (номеров) и года дел (журналов))*.
2. Все учетные номера в журналах (картотеках) закрыты.
3. Номера дел (документов инвентарного (выделенного) хранения, документов по другим формам учета) не учтены.
4. Все учетные данные, проставленные на носителях, документах, делах, журналах (картотеках) учета, соответствуют данным, проставленным в учетных формах. (*Если в процессе проверки были обнаружены факты несоответствия, то пишется «кроме», с указанием по каждому документу (носителю, делу), в чем они проявились*).
5. Все отметки о движении документов, дел и носителей соответствуют сопроводительным (оправдательным) материалам и фактическому местонахождению документов. (*Если в процессе проверки были обнаружены факты несоответствия, то пишется «кроме», с указанием по каждому документу (носителю, делу), в чем они проявились).*
6. Имеются следующие ошибки и нарушения в учете и хранении документов. *(Перечисляются ошибки, нарушения и меры, принятые по их устранению. Пункт включается в акт при выявлении ошибок и нарушений).*

ОГЛАВЛЕНИЕ

Учебное издание

Александра Владимировна Спичак

КОНФИДЕНЦИАЛЬНОЕ ДЕЛОПРОИЗВОДСТВО

Учебное пособие

Редактор *Н.В. Титова*
Технический редактор *Н.В. Титова*

Изд. лиц. ЛР № 020742. Подписано в печать 20.05.2020
Формат 60×84/8. Бумага для множительных аппаратов
Гарнитура Times. Усл. печ. листов 14,75
Тираж 300 экз. Заказ 2137

Нижневартовский государственный университет
628616, Тюменская область, г.Нижневартовск, ул. Маршала Жукова, 4
Тел./факс: (3466) 24-50-51, e-mail: izdatelstvo@nggu.ru