

МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ПУТЕЙ СООБЩЕНИЯ ИМПЕРАТОРА НИКОЛАЯ II (МИИТ)

ЮРИДИЧЕСКИЙ ИНСТИТУТ

В. П. ЕГОРОВ,
А. В. СЛИНЬКОВ

ДЕЛОПРОИЗВОДСТВО И РЕЖИМ СЕКРЕТНОСТИ

Учебное пособие

МОСКВА—2016

УДК 651
ББК 63.2
Е—30

Авторы:

Егоров В. П., почетный работник высшего профессионального образования Российской Федерации, доктор военных наук, профессор, заведующий кафедрой «Документоведение и документационное обеспечение управления» Юридического института МИИТ — предисловие, гл. 1—6.

Слиньков А. В., методист учебно-методического Центра «Наследие Митрополита Пителима» МИИТ — гл. 7—13.

Рецензенты:

Фроликов И. И. — кандидат технических наук, начальник учебно-методического управления МИИТ;

Зейналова Р. М. — кандидат юридических наук, доцент кафедры «Теория и история государства и права», декан Юридического факультета имени С. Ю. Витте.

Егоров, В. П. Делопроизводство и режим секретности : учеб. пособие / В. П. Егоров, А. В. Слиньков. — М. : Юридический институт МИИТ, 2016. — 185 с.

В учебном пособии изложено современное состояние документоведения и документационного обеспечения управления. Раскрываются их значение и место в обществе. Особое внимание уделено содержанию документов и использованию электронных документов в системе управления в вопросах правового обеспечения национальной безопасности и правоохранительной деятельности. Структура пособия отражает последовательность этапов работы с документами, соблюдение персональной ответственности за сохранность документов и обеспечении конфиденциальности и секретности содержащихся в них сведений.

Книга рекомендуется преподавателям, студентам высших и средних учебных заведений, обучающихся по направлениям 40.05.01 «Правовое обеспечение национальной безопасности», 40.05.02 «Правоохранительная деятельность», 46.03.02 «Документоведение и архивоведение».

Учебное пособие издается в авторской редакции с сокращениями.

В работе использована справочная правовая система КонсультантПлюс.

© Юридический институт МИИТа, 2016

Оглавление

<i>Предисловие</i>	6
Раздел I. Документоведение, документ и система документов	10
Глава 1. Документ и его место в системе управления.....	10
1.1. Понятия «документ», «информация»	10
1.2. Способы документирования	11
1.3. Система документации и управление	14
Глава 2. Информационно-документационное обеспечение работы аппарата управления	18
2.1. Основные виды документной деятельности	18
2.2. Информация в управленческой деятельности.....	20
2.3. Управление документацией	27
2.4. Организация информационно-поисковых систем по документам учреждения	30
2.5. Основные функциональные системы документации в Российской Федерации	39
2.6. Унифицированные системы документации	46
Раздел II. Введение в конфиденциальное делопроизводство.	
Оформление и учет носителей конфиденциальной информации	48
Глава 3. Введение в организацию конфиденциального делопроизводства. Виды тайн и их классификация	48
3.1. Цели защиты конфиденциальной информации	48
3.2. Два взгляда на организацию конфиденциального делопроизводства	50
3.3. Основные термины и определения	52
3.4. Виды тайн и их классификация.....	55
Глава 4. Структура защищенного документооборота	59
4.1. Структура защищенного документооборота	59
4.2. Сущность задачи и особенности конфиденциального делопроизводства.....	61
4.3. Система доступа к конфиденциальным документам.....	69
Глава 5. Организация исполнения конфиденциальных документов.....	73
5.1. Организация исполнения конфиденциальных документов	73
5.2. Отправление конфиденциальных документов.....	79
Глава 6. Организация конфиденциального делопроизводства	82
6.1. Подразделения конфиденциального делопроизводства	82
6.2. Организационно-правовые документы, регламентирующие статус подразделения и каждого из его сотрудников. Требования к помещениям и режиму работы	85

6.3. Постоянно действующая экспертная комиссия и ее задачи	89
Глава 7. Определение состава конфиденциальных документов	90
7.1. Определение состава конфиденциальных документов	90
7.2. Перечень сведений, составляющих коммерческую тайну	92
7.3. Критерии документирования информации	98
Глава 8. Подготовка и издание конфиденциальных документов	102
8.1. Оформление и учет носителей конфиденциальной информации	102
8.2. Изготовление и учет носителей конфиденциальной информации	108
8.3. Оформление издаваемых конфиденциальных документов	116
Глава 9. Общие требования к учету документов	118
9.1. Общие требования к учету конфиденциальных документов	118
9.2. Учет изданных конфиденциальных документов	122
9.3. Учет поступивших конфиденциальных документов	123
9.4. Учет конфиденциальных документов выделенного хранения	129
9.5. Размножение конфиденциальных документов	131
Раздел III. Режим хранения, виды и принципы проверок конфиденциальных документов	137
Глава 10. Режим хранения конфиденциальных документов и обращения с ними.....	137
10.1. Режим хранения конфиденциальных документов	137
10.2. Порядок обращения с конфиденциальными документами	142
Глава 11. Принципы проведения проверок наличия конфиденциальных документов	145
11.1. Назначение, виды и принципы проведения проверок наличия конфиденциальных документов	145
11.2. Проверка правильности проставления регистрационных данных конфиденциальных носителей, документов, дел и учетных журналов (карточек)	148
11.3. Проверки правильности проставления отметок о движении конфиденциальных документов дел и носителей.....	151
Глава 12. Виды проверок наличия конфиденциальных документов	155
12.1. Квартальные проверки фактического наличия конфиденциальных носителей и документов.....	155
12.2. Годовая проверка наличия конфиденциальных дел	157
12.3. Нерегламентированные проверки наличия конфиденциальных носителей, документов и дел	159
Глава 13. Режим секретности	161
13.1. Тайна и государственная тайна, режим секретности	161
13.2. Роль и место внутриобъектового и пропускного режимов в системе защиты информации предприятия	163

13.2.1. Внутриобъектовый и пропускной режимы	163
13.2.2. Работа по организации внутри объектового режима. Основные подходы и принципы	164
13.2.3. Меры, которые предусматривает внутри объектовый режим	166
13.2.4. Силы и средства, используемые при организации внутри объектового режима	168
13.2.5. Организационные средства защиты информации	170
13.3. Компоненты защиты режима секретности	177
Рекомендуемая литература	183

Предисловие

В последнее время в различных слоях российского общества не утихают разговоры о необходимости политической и экономической модернизации страны. Так что само время определило задачу совершенствования организационной структуры и методов управления как важного звена в улучшении руководства экономикой. Значительное место в успешном решении этой задачи занимает документоведение и документационное обеспечение управления (далее — «делопроизводство») особенно в сферах правового обеспечения национальной безопасности и правоохранительной деятельности.

Документоведение и документационное обеспечение управления (делопроизводство) — это один из инструментов управления (менеджмента).

Документ — явление сложное и древнее. Его появление, эволюция, функции, требования, предъявляемые к его составлению и оформлению, а также весь порядок работы с ним изучаются в профессиональном цикле.

Значение делопроизводственного обслуживания, как одной из сфер управленческой деятельности, определяется универсальностью делопроизводства, поскольку основу информационного хозяйства любого предприятия, учреждения или организации составляют традиционные, рукописные, типографские документы, документы на магнитных носителях, электронные документы и др.

Велик удельный вес делопроизводственных операций в общем объеме управленческого труда. На работу с документами специалисты тратят 20-60% рабочего времени.

Организация делопроизводства влияет на оперативность, экономичность, надежность функционирования аппарата управления, организацию и культуру труда управленческих работников. При рационально организованном делопроизводственном процессе специалисты и руководители освобождаются от несвойственных им операций, повышается производительность и эффективность их труда и сокращаются затраты, связанные с функционированием аппарата управления.

В правильной организации делопроизводства заложены основы сохранности и эффективного использования документов в будущем.

С целью регламентации и рационализации работы с документами в учреждениях, организациях и на предприятиях на основе государственной системы делопроизводства разрабатывается своя система документооборота. Цель государственной системы документационного обеспечения управления — доведение до уровня общей нормы оправдавших себя на практике и апробированных рациональных форм и методов обработки служебной документации — может быть достигнута, если служащие, занятые обработкой документов, будут использовать в практической деятельности правила и нормы рационального делопроизводства.

В современном мире, когда прямо или косвенно затрагиваются вопросы управления, неминуемо присутствует понятие «система» или система управления.

Под системой следует понимать некое целостное образование, состоящее из отдельных элементов. Эти элементы связаны между собой энергетическими или информационными (а чаще и теми и другими) связями.

Проблема защиты информации от несанкционированного доступа к ней возникла давно, с той поры, когда человеку по каким-либо причинам не хотелось делиться ею ни с кем или не с каждым человеком. С развитием человеческого общества, появлением частной собственности, государственного строя, борьбой за власть и дальнейшим расширением масштабов человеческой деятельности информация приобретает цену. Ценной становится та информация, обладание которой позволит ее существующему и потенциальному владельцам получить какой-либо выигрыш: материальный, политический, военный и т.д. С переходом на использование технических средств связи информация подвергается воздействию случайных процессов: неисправностям и сбоям оборудования, ошибкам операторов и т.д., которые могут привести к ее разрушению, изменению на ложную, а также создать предпосылки к доступу к ней посторонних лиц. С дальнейшим усложнением и широким распространением технических средств связи возросли возможности для преднамеренного доступа к информации. Увеличение объемов информации, необходимость сосредоточения ее в единые базы данных, автоматизация обмена информацией на больших расстояниях, расширение круга пользователей и увеличение количества технических средств и связей в автома-

тизированных системах управления и обработки данных стало предпосылкой создания сложных автоматизированных систем.

С появлением сложных автоматизированных систем управления, связанных с автоматизированным вводом, хранением, обработкой и выводом информации, проблема ее защиты приобретает еще большее значение.

К настоящему времени и в самом человеческом обществе, и в технологии обработки данных и документов произошли большие изменения, которые повлияли на саму суть проблемы защиты информации.

Каждый руководитель, предприниматель (деловой человек) выступает за порядок, базирующийся на экономической и организационной основах, а не на эмоциях. А это может дать система, где каждому нормальному здоровому человеку были бы предоставлены возможности приложить свои способности за достойную плату. Формы управления слепо копироваться не должны, но основы управления (системы управления) должны быть заложены в организационно-штатные структуры и функциональные обязанности должностных лиц (должностные инструкции).

Решающим фактором в управлении выступает человек во всей сложности своей социальной сущности и психологии.

Как научная дисциплина «Документоведение» тесно связано с архивоведением, информатикой, источниковедением, теорией управления, правовыми дисциплинами и др.

На развитие документоведения и документационного обеспечения управления значительное влияние оказывает теория управления, поскольку в документах отражаются функции управления. В документах фиксируется вся многогранная деятельность учреждений, организаций и предприятий.

К настоящему времени создана определенная нормативно-методическая база, представляющая собой совокупность законов, нормативных правовых актов и методических документов, регламентирующих основные процессы создания, обработки, хранения и использования документов.

Она включает:

— законодательные акты РФ в сфере информации и документации: Федеральные законы от 27.07.2006 № 149-ФЗ «Об информации,

информационных технологиях и о защите информации», от 06.04.2011 № 63-ФЗ «Об электронной подписи», от 22.10.2004 № 125-ФЗ «Об архивном деле в Российской Федерации», Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне» и др.;

— указы и распоряжения Президента РФ, постановления и распоряжения Правительства РФ (в том числе постановление Правительства РФ от 15.06.2009 № 477 «Об утверждении Правил делопроизводства в федеральных органах исполнительной власти»);

— правовые акты федеральных органов исполнительной власти и субъектов РФ;

— правовые акты нормативного и инструктивного характера, методические документы по делопроизводству учреждений, организаций, предприятий;

— ГОСТ на документацию, унифицированные системы документации (УСД), Общероссийские классификаторы технико-экономической и социальной информации и некоторые другие документы нормативно-правового и методического характера.

Рациональная организация документных работ способствует совершенствованию управленческой деятельности особенно в сферах правового обеспечения национальной безопасности и правоохранительной деятельности.

Раздел I. Документоведение, документ и система документов

Глава 1. Документ и его место в системе управления

1.1. Понятия «документ», «информация»

Подготовка по направлению «Документоведение и архивоведение» сегодня открыта во многих вузах, получаемая выпускниками квалификации «Документовед». Вдумаемся в эти названия. Ключевым, базовым понятием в них выступает слово «документ». Документоведение и документовед — т.е. всеведающий, знающий о документе. Что же это такое «документ», о котором надо так много знать, что необходимо учиться в высшем учебном заведении.

Документ — явление сложное и древнее. Его появление, эволюция, функции документа, требования, предъявляемые к его составлению и оформлению, а также порядок работы с ним изучаются в цикле общепрофессиональных дисциплин. В рамках данного материала остановимся лишь на значении документа, чтобы понять, почему он заслуживает такого углубленного изучения. Понятие «документ» имеет много определений, их можно найти в каждом словаре и в энциклопедии. Анализу и сопоставлению этих определений посвящаются специальные занятия в курсе «Документоведение». И хотя определения будут отличаться в зависимости от акцента на различные свойства документа и его функции (назначение), в них одно общее — *они рассматривают документ как носитель информации, как результат ее запечатления*. Таким образом, документ неразрывно связан с информацией.

Понятие *информация* не менее сложно, чем документ, и в его определении также много вариантов. Пока для целей введения в специальность ограничимся определением, данным в Федеральном законе «Об информации, информационных технологиях и о защите информации». В нем информация определяется как «сведения (сообщения, данные) независимо от формы их представления». Естественная потребность человека — сообщить другим о том, что он узнал, видел, о чем думал.

Информация побуждает человека к размышлению, к осмыслению событий, фактов, к поступкам, действиям. Можно сказать, что информация является побудителем к любому действию. Только на базе информации, узнав о чем-либо, принимается решение что-то предпринять, сделать, куда-то отправиться и т.д.

Всякое сообщество может существовать, только обмениваясь информацией. Лишь располагая своевременно полученной и достаточной информацией можно принять правильное решение и выиграть сражение, захватить власть, получить прибыль. Шпионаж — это тоже добыча информации о противнике или конкуренте, чтобы на ее основе предпринять какие-либо предупреждающие действия. Не случайно у немцев существует поговорка: кто владеет информацией, тот владеет ситуацией, тот и король.

В настоящее время мир переживает информационный бум, что напрямую связано с развитием человечества и научно-технической революцией, изменившей способы фиксации и передачи информации и средства связи.

XXI век назван веком информатизации, а информация рассматривается как стратегический ресурс. Давно известны такие понятия, как ресурсы полезных ископаемых, трудовые ресурсы, финансовые ресурсы, а во второй половине XX в. появляется понятие *информационные ресурсы*. Но информация часто нуждается в сохранении, чтобы к ней можно было обратиться спустя какое-то время, и в передаче ее на расстояние. Поэтому человек ищет способ закрепить информацию для передачи во времени и пространстве. Так появляется документ.

Документ, зафиксировав (отобразив) информацию, тем самым обеспечивает ее сохранение и накопление, возможность передачи другому лицу, многократное использование, возвращение к информации во времени.

1.2. Способы документирования

Способы фиксации информации, т.е. способы документирования (документирование определяется стандартом на термины и определения как запись информации на различных носителях по установленным правилам) в течение многих веков изменялись и обогащались. Проходят эволюцию и материалы, на которых можно было бы на-

дежно закрепить информацию и сделать ее доступной для многих. В частности, законы должны знать все и поэтому в древности они высекались на камне.

Например, в XVIII в. до н.э. вавилонские законы царя Хаммурапи были высечены на каменном столбе высотой 2,25 м. Деяния египетских фараонов рисовались красной краской или высекались иероглифами на стенах пирамид. Для оперативной переписки применяли глиняные и деревянные дощечки, папирус, пергамент. Затем появляется бумага, а с XIX в. начинают быстро развиваться новые носители информации — фото-, фоно-, кинодокументы, в XX в. появляются магнитные ленты, цифровые носители информации.

Изучению способов документирования и материалов для фиксации информации от рукописного текста до электронного документа, включая фото-, фоно-, кино- и техническое документирование, посвящены специальные разделы курса «Документоведение». Особенно эти знания нужны при применении новейших информационных технологий.

Документ сопровождает человека от рождения до смерти и в нем фиксируются важнейшие события всей его жизни: рождение, окончание школы, получение специального среднего и высшего образования, вступление в брак и т.д. В далеком прошлом документ появляется, прежде всего, для того, чтобы закрепить, подтвердить право отдельного лица, семьи, рода на землю, какое-то имущество, право на власть и т.д.

Документ стал нужен для учета скота, денег, других ценностей, для передачи распоряжений правителя. Наличие или отсутствие какого-либо документа может изменить всю жизнь человека. Еще большую роль документ играет в жизни общества, закрепляя и отражая в законах порядок организации и управления государством, правила поведения людей, порядок их взаимоотношений, принятую мораль и т.д. Таким образом, документ может выполнять много функций, иметь различные назначения. Функции документа нуждаются в детальном изучении, им посвящается раздел в курсе «Документоведение».

При появлении управляющих и управляемых структур возникает потребность передать управленческое решение и отчитаться в его выполнении. Конечно, возможны и устные поручения, но слово крат-

ковременно, может быть быстро забыто, не так понято и передано. Если же вопрос касается передачи права на землю, дарения или дачи каких-либо привилегий, то получающий их, конечно, хочет иметь письменные подтверждения этих прав или привилегий, закрепления их, возможность предъявить другим, передать потомкам. Первоначально в документах закрепляются лишь отдельные события, факты, и мы говорим об отдельных актах документирования. Но с появлением и развитием государства функции управления усложняются. Уже не отдельный человек выполняет поручения правителя, а сначала группа людей, а затем специально созданный аппарат, который занимается определенным направлением управленческой деятельности, например, дипломатическим, учетным, управляет конкретной территорией и т.д. Устанавливаются информационные связи, которые закрепляются в документах. *Вся управленческая деятельность обязательно документируется.*

Как носитель информации документ выступает в качестве постоянного элемента внутренней организации любого учреждения, предприятия, фирмы, обеспечивая взаимодействие их частей. Информация является основанием для принятия управленческих решений, служит доказательством их исполнения и источником для обобщений, а также материалом для справочно-поисковой работы. *В управленческой деятельности документ выступает и как предмет труда, и как результат труда, так как принятое решение записывают, закрепляют в документе.*

Но управленческие взаимосвязи сложны и формы управленческой деятельности выражаются посредством соответствующих взаимосвязанных документов: планирование — посредством подготовки различных планов, учет — в виде составления и обработки статистической, бухгалтерской и оперативно-технической документации; структурирование — в виде издания инструкций, методических указаний; контроль — путем сбора сведений в письменном виде и т.д.

Таким образом, документация, будучи тесно связана со всеми формами управленческой деятельности, отражает эту деятельность и в то же время используется аппаратом управления в качестве способа и средства реализации возложенных на него функций. Кроме того, документирование во многих случаях является обязательным, предписывается законом и актами государственного управления.

Федеральный закон «Об информации, информационных технологиях и о защите информации» в ст. 11 указывает, что в федеральных органах исполнительной власти документирование информации осуществляется в порядке, устанавливаемом Правительством РФ. Этот порядок закреплён в Правилах делопроизводства в федеральных органах исполнительной власти, утвержденных постановлением Правительства РФ от 15.06.2009 № 477

Федеральный закон от 06.12.2011 № 402-ФЗ «О бухгалтерском учете», указав, что бухгалтерский учет осуществляется путем «сплошного, непрерывного и документального учета всех хозяйственных операций», специальную статью (ст. 9) посвящает составлению первичных учетных документов. В ней подчеркивается, что все хозяйственные операции, проводимые организацией, должны оформляться оправдательными документами. Эти документы служат первичными учетными документами, на основании которых ведется бухгалтерский учет.

Таким образом, документ является одним из *средств укрепления законности и контроля*.

Чрезвычайно важна для управленческой деятельности *юридическая сила документов*, так как они служат способом доказательства заключенной в них информации и представляют одну из форм выражения права.

Определенные документы, например, законодательно-правовые акты представительных и распорядительных органов, судебные, прокурорские, нотариальные и арбитражные акты, договорная документация, изначально обладают юридической функцией, устанавливая, закрепляя и изменяя правовые нормы и правоотношения или прекращая их действие. Другие документы наделяются юридической функцией в случае использования их как доказательства в суде, органах следствия и прокуратуры, нотариате, арбитраже и др. Но для того, чтобы документ выполнил функцию доказательства он должен быть оформлен надлежащим образом.

1.3. Система документации и управление

Однако один документ — это единичный акт документирования. Но деятельность учреждения оформляется и отражается совокупно-

стью целого ряда определенным образом взаимодействующих документов, обычно соответствующих функциям управления. «Совокупность документов, взаимосвязанных по признакам происхождения, назначения, вида, сферы деятельности, единых требований к их оформлению» составляет систему документации (ГОСТ Р 7.0.8—2013 СИБИД. Делопроизводство и архивное дело. Термины и определения).

Ряд функций управления является типовым, присущим любому управленческому аппарату. К таким функциям относятся, например, прогнозирование и планирование, организационно-распорядительная деятельность, учет и отчетность, финансирование, материально-техническое обеспечение и др. Эти функции отражаются в документах, общих для всех учреждений, фирм.

Можно выделить функциональные системы документации, имеющие межотраслевое значение, но можно рассматривать и отраслевую систему документации в целом. В ней найдет отражение специфика той или иной сферы деятельности.

Некоторые системы документации будут являться предметом отдельного изучения в процессе подготовки документоведа, например бухгалтерская, статистическая, таможенная и т.д.

Подавляющее количество документов создается именно в сфере управления, где все документы надо не только составить и оформить или получить извне, но и учесть, передать по назначению, проконтролировать исполнение, сохранить, определить срок его дальнейшего хранения, передать в архив или уничтожить в соответствии с установленными правилами. Сегодня многие работы по составлению и оформлению документов, их обработке и хранению проводятся с внедрением компьютерных технологий и требуют специальных знаний и умений. Таким образом, мы подошли ко второй части названия нашей специальности — документационное обеспечение управления. Специалист готовится к работе именно в сфере управления, так как информационные потоки там наиболее крупные и нуждаются в организации.

Но фиксируют информацию, имеющую официальный характер, не как попало. От документа требуется подтверждение его подлинности. Он сразу должен иметь юридическую силу. Поэтому и документ с древнейших времен составляют по особым правилам, первоначаль-

но выработанным традициями, а затем установленными нормативными актами.

В нашем государстве документы, сохранившиеся от периода до образования централизованного государства (IX—XV вв.) — договора, жалованные, ссудные, вкладные и т.п. грамоты и другие документы, показывают, что их составление уже тогда требовало определенных навыков, умения. Их не мог составить любой человек. В Судебнике 1550 г. и Соборном уложении 1649 г. имеются статьи, посвященные порядку составления документов.

В процессе становления и укрепления централизованного государства складывается единая система центральных и местных правительственных учреждений, выполнявших административные, военные, финансовые, судебные и другие функции. Эти органы были связаны с высшим государственным органом и между собой. Они постоянно обменивались документами: от вышестоящих к нижестоящим, от нижестоящих к вышестоящим и между равностоящими. Здесь уже складываются определенные правила не только по оформлению документов, но и работе с ними.

В XVI в. слово *дело* начинает употребляться как собрание документов, относящихся к какому-либо делу, вопросу. Впервые в этом понятии слово «дело» зафиксировано в документах 1584 г. (Словарь русского языка (XI—XVII вв.). — Вып. 4. — М. : Институт русского языка АН СССР, 1977. — С. 207).

В XVII в. первоначально в устной речи появляется термин «дело-производство», означающий сам процесс решения (производство) дела, «дело производить», решать вопрос, с XVIII в. термин «дело-производство» начинает широко применяться.

XVIII век приносит крупные перемены в сферу управления. Государство растет, расширяется. Петр I, побывав за границей, внедряет зарубежный опыт построения и работы госаппарата в России. Новые органы власти и управления должны работать более оперативно и, следовательно, увеличивается поток документов, фиксирующих и отражающих их деятельность. Выделяются специальные структурные подразделения, регулирующие документопотоки — канцелярии. Процесс документирования и работы с документами начинает законодательно регулироваться, и первым таким документом считается Генеральный регламент 1720 г., а в XIX в. все процессы документи-

рования и работы с документами скрупулезно расписаны в нормативных актах.

Развитие человечества объективно сопровождает рост объемов информации и ее носителей — документов. Естественно, что работа с ними требует больших трудозатрат и привлечения все большего количества людей, занятых в этой сфере. Резкое увеличение объемов документов начинает отчетливо прослеживаться в XIX в. и именно в это время изобретаются новые средства связи — телеграф, затем телефон, радио, внедряются средства размножения документов, а с конца XIX в. начинается применение пишущих машинок. Резко меняется внешний вид документа и технология работы с ним.

XX век приносит коренные изменения в организацию труда. Возникает понятие «научная организация труда» — НОТ, которое касается и сферы управления и в первую очередь — делопроизводства. Согласно НОТ всякую работу надо поставить наилучшим образом, выполнять ее легче, быстрее и качественнее. В 1920-е гг. возникают первые оргпроектные работы по документационному обеспечению управленческой деятельности, внедряющие в аппарат управления различные средства механизации.

Но настоящей революцией в сфере управления можно считать последнюю четверть XX в. — внедрение электронно-вычислительных машин. Они внесли радикальные изменения в процесс создания, обработки и хранения документов. Требования к структурным подразделениям и их работникам, занятым в сфере информационно-документационного обеспечения управления, резко возросли.

Таким образом, мы установили, что с развитием общества постоянно усложняется процесс управления и приходится решать все более сложные комплексы взаимоувязанных задач. Их решение зиждется на информации об управляемых объектах, носителем которой выступает документ. Международный стандарт Р ИСО 15489-1—2007 «Управление документами. Общие требования» и определяет документ как «зафиксированная на материальном носителе идентифицируемая информация, созданная, полученная и сохраняемая организацией или физическим лицом в качестве доказательств при подтверждении правовых обязательств или деловой деятельности». Параллельно с усложнением процесса управления увеличиваются и усложняются задачи служб, работающих с документами, и все большие требования предъявляются к лицам, занимающимся этим трудом.

Но и с самого начала появления официального документа, его составление, оформление, хранение требовало специальных знаний. Эту работу всегда могли выполнять только профессионалы.

Глава 2. Информационно-документационное обеспечение работы аппарата управления

2.1. Основные виды документной деятельности

На ранних этапах становления и развития сферы управления, науки, техники, равно как и других отраслей человеческой деятельности, работа с документами входила в число вспомогательных операций для лиц, занятых в этих сферах. Но постепенно объем подобного рода операций увеличился настолько, что вызвал необходимость выделения специальных профессиональных групп для их выполнения. В результате работа, связанная с созданием, обработкой, хранением, распространением документов, стала обособляться в отдельную отрасль профессиональной документной деятельности. Так появились делопроизводители, библиотекари, переводчики, архивариусы и многие другие подобного рода профессии.

Со временем произошла институционализация информационно-документационной сферы. Появился целый ряд специальных социальных институтов, занимающихся исключительно упорядочением информационного пространства, оптимизацией и направлением движения информационных потоков, обеспечением сохранности накопленных информационных ресурсов или, иначе говоря, созданием, распространением, хранением, поиском, организацией использования документов.

На современном этапе документная деятельность представляет собой сложно-структурированную систему.

В ней выделяют четыре основных направления:

— непосредственная работа с документами, осуществляемая практическими сотрудниками (делопроизводителями, секретарями, архивистами, библиотекарями и т.д.) на предприятиях, в учреждениях, организациях;

— административно-управленческая деятельность, регулирующая работу документоведов-практиков. Ею занимаются руководители соответствующих организаций, учреждений, предприятий, а также руководители их специализированных структурных подразделений (общие отделы, канцелярии, отделы кадров и т.п.);

— научная деятельность, ориентированная на разработку теоретических проблем и рационализацию практики работы с документами.

Ее осуществляют, главным образом, ученые вузов, работающие на кафедрах документоведческого профиля, а также сотрудники специализированных научно-исследовательских институтов (например, ВНИИДАД), ведущие специалисты крупных архивов, библиотек, центров научно-технической информации;

— информационно-методическая деятельность, направленная на внедрение в практику результатов научных исследований и передового опыта работы с документами.

Она выполняется, в частности, сотрудниками научно-методических отделов архивов, библиотек. Важное место в этой работе занимают специализированные журналы документоведческого профиля («Делопроизводство», «Секретарское дело» и др.).

Документная деятельность включает всю совокупность действий, связанных с документом от момента его создания до утилизации или организации постоянного хранения и дальнейшего использования.

Важнейшими видами документной деятельности являются:

- производство документов;
- обработка документов;
- хранение документов;
- поиск документов;
- использование документов.

В основе системы организации и технологии работы с документами лежат научные принципы и методы, а также огромный практический опыт, накопленный за многие сотни лет документной деятельности в различных сферах и разных странах. Это обусловило формирование и развитие не только специализированных учреждений, учебных заведений соответствующих профессий, специальностей и специализаций, но и появление целого ряда прикладных документоведческих дисциплин, ориентированных на разработку оптимальных методов работы с теми или иными конкретными видами документов и системами документации.

2.2. Информация в управленческой деятельности

Под *управленческой информацией* понимается совокупность сведений о процессах, протекающих внутри организации и ее окружении, которые служат основой принятия управленческих решений.

Управление любым предприятием — это информационный процесс, в котором информация принимается, обрабатывается, вырабатывается решение, решение доводится до исполнителей, действия которых контролируются (рис. 2.1).

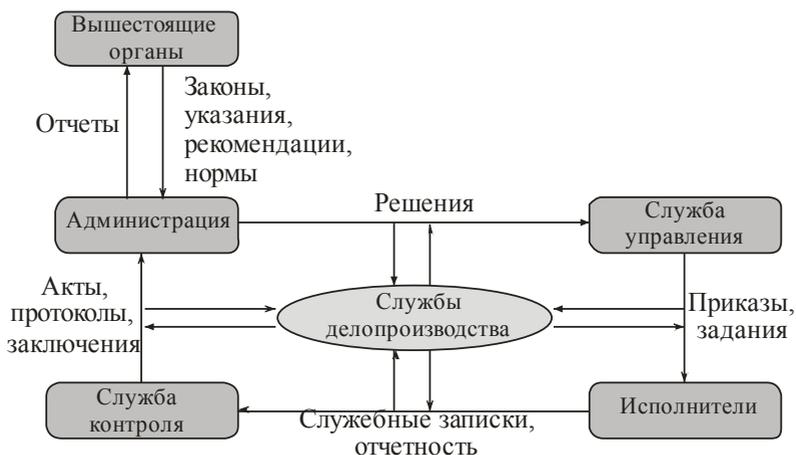


Рис. 2.1. Общая структура документационного обеспечения управления

Процесс организации работы с документами, включая их создание, регистрацию, контроль, продвижение, систематизацию и хранение, называют делопроизводством.

Информация может быть классифицирована по ряду позиций, в частности:

— *по назначению* (одноцелевая, связана с решением одной конкретной проблемы; многоцелевая используется при решении нескольких разнообразных проблем);

— *по возможности хранения* (фиксируемая информация может храниться практически бесконечно, не подвергаясь при этом искажению, о чем свидетельствуют наскальные надписи и рисунки, не фиксируемая информация используется в момент получения: она также

может храниться некоторое время, но при этом постепенно искажается и исчезает);

— *по степени готовности* для использования (первичная информация представляет собой совокупность полученных непосредственно из источника и систематизированных данных, содержащих много лишнего и ненужного; промежуточная информация состоит из сведений, прошедших процессы предварительной «очистки» и систематизации, позволяющих решить вопрос о конкретных направлениях и способах их дальнейшего применения; конечная информация дает возможность принимать обоснованные управленческие решения);

— *по полноте* информация может быть частичной или комплексной (последняя дает всесторонние исчерпывающие сведения об объекте и возможность непосредственно принимать любые решения; первая на практике может использоваться только в совокупности с другой информацией);

— *по степени надежности* информацию можно разделить на достоверную и вероятностную (вероятностный характер может быть обусловлен принципиальной невозможностью получить от существующего источника надежные сведения, поскольку имеющиеся методы не позволяют этого сделать; неизбежными искажениями при их передаче, особенно в условиях иерархии управленческой структуры; заведомым распространением изначально ложных сведений).

Информация может быть также классифицирована *по объему, источникам, возрасту, способам передачи и распространения.*

Существующие на сегодняшний день определения информации применительно к человеческому обществу выражаются в виде:

- *сведений*, запечатленных в организмах результатах отражения движения объектов материального мира и являющихся одной из форм проявления информации;

- *сообщений*, образуемых организмами в целях обмена сведениями с другими организмами, представляющих собой другую форму проявления информации.

Нетрудно заметить, что каждое из рассмотренных определений является всего лишь частным случаем одного из двух ранее рассмотренных классов информации: внутренней (структурной) и внешней (оперативной) соответственно.

Мы живем в информационном мире. Все, что мы видим, слышим, помним, знаем, переживаем, — это различные формы информации.

Совокупность сведений становится знанием лишь после интерпретации их субъектом и включения их в свою информационную модель окружающей действительности. Следовательно, информацию в широком смысле можно определить так же, как совокупность знаний об окружающем нас мире. В таком понимании информация является важнейшим ресурсом научно-технического и социально-экономического развития общества.

Под *информационными ресурсами* в широком смысле понимается вся накопленная человечеством информация об окружающей нас действительности, зафиксированная на материальных носителях, обеспечивающих ее хранение и передачу во времени и пространстве между различными потребителями для удовлетворения их потребностей.

В отличие от материального и энергетического ресурсов, информационный ресурс не уменьшается при потреблении, а накапливается со временем, сравнительно легко и просто с помощью технических средств обрабатывается, хранится и передается на значительные расстояния.

В зависимости от потребителя информационные ресурсы могут быть *государственными, информационными ресурсами предприятия (организации) и конкретного индивидуума.*

Информация, содержащаяся в государственных информационных системах, а также иные имеющиеся в распоряжении государственных органов сведения и документы являются государственными информационными ресурсами.

Под *информационной системой* понимается совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств. Таким образом, в жизни общества информация проявляется в форме сведений и сообщений (содержащих эти сведения), предназначенных для их доставки и обмена между элементами социума, которые при этом вступают в информационные отношения.

Под *информационными отношениями* понимаются регулируемые правом общественные отношения, возникающие в процессе взаимодействия субъектов в целях удовлетворения их интересов в обладании необходимой информацией, передаче части имеющейся информации другим субъектам, а также в сохранении в тайне оставшейся части информации.

Интересы, возникающие в социуме и связанные с информацией, подразделяются на три основные группы:

1. *Интересы человека* — обуславливаются необходимостью адаптации к условиям существования в природной и социальной среде и заключаются в обладании требуемой для этого информацией, обмене информацией с другими людьми и сохранении в неизвестности для других людей части имеющейся информации. Последнее обстоятельство обеспечивает определенную степень независимости человека от других лиц, повышает комфортность его существования;

2. *Интересы общества* — обуславливаются необходимостью поддержания общественной стабильности, обеспечения лучших условий жизни своих членов (граждан) и безопасности социального развития. Они заключаются в обладании институциональными социальными образованиями требуемой информацией, обмене информацией между членами социальных образований, сохранении в неизвестности для других лиц части информации, которой обладают члены данного социального образования. Это повышает устойчивость функционирования данного социального образования в условиях существования часто встречающегося конфликта его интересов с интересами других социальных образований;

3. *Интересы государства* — обуславливаются необходимостью эффективного выполнения функций по управлению делами общества, обеспечению безопасности его существования и развития. Эти интересы заключаются в обладании государственными органами определенной информацией, передаче части этой информации гражданам, социальным образованиям и сохранении в тайне для неуполномоченных лиц информации, разглашение которой может нанести вред выполнению функций государства.

Информация как объект правовых отношений в социуме классифицируется следующим образом:

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

2. Информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию,

доступ к которой ограничен федеральными законами (информация ограниченного доступа).

3. Информация в зависимости от порядка ее предоставления или распространения подразделяется:

- на свободно распространяемую;
- предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;
- подлежащую предоставлению или распространению в соответствии с федеральными законами;
- запрещенную к распространению в Российской Федерации или распространение которой ограничено.

Кроме того, законодательством РФ могут быть установлены виды информации в зависимости от ее содержания или обладателя.

Поскольку регулируемые правом общественные отношения выражаются через информационные посредством фиксации юридических фактов в виде сообщений, именуемых документами, то предметом нашего дальнейшего рассмотрения является документ как частный случай сообщения.

Существующее определение: документ — это зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать (где реквизит документа — обязательный элемент оформления официального документа).

Это определение недостаточно полно и адекватно существующим реалиям, поскольку за его рамками остались некоторые весьма важные свойства документа как сообщения.

При разговоре по телефону сообщением является непрерывное изменение во времени звукового давления, отображающее не только содержание, но и интонацию, тембр, ритм и иные свойства речи. При передаче движущихся изображений в телевизионных системах сообщение представляет собой изменение во времени яркости элементов изображения.

Таким образом, сообщение представляет собой кодированный эквивалент события, зафиксированный источником информации и выраженный с помощью последовательности условных физических символов (алфавита), образующих некоторую упорядоченную совокупность.

Передача сообщений (следовательно, и информации) на расстояние осуществляется с помощью какого-либо материального носителя

(бумаги, магнитной ленты и т.д.) или физического процесса (звуковых или электромагнитных волн, электрического тока, являющихся также материальными носителями). Физический процесс, отображающий (несущий) передаваемое сообщение, называется *сигналом*.

Следовательно, в настоящее время существуют два принципиально отличных (относительно системы восприятия человека) вида носителей сообщения (документа): предмет и процесс — и соответственно два направления защиты: *традиционная защита носителя сообщения* (документа) и новое направление — *защита информационных технологий как процессов* обработки электронных сообщений (документов).

Главной характеристикой предмета в качестве носителя сообщения (документа) является неизменность его параметров в течение длительного времени, что позволяет ему успешно выполнять функцию транспортировки во времени, т.е. хранения сообщения (документа). При передаче и обработке электронного сообщения (документа) оно существует в форме процесса, что позволяет ему более успешно выполнять функцию транспортировки информации в пространстве.

Поскольку технологии изготовления сообщений (документов) относятся к информационным, приведем существующее определение этого понятия.

Информационные технологии — процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов. Следовательно, в процессе изготовления электронного сообщения (документа) участвуют следующие объекты:

- компьютеры;
- данные (другие электронные средства);
- сетевые (телекоммуникационные) средства;
- информационные технологии.

Коренным отличием новых (цифровых, электронных) информационных технологий от традиционных аналоговых является то, что при изготовлении электронного сообщения (документа) отсутствует его привязка к конкретному (уникальному) носителю.

В первом приближении переменные, функцией которых является сообщение, могут быть заданы следующим далеко не полным перечнем:

1. Целевая направленность сведений, отраженных в сообщении, определяющая область их применения:

- научно-техническая информация;
- экономическая информация;
- управленческая информация;
- технологическая информация;
- производственная информация;
- юридическая информация;
- справочная информация;
- социальная информация;
- медицинская информация;
- прочая информация (в том числе художественная, религиозная, музыка, искусство, литература).

2. Содержание сообщения — различные сведения, отражаемые в сообщении и определяющие его прагматическую ценность.

3. Пространственно-временные характеристики сообщения — сведения о его местонахождении в определенный момент времени.

4. Языки (алфавиты, правила, способы, методы, алгоритмы, программы) преобразования информации (сведений и соответствующих им сообщений), в том числе при изменении носителя информации, устройств воспроизведения, фиксации, сбора, передачи, хранения, обработки, ввода-вывода сообщений:

- алфавит преобразования сведений в сообщения: буквы, цифры; символы иероглифических систем письменности;

- знаки — математические и химические, почтовые, картографические, железнодорожные и пароходные, метеорологические, астрономические, правил уличного движения, прочие системы специальных знаков и условных обозначений (знаки радиоэлектронных схем, технологических процессов и т.п.);

- преобразования: информации (сведений и сообщений) — кодирование-декодирование, транслитерация, ранскрибирование носителей, технических средств, алгоритмов, программ, правил.

5. Устройства, обеспечивающие взаимодействие источника и приемника при приеме-передаче сообщений, а также их обработку:

- средства ручной обработки;
- оргтехника;
- кинофототехника;

- электронно-вычислительная техника;
- средства и каналы связи.

6. Способ сохранения (закрепления, записи) информации:

- тексты;
- графика (рисунки, чертежи, карты, изображения, видеоматериалы и т.п.);
- представление пространственных данных;
- аудиоинформация;
- аудиовизуальная информация;
- цифровая и аналоговая информация, записываемая различной регистрирующей аппаратурой;
- перфорация (от азбуки для слепых до кодовых комбинаций на перфоносителях).

7. Носитель информации:

- бумажный носитель для традиционных средств полиграфии, печатающих устройств, перфоленга, перфокарта;
- магнитные и магнитооптические носители — магнитная лента, магнитные диски, СД ROM, оперативная память;
- микрофильмовые носители и кинофотоматериалы — микрофильмы, микрофиши, фотоносители, киноматериалы;
- устройства отображения — табло для алфавитно-цифровой информации, экраны, самописцы;
- сигналы — переносчики сообщений, передаваемых по линиям связи.

2.3. Управление документацией

В различных странах управление документацией организовано по-разному. Однако практика работы с документами, а также международные связи и рекомендации международных организаций (ЮНЕСКО, Международный совет архивов, ИСО и некоторые др.) обусловили ряд общих черт и тенденций.

Как правило, в развитых странах основные функции по управлению документацией выполняют соответствующие государственные органы. К примеру, управление документацией административного характера обычно тесно связано с архивными службами.

Можно выделить несколько уровней управления документацией.

В России на федеральном уровне это управление осуществляется Президентом РФ и Правительством РФ, определяющими единую государственную политику в сфере информации и документации (подтверждением чего является постановление Правительства РФ от 15 июня 2009 г. № 477). Однако применительно к конкретным документным ресурсам и сложным комплексам документированной информации (архивная, библиотечная, научно-техническая и др.) управление имеет свои особенности.

Так, непосредственное управление архивной документацией в Российской Федерации осуществляется архивными органами, возглавляемыми Росархивом при Минкультуры России в соответствии с Положением о Федеральном архивном агентстве, утвержденном постановлением Правительства РФ от 17.06.2004 № 290. Будучи федеральным органом исполнительной власти, Росархив выполняет функции по оказанию государственных услуг, управлению федеральным имуществом в сфере архивного дела, контролю за сохранностью, комплектованием и использованием документов Архивного фонда РФ. Он также осуществляет «согласование перечней документов, образующихся в процессе деятельности федеральных органов государственной власти и подведомственных им организаций, с указанием сроков их хранения, а также примерных номенклатур дел, инструкций по делопроизводству федеральных органов государственной власти».

Росархив выполняет свои функции непосредственно и через подведомственные ему организации, к числу которых относятся федеральные государственные архивы, центры хранения документации, научные учреждения (в частности, ВНИИДАД) и др. Он действует в контакте с другими федеральными органами исполнительной власти, органами исполнительной власти субъектов РФ, органами местного самоуправления, общественными объединениями и иными организациями. К примеру, плодотворным является его сотрудничество с органами стандартизации, метрологии и сертификации, осуществляющими государственное управление стандартизацией в РФ, в том числе в области документации. Росархив, в частности, осуществляет экспертизу проектов национальных стандартов в области архивного дела и документационного обеспечения управления (ДОУ).

На уровне субъектов РФ управление архивным делом осуществляется местными органами власти, в структуре которых имеются со-

ответствующие органы, которые разрабатывают и утверждают нормативно-методические документы, определяющие работу местных архивных служб.

На уровне муниципальных образований управление архивной документацией осуществляют органы местного самоуправления.

На уровне организации, учреждений, предприятий для управления документацией создаются специальные структурные подразделения — управления делами, канцелярии, общие отделы, либо эту работу выполняют секретари учреждения, структурного подразделения и т.п.

В управлении административной документацией важную роль играют органы ведомственного управления (т.е. все вышестоящие органы в отношении всех подчиненных им органов), осуществляющие функции по созданию ведомственных архивов, принимающие меры по организации работы с документами, утверждению инструкций по делопроизводству в системе подчиненных органов.

В последнее время в связи с широкомасштабным использованием новых информационных технологий управление документацией становится важнейшей органической частью управления информационными ресурсами организации — информационного менеджмента.

Таким образом, в организационной структуре управления документацией в нашей стране прослеживается как отраслевой, так и территориальный принцип. Вместе с тем отсутствует орган, который бы в полном объеме осуществлял управление документацией. В результате функции по государственному регулированию в сфере ДООУ в Российской Федерации рассредоточены и не скоординированы. Отсутствует также и закон, который бы регулировал весь комплекс вопросов по управлению документацией в стране.

Тем не менее к настоящему времени создана определенная нормативно-методическая база, представляющая собой совокупность законов, нормативных правовых актов и методических документов, регламентирующих основные процессы создания, обработки, хранения и использования документов.

Наблюдающийся комплексный подход к решению многих проблем российского общества благотворно сказывается и на информационно-документационной сфере.

Примером может служить утвержденная постановлением Правительства РФ от 28.01.2002 № 65 Федеральная целевая программа

«Электронная Россия (2002—2010 годы)». В результате реализации этой программы органы государственной власти и многие органы местного самоуправления (более половины городов с населением свыше 50 тыс. чел.) перешли к электронному документообороту и придали своим документам более открытый характер.

В 2001 г. разработан первый международный стандарт по управлению деловой документацией — ИСО 15489-2001 «Информация и документация. Управление документацией». Его появление обусловлено изменившимися реалиями в мире, формированием не только единого информационного, но также и экономического пространства, единого рынка целого ряда развитых стран, расширением деятельности транснациональных корпораций.

На основе ИСО 15489 в ряде стран мира осуществляется подготовка национальных стандартов по управлению деловой документацией. В 2007 г. в России был принят ГОСТ ИСО 15489-1—2007 «Управление документами. Общие требования (СИБИД)» — стандарт, идентичный международному ИСО 15489-2001.

2.4. Организация информационно-поисковых систем по документам учреждения

Поиск документов. Документированная информация практически не используется в месте своего возникновения и в момент создания. Более того, информация вообще не существует ни как субстанция, ни как функция состояния. Она реальна, объективна только как процесс, состоящий из различных стадий. Важную роль в этом процессе играют поиск и сбор нужной информации. В свою очередь, поиск документированной информации самым тесным образом связан с ее рассеянием в пространстве (по множеству источников) и во времени.

Проблема поиска необходимой информации является весьма актуальной в самых различных сферах человеческой деятельности: в науке, управлении, образовании и т.д.

По некоторым данным, разработчик или исследователь примерно половину своего рабочего времени тратит на эти цели. Отсюда вытекает важность и социальная значимость теоретических разработок и обобщения практики поиска необходимой документированной информации.

Алгоритм поиска заключается в последовательном обращении к источникам. Однако нужная информация крайне неравномерно сосредоточена (рассеяна) по различным источникам. Поэтому простой перебор всех источников, содержащих необходимую информацию, может привести к нерациональным затратам времени и средств. Увеличение полноты информации непосредственно связано с нарастанием трудностей в ее поиске.

Большие затруднения вызывает также и поиск документированной информации, рассеянной во времени. При этом необходимо учитывать фактор ее старения, которое зависит от многих обстоятельств. Старение проявляется в том, что постоянно возникают все новые документы, новые источники, содержащие более полную, точную, достоверную информацию. Поэтому с целью экономии времени и ресурсов оправдано первоочередное обращение именно к этим источникам.

Поиск информации, прежде всего научной, облегчают действующие в различных странах информационные центры, институты научной информации и другие учреждения, одновременно выполняющие также функции обработки и хранения документированной информации.

Непосредственный поиск документов в том или ином документном массиве представляет собой совокупность логических и технических операций. Он осуществляется в рамках информационно-поисковых комплексов (архивные описи, каталоги библиотек и архивов, компьютерные базы данных и т.п.), содержащих поисковые образы и адреса хранения документов. Для успешного поиска документов необходимо четкое закрепление места каждого документа в документном массиве и выделение поисковых признаков каждого из документов. Иначе говоря, необходима достаточно полная документографическая (библиографическая) картина того или иного комплекса документов.

Информационно-поисковые системы (ИПС) могут быть ручными (карточными) и автоматизированными (электронными).

В ручных ИПС поиск осуществляется по краткому формализованному описанию документа на карточке, т.е. по регистрационному номеру либо индексу дела по номенклатуре, архивному, либо библиотечному шифру и т.п. Систематизированное собрание карточек представляет собой картотеку. В текущем делопроизводстве, к при-

меру, создаются *регистрационные листки, карточки (карты)* (РКК). РКК в картотеке отделяются друг от друга разделителями с проставленными на них цифровыми, буквенными, буквенно-цифровыми шифрами. Примерами ручных ИПС могут быть также телефонный справочник, адресная книга, каталог изделий и т.п.

В ручных ИПС поиск возможен лишь по одному какому-либо признаку (реквизиту), являющемуся основным в данной поисковой системе, — по автору, адресату, содержанию и т.д.

В отличие от ручных, автоматизированные компьютерные ИПС позволяют совмещать несколько вариантов поиска документированной информации:

— по поисковому образу документа (осуществляется аналогично ручным карточным системам);

— по полному тексту документа (на основе формализации текста, перевода его в машиночитаемую форму);

— по гипертекстовым ссылкам (с учетом множества логических и ассоциативных взаимосвязей между документами).

Компьютерные ИПС позволяют в считанные секунды осуществлять поиск практически по любому реквизиту либо по совокупности реквизитов документа: по дате регистрации, номеру, автору, адресату, краткому содержанию, виду отправления (электронная почта, почтовое сообщение, факс), по резолюции, исполнителям, отметке о контроле, приложении и другим.

В зависимости от формы представления информации ИПС подразделяют:

— на документографические (производят поиск по поисковым образам документов, т.е. по индивидуальным кодам, которые присваиваются каждому документу и содержат информацию о его местонахождении. В частности, так ведется поиск книг по заказам читателей в крупных библиотеках).

— фактографические (помогают найти отдельные сведения, факты, содержащиеся в текстах документов и относящиеся к какой-либо предметной области);

— документно-фактографические занимают промежуточное положение между предыдущими (позволяют отыскать необходимые сведения со ссылкой на конкретный документ, в котором они содержатся).

Поиск документированной информации, как правило, состоит из нескольких последовательных этапов:

- составление поискового запроса;
- анализ и перевод его с естественного языка на язык формальных признаков документа (библиографического описания, классификационного индекса, перечня дескрипторов и т.д.), т.е. выражение на языке запросов используемой информационно-поисковой системы;
- выборка в соответствующем документном массиве всех документов, отвечающих данным формальным признакам (так называемых релевантных документов);
- выбор из числа найденных тех документов, которые соответствуют информационным потребностям реципиента (так называемых pertinentных документов).

В зависимости от местонахождения документированной информации (в текущем делопроизводстве, в архиве учреждения, в государственном архиве, в библиотеке и т.п.) поиск ее имеет свои особенности.

К примеру, поиск архивных документов начинается с установления фондообразователей, в деятельности которых могла возникнуть интересующая информация. Затем устанавливаются названия архивов, музеев, библиотек, в которых хранятся или могут храниться необходимые документы.

На третьем этапе поиск осуществляется уже на уровне конкретного архива, где выявляются названия и номера фондов, в которых отложились нужные документы. Затем он продолжается на уровне отдельного архивного фонда с целью установления номеров единиц хранения. Завершением поиска становится выявление нужного документа в рамках первичного комплекса, т.е. единицы хранения. В результате определяется архивный шифр документа, состоящий из названия архива, номера фонда, номера описи, номера дела по описи и номера листа.

В отличие от поиска в отдельно взятом документном массиве или в ограниченной совокупности таких ресурсов поиск документов в информационной среде, т.е. в неограниченной совокупности информационных ресурсов, имеет свои особенности.

В частности, в Интернете он осуществляется с помощью поисковых машин, а также посредством индексированных каталогов (рубри-

каторов), рейтингов и топов, метапоисковых систем и тематических списков ссылок, онлайн-энциклопедий и справочников. Наиболее популярными поисковыми системами в Рунете являются Яндекс и Рамблер. Среди западных поисковых систем выделяется Google.

Принцип работы поисковой машины заключается в том, что она по внутреннему каталогу (базе данных) ищет по ключевым словам, указанным в поле запроса, и выдает список ссылок, ранжированный по релевантности. С помощью метапоисковых систем можно вести поиск сразу в нескольких поисковых системах.

Скорость поиска и полнота найденной документированной информации, с использованием как традиционных, так и автоматизированных технологий, зависят от качества и уровня имеющихся классификационных схем документов.

Разработка оптимальных вариантов поиска документов осуществляется в рамках отдельных специальных документоведческих дисциплин, в частности, таких научно — практических направлений, как архивная эвристика, библиографическая эвристика. Большое внимание вопросам оптимизации поиска документированной информации уделяется в информатике.

Регистрация и индексация документов. Для обеспечения эффективного использования информации при принятии различного рода решений, предоставления в распоряжение специалистов всего массива информации по определенному вопросу в кратчайшее время в организации должна быть построена рациональная поисковая система.

Современная ИПС должна включать информацию обо всех документах, которыми располагает организация.

Основой построения поисковых систем является регистрация документов — фиксация факта создания или поступления документа путем проставления на нем даты и регистрационного индекса с последующим внесением необходимых сведений о документе в регистрационную базу данных (журнал, картотека, входной экраный формат или дело).

Главное назначение регистрации — придание документу юридической силы, подтверждение факта его создания или поступления. Так, пока приказ не зарегистрирован, он фактически не существует; если поступивший документ не зарегистрирован, организация не берет на себя ответственности за него, его нет, так как не подтвержден

факт его поступления. На базе регистрационных данных традиционно строится учет документов, поиск и контроль исполнения.

Вместе с тем, при существующей системе делопроизводства регистрируется от четверти до половины документов, остальные в организации не учитываются, а их поиск строится лишь на предположениях специалистов об их существовании и возможном месте хранения.

Индекс документа составляется в зависимости от принятого для каждого массива документов принципа формирования дел. Обязательным элементом индекса является порядковый регистрационный номер в пределах регистрируемого массива, как правило, за год. В комплексе с датой и названием он служит поисковым образцом документа и используется также для целей учета. Дополнения к порядковому номеру указывают место исполнения и хранения документа, принадлежность его к определенному вопросу, территории, периоду, лицу и т.д. и служат целям облегчения поиска.

Индексом документов, формируемых в дела только по названиям и авторам (бухгалтерские балансы, протоколы, наряды и др.), служит порядковый номер в пределах регистрируемого массива.

Индексом документов, формируемых в дела по вопросам, корреспондентам, территории (докладные записки, любая переписка, отзывы и др.), служит порядковый регистрационный номер, дополненный индексом по номенклатуре дел, который и определяет место хранения документа.

При необходимости выделения части документов из единого регистрационного массива возможно использование дополнительного буквенного индекса. Так, при регистрации приложений, заявлений и жалоб граждан порядковый регистрационный номер дополняется начальной буквой фамилии заявителя, например, И-221, К-212, А-213 и т.д.; при регистрации коллективных предложений, заявлений и жалоб проставляется только порядковый регистрационный номер; при регистрации приказов по вопросам управления кадрами порядковый номер дополняется буквой К.

Индекс документов, составленных несколькими организациями, образуется из порядковых регистрационных номеров, присвоенных в каждой организации-авторе, их последовательность определяется последовательностью указания авторов в оформляющей части документа.

При регистрации документа индекс, как и другие его регистрационные данные, переносится в регистрационные формы. Причем в регистрационных формах могут указываться и другие реквизиты (сведения), которые вносятся при первичной регистрации или заполняются в процессе исполнения документа.

В ИПС разрабатываются и используются различные классификационные справочники. Их набор зависит от принципов и правил ввода и вывода документной информации и базируется на комплексе регистрационных характеристик документа как в автоматизированной, так и традиционной поисковых системах.

В соответствии с регистрационными данными документа наибольшее распространение в ИПС находят следующие классификаторы:

- название документа — классификатор названий документов;
- автор (корреспондент) — классификатор корреспондентов;
- заголовок документов или его краткое содержание — классификатор вопросов деятельности организации;
- резолюция — классификатор резолюций;
- исполнитель — классификатор структурных подразделений и (или) конкретных исполнителей;
- отметка об исполнении — классификатор результатов исполнения документов (причин неисполнения);
- адрес хранения — номенклатура дел.

Помимо перечисленных, в конкретных ИПС могут составляться и другие классификаторы в зависимости от потребностей ввода и поиска документов и информации.

Для обеспечения информационной совместимости поисковых массивов рекомендуется централизованная разработка классификаторов в пределах одной отрасли, объединения или крупной организации.

Классификатор названий (видов) документов разрабатывается на основе всех документов, используемых в организации, как составляемых, так и получаемых. При формулировании названий (видов) документов необходимо использовать наименования унифицированных форм управленческих документов, вошедшие в Общероссийский классификатор управленческой документации (ОКУД), отраслевые унифицированные формы документов, основные положения Государственной системы документационного обеспечения управления (ГСДОУ).

Классификатор корреспондентов разрабатывается на основе перечня названий организаций, предприятий и учреждений, с которыми данная организация связана в своей деятельности. Состав и объем классификатора корреспондентов обычно зависит от принадлежности данной организации к определенной отрасли и уровня в системе управления, от вопросов основной деятельности, которые она решает в пределах своей компетенции.

Классификатор вопросов деятельности организации представляет собой перечень вопросов, входящих в компетенцию как организации в целом, так и ее структурных подразделений.

Классификатор разрабатывается на основе организационных и распорядительных документов, содержащих сведения о функциях, правах, обязанностях (уставы, положения об организации, положения о структурных подразделениях, приказы о распределении обязанностей между руководителями организации, планы, отчеты о деятельности и др.).

Классификатор структурных подразделений разрабатывается на основе утвержденной структуры, штатного расписания организаций, предприятий и учреждений.

В отрасли может создаваться типовой классификатор структурных подразделений для какой-либо группы однородных организаций (промышленные предприятия, научно— исследовательские институты и т.д.). Формулировки объектов в классификаторе структурных подразделений даются в соответствии с действующими нормативными документами.

При разработке в отрасли типового классификатора структурных подразделений учитывается наличие различных наименований аналогичных структурных подразделений. Для их формулировок используются наиболее распространенные названия с указанием возможных вариантов их толкования.

Систематизация объектов в классификаторе сохраняет последовательность наименований структурных подразделений, закрепленную в действующих нормативных документах (типовая структура, структура и штатная численность, штатное расписание). Отличие заключается лишь в том, что в классификаторе на первое место ставится служба ДОО (управления делами, канцелярии и т.д.). В классификаторе структурных подразделений включаются также общественные организации, общества, союзы.

Классификатор исполнителей или только ответственных исполнителей представляет собой перечень фамилий руководителей структурных подразделений, которые отвечают за исполнение документов, поручений. Фамилии в классификаторе перечисляются в последовательности, соответствующей перечислению наименований структурных подразделений в действующих нормативах (типовая или примерная структура, структура и штатная численность, штатное расписание). Для визуального отличия регистрируемых групп документов на регистрационные формы могут наноситься цветные маркировальные полосы по верхнему краю или по диагонали; ручные и механизированные регистрационные формы могут изготавливаться на бумаге различных цветов и светлых тонов.

Введение регистрационных журналов целесообразно для документов, в состав индекса которых входит только порядковый номер (пропуска, справки, дипломы и т.д.), или в случаях минимального объема документооборота (в структурных подразделениях). Журнал рекомендуется составлять из отдельных листов-бланков, что позволит заполнять их с помощью пишущей машины, принтера, других средств организационной техники и постепенно формировать сам журнал, в том числе с одновременным вводом информации в машинную память.

При использовании компьютерных технологий ввод сведений о документе в автоматизированную ИПС осуществляется непосредственно с документа на входной формат с помощью клавиатуры и других устройств ввода, например сканера. Одновременно может изготавливаться один экземпляр регистрационной формы на бумажном носителе в качестве страхового массива.

Ручной информационно-поисковый массив организации состоит из картотек, составленных из РКК и кодификационных тематических карточек и регистрационных журналов. Информационно-поисковые массивы обеспечивают оперативный поиск документов в контрольных и справочных целях и ведутся в местах регистрации документов. Как правило, составляются самостоятельные контрольно-справочные картотеки (информационные базы данных), картотеки по предложениям, заявлениям и жалобам, тематические (кодификационные) картотеки к ведомственным нормативным актам: приказам, решениям, поручениям.

Контрольно-справочные картотеки делятся на две части: по неисполненным и исполненным документам.

Первая часть картотеки служит для фиксации и поиска сведений о документах в процессе их исполнения и может выполнять контрольную функцию. Карточки в ней могут систематизироваться по исполнителям, структурным подразделениям, корреспондентам, срокам исполнения документов. По мере исполнения документов карточки с проставленными на них необходимыми отметками перемещаются из первой части картотеки в соответствующие разделы и рубрики второй части.

Вторая часть картотеки служит для поиска уже исполненных документов. Карточки в этой части картотеки могут систематизироваться по вопросам, корреспондентам, номенклатуре дел. Аналогично целесообразно формировать машинные базы данных.

В зависимости от объема документов, системы регистрации, контроля и задач поиска может вестись единая контрольно-справочная картотека (база данных) или несколько самостоятельных.

Автоматизированный информационно-поисковый массив ведется в соответствии с применяемым в местах регистрации документов программным обеспечением.

Выбор той или иной технологии ведения информационно-поисковой системы находится в компетенции руководства организации. Также признано нецелесообразным вводить единую, строго регламентированную форму входного формата информационно-поисковой системы. Вместе с тем необходимость обеспечения совместимости, понятности и полноты информационного содержания информационных систем не подлежит сомнению.

2.5. Основные функциональные системы документации в Российской Федерации

Система организационно-распорядительной документации (ОРД) это одна из важнейших систем документации. Она включает документы, фиксирующие решения самых различных вопросов управления и функционирования органов власти, учреждений, предприятий, организаций, отдельных должностных лиц.

Система ОРД состоит из двух подсистем, которые иногда рассматриваются в качестве самостоятельных систем документации:

— подсистема организационной (организационно-правовой) документации;

— подсистема распорядительной документации.

Подсистема организационно-правовой документации представляет собой совокупность документов, которые содержат правила, нормы, положения, устанавливающие статус организации, учреждения, предприятия, их компетенцию, структуру, штатную численность, содержание деятельности и т.д.

К организационно-правовым относятся такие виды документов, как:

— устав (регулирует деятельность организаций, учреждений, обществ, граждан, определяет их права и обязанности);

— положение об организации;

— штатное расписание;

— должностные инструкции, а также некоторые другие.

В подсистему распорядительной документации входят документы, регулирующие деятельность учреждений, организаций, предприятий: постановление, решение, приказ, распоряжение, указание и др.

Система плановой документации — фиксирует результаты планирования деятельности учреждения. Основные виды плановых документов: программа, план (перспективный, годовой и т.д.), а также график, смета расходов и некоторые другие.

Система информационно-справочной и информационно-аналитической документации. Документы этой системы выполняют подчиненную, обслуживающую роль по отношению к организационно-распорядительным документам.

К *информационно-справочной документации* относятся: протокол, докладная записка, объяснительная записка, заявление, служебное (деловое) письмо, телеграмма, факсограмма, телефонограмма, электронное сообщение и некоторые другие.

В состав *информационно-аналитических документов* входят: акт, справка, сводка, заключение, отзыв, перечень, список.

Система отчетной документации состоит из документов, содержащих сведения о результатах деятельности учреждения, организации, предприятия за определенный период времени. Основным видом документов этой системы — отчет. Широко используется также отчетный доклад.

Кадровая информационно-документационная система состоит из широкого круга документов, содержащих сведения о работниках предприятия, учреждения, организации, а также о деятельности самой кадровой службы. Наряду с организационными, распорядительными, информационно-справочными документами в ее состав входят также учетные документы (личная карточка, личный листок по учету кадров и др.).

Основную массу документов этой системы составляют персональные документы, к числу которых относятся:

— документы, выданные гражданам соответствующими государственными органами и юридически подтверждающие сведения, сообщенные гражданами о себе: паспорт, трудовая книжка, военный билет, диплом, свидетельство, аттестат, листок нетрудоспособности, медицинская справка и др.;

— документы, выдаваемые предприятием, учреждением, организацией своим работникам с целью подтверждения тех или иных правовых фактов: ходатайство, характеристика, справка (с подтверждением места работы, должности, заработной платы), удостоверение, пропуск, командировочное удостоверение и т.п.;

— документы, составляемые гражданами и направляемые в адрес администрации или профсоюзной организации с целью установления, изменения или прекращения трудовых или иных правоотношений: заявление, автобиография, резюме, объяснительная записка и др.;

— служебные документы, характеризующие деловые, профессиональные, личностные качества работника, но не предназначенные для передачи этому работнику: представление к назначению на должность, аттестационный лист, результаты тестирования и анкетирования, справка-объективка, докладные и служебные записки и т.п.

Кадровая информационно-документационная система имеет ответвления, которые представляют собой во многом самостоятельные специфические комплексы документов, выступающие по отношению к ней как подсистемы кадровой документации:

— документация по получению гражданином среднего и высшего образования, специальности, рабочей профессии (студенческий билет, зачетная книжка, академическая справка, диплом об окончании учебного заведения и т.п.);

— документация по присуждению ученых степеней и ученых званий (стенограмма заседания диссертационного совета, диплом доктора, кандидата наук; аттестат профессора, доцента и т.д.);

- документация по прохождению воинской службы;
- документация по повышению квалификации рабочих и служащих и т.д.

Система научно-исследовательской документации возникает в процессе проведения научных исследований и выполнения научно-технических разработок. К основным видам документов этой системы относятся:

- отчеты о результатах научно-исследовательских и опытно-конструкторских работ (НИОКР), опытно-технологических и экспериментально-проектных работ;
- отчеты, доклады о научных экспедициях, научных и технических командировках специалистов;
- программы научно-исследовательских работ;
- технико-экономические обоснования, обзоры, доклады, записки и др.;
- заключения, отзывы, рецензии, аннотации;
- монографии, диссертации и авторефераты к ним, другие научные публикации и отзывы на них;
- депонированные рукописи;
- первичная документация, образующаяся в ходе проведения научно-исследовательских работ (результаты анализов, журналы записей экспериментов и т.п.).

Система проектно-конструкторской документации. Во всех группах технической документации значительный удельный вес занимают чертежи, имеющие, в свою очередь, множество разновидностей, обусловленных:

- характером изображаемого предмета (чертежи предметов промышленного производства, объектов капитального строительства);
- степенью подробности изображения (генеральные планы, габаритные чертежи, собственно чертежи);
- полнотой изображения (чертежи общего вида, чертежи сборочных единиц, чертежи деталей) и др. В конструкторской документации, к примеру, чертеж детали, наряду со спецификациями (содержат сведения о составе сборочной единицы, комплекса или комплекта), является основным видом документов. Кроме того, существуют теоретические, монтажные, электромонтажные, упаковочные чертежи.

К важнейшим видам *технических документов* относятся также:

— схемы — документы, в которых основные части изделий и связи между ними показаны в виде условных изображений или обозначений;

— технические условия (ТУ) (содержат требования к изделию, его изготовлению, контролю и т.п.);

— пояснительные записки (содержат описание устройства и принципа действия разрабатываемого изделия, обоснование принятых при его разработке технических и технико-экономических решений);

— расчеты (содержат расчеты параметров и величин для обоснования конструктивных решений);

— инструкции и др.

К числу технических документов относятся рисунки, позволяющие рельефно представить предмет, особенно в тех случаях, когда изделие оценивается не только с технической, но и с художественной стороны (рисунки обоев, тканей, упаковочных коробок, а также архитектуры домов и т.д.).

Технические описания — содержат информацию об особенностях изделия, его основных характеристиках, назначении, устройстве, работе отдельных частей. К текстовым техническим документам относятся также пояснительные записки. В них приводятся сведения об устройстве и принципе работы изделия, дается обоснование технических и технико-экономических решений. К техническим описаниям и пояснительным запискам тесно примыкают паспорта изделий, расчеты, инструкции, схемы, графики и т.д.

Система технологической документации включает документы, являющиеся результатом документирования процесса труда. Они содержат информацию не о самих предметах, изделиях и т.п., а о способах их изготовления, сборки, строительства, эксплуатации, ремонта, организации производственного процесса. Основным технологическим документом является технологическая карта, содержащая подробную информацию обо всех производственных операциях, необходимых для изготовления изделия. Существует несколько разновидностей технологических карт:

— операционные (фиксируют одну производственную операцию);

— общие или маршрутные (показывают последовательность всех операций по изготовлению изделия или детали);

— цикловые (содержат информацию о группе операций, которые выполняются одним работником или в одном цехе);

— карты типовых технологических процессов (содержат сведения о средствах технологического оснащения и материальных нормативах для изготовления группы деталей и сборочных единиц).

Технологические карты содержат информацию о названии проводимых операций, о схеме установки и обработки изделия, об используемом оборудовании и инструментах, о режиме работы, времени обработки, стоимости каждой операции.

На предприятиях с непрерывным производственным циклом (химических, нефтеперерабатывающих, целлюлозно-бумажных и т.п.) важнейшим технологическим документом являются заводские регламенты, содержащие сведения об основных физико-химических процессах, их обеспечении для получения конечного продукта.

В систему технологической документации входят также графики работ цехов и бригад; технические условия на обработку деталей, сборку конструкций, строительство объектов и выполнение других производственных задач; прикладное программное обеспечение автоматизированных технологических процессов. К технологическим документам относится и эксплуатационная документация, регламентирующая порядок использования оборудования, содержащая правила техники безопасности и т.п.

В систему документов, связанных со сферой обслуживания и потребления, способствующую использованию технических средств, входят:

— паспорта технических изделий, руководства по эксплуатации;

— промышленные каталоги;

— прейскуранты (прайс-листы);

— рекламные чертежи, рисунки и т.д.

Система документов, фиксирующих информацию о природе как объекте человеческой деятельности. В составе этой многочисленной группы документов выделяют:

— картографическую документацию;

— инженерно-геологическую документацию;

— топографо-геодезическую документацию;

- почвенную документацию;
- гидрологическую документацию;
- аэрокосмосъемочную документацию.

К числу важнейших видов документов, входящих в эту систему, относятся карты, кадастры, аэрофотоснимки и др., имеющие, в свою очередь, многочисленные разновидности. В частности, карты (карта-чертеж поверхности Земли, небесного тела или звездного неба) могут быть общегеографическими и специальными (физико-географическими, социально-экономическими, историческими и т.п.). Они различаются по охвату территории, по масштабам, краскам и т.д.

Кадастры (содержат инвентаризацию природных ресурсов) представлены земельными, водными, ветровыми разновидностями.

Патентная документация и стандарты — составляют особую подсистему научно-технической документации. Особенность этих документов заключается, прежде всего, в том, что они имеют правовое значение.

Патентная документация представляет собой совокупность сведений о результатах научно-технической деятельности. Это документы, устанавливающие официальное признание наличия изобретений, промышленных образцов и полезных моделей. Они играют важную роль в процессе создания и освоения новой техники, являются одним из основных источников знаний о технической мысли, воплощенной в полезные модели и промышленные образцы, в современные технологии производства.

По мере ускорения научно-технического прогресса значение патентной информации возрастает. Связано это с принципиальной особенностью патентной документации, заключающейся в том, что более 80% содержащейся в ней информации не публикуется в каких-либо других источниках. Кроме того, эта информация прошла экспертную проверку на новизну и содержит практические рекомендации по ее реализации.

Исторически далекими предшественниками патентной документации являлись охранные грамоты и привилегии. В России это были жалованные грамоты — привилегии, которые предоставлялись, главным образом, монастырям и реже — отдельным лицам.

Основными видами патентной документации в нашей стране являются:

- авторское свидетельство;
- патент (от лат. *patens* — свидетельство, грамота).

До начала 1990-х гг. в СССР выдавались только авторские свидетельства. В настоящее время в Российской Федерации выдаются патенты — документы, удостоверяющие официальное признание чего-либо изобретением и право изобретателя на него. Их выдача осуществляется государственным патентным ведомством (Федеральная служба по интеллектуальной собственности, патентам и товарным знакам). Патент на изобретение в Российской Федерации действует в течение 20 лет. Он является объектом купли-продажи, т.е. товаром. Формой реализации имущественных прав, вытекающих из собственности на патент, является лицензия.

К патентной документации примыкают документы на товарные знаки. Важнейшим из них является свидетельство на товарный знак, удостоверяющее исключительное право владельца на соответствующий товарный знак.

Кроме рассмотренных, существует еще несколько десятков функциональных систем документации, состоящих из большого по объему и разнообразного по видовому составу количества документов, предназначенных удовлетворять соответствующие потребности общества.

Эти процессы, по мнению некоторых документоведов, объективно регулируются законом соответствия содержания, количества и видового состава документов потребностям общества.

2.6. Унифицированные системы документации

В последней трети XX в. с началом широкомасштабного использования новых информационных технологий, встал вопрос о необходимости унификации документированной информации, прежде всего, в сфере управления.

В начале 1980-х гг. в СССР фактически впервые в отечественной и зарубежной практике была создана система ДОУ с целью установления единого порядка документирования управленческой деятельности в масштабах государства. Она получила условное название ЕГСД-1973. В общей сложности в СССР было разработано 16 унифицированных систем документации (УСД).

УСД (согласно стандартизованному определению) — это «система документации, созданная по единым правилам и требованиям, со-

держащая информацию, необходимую для управления в определенной сфере деятельности» (ГОСТ Р 7.0.8—2013 СИБИБД. Делопроизводство и архивное дело. Термины и определения).

Главной целью создания УСД является установление рационального состава форм документов, а также совокупности взаимосвязанных технико-экономических и социальных показателей.

УСД способствует:

- сокращению затрат ручного труда в информационных процессах (в результате от человека требуется минимум усилий для заполнения или прочтения документов);

- широкому использованию персональных компьютеров, поскольку унифицированные формы документов удобны для электронной обработки (это достигается обеспечением программной, технической и информационной совместимости документов, разработкой соответствующих форм документов, классификаторов, словарей и т.п.);

- упорядочению информационных потоков;

- сокращению количества документов;

- дальнейшему совершенствованию культуры документа и в целом информационной культуры.

Все это вместе взятое позволяет повысить эффективность управления, так как достигается большая оперативность в получении качественной информации, снижается количество ошибок в документах, сокращаются ручные операции, повышается творческий характер управленческого труда, уменьшаются финансовые затраты на работу с документами.

Формой юридического закрепления результатов унификации является стандартизация. Поэтому УСД представляет собой комплекс государственных стандартов, определяющих, во-первых, основные положения унифицированной системы и, во-вторых, единую форму всех входящих в нее документов.

Ядро всей УСД составляют унифицированные формы документов. В зависимости от уровня утверждения они разделяются на следующие категории:

- общероссийские;

- отраслевые (ведомственные);

- формы документов субъектов РФ;

- формы документов объединений, предприятий, организаций.

Раздел II. Введение в конфиденциальное делопроизводство. Оформление и учет носителей конфиденциальной информации

Глава 3. Введение в организацию конфиденциального делопроизводства. Виды тайн и их классификация

3.1. Цели защиты конфиденциальной информации

Проблема защиты информации от несанкционированного доступа к ней возникла давно, с той поры, когда человеку по каким-либо причинам не хотелось делиться ею ни с кем или не с каждым человеком. С развитием человеческого общества, появлением частной собственности, государственного строя, борьбой за власть и дальнейшим расширением масштабов человеческой деятельности информация приобретает цену.

Ценной становится та информация, обладание которой позволит ее существующему и потенциальному владельцам получить какой-либо выигрыш: материальный, политический, военный и т.д. С переходом на использование технических средств связи *информация подвергается воздействию случайных процессов*: неисправностям и сбоям оборудования, ошибкам операторов и т.д., которые могут привести к ее разрушению, изменению на ложную, а также создать предпосылки к доступу к ней посторонних лиц. С дальнейшим усложнением и широким распространением технических средств связи возросли возможности для преднамеренного доступа к информации. Увеличение объемов информации, необходимость сосредоточения ее в единые *базы данных*, автоматизация обмена информацией на больших расстояниях, расширение круга пользователей и увеличение количества технических средств и связей в автоматизированных системах управления и обработки данных стало предпосылкой сложных автоматизированных систем.

Основными целями защиты информации, являются:

- предотвращение утечки, хищения, искажения, подделки информации;
- обеспечение безопасности личности, общества, государства;

- предотвращение несанкционированных действий по уничтожению, искажению, блокированию информации;
- защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных;
- сохранение государственной тайны, конфиденциальности документированной информации (рис. 3.1).



Рис. 3.1. Основные способы защиты конфиденциальной информации

Известно много способов несанкционированного доступа к информации в системе обработки данных: просмотр, копирование и подмена данных, ввод ложных программ, команд и сообщений, подключение с этой целью к линиям и каналам связи, использование отладочных и аварийных программ и устройств, прием сигналов побочного электромагнитного излучения и наводок информации, использование неисправностей и сбоев аппаратуры, ошибок операторов, программных ошибок. Для того чтобы *остановить нарушителя*, необходимо определить возможные точки приложения его усилий на авто-

матризированной системе обработки данных и установить на его пути систему соответствующих преград достаточной прочности.

Вместе с тем надо учитывать, что защите подлежит информация ограниченного доступа, а степень ее защиты определяет собственник этой информации. *Ответственность за выполнение мер защиты лежит не только на собственнике, но и на пользователе информации.*

Однако, основным способом похищения информации — была и остается банальная кража документов, содержащих коммерческую тайну или иные конфиденциальные сведения, или носителей, содержащих такие сведения. Вторым по распространенности способом, является внедрение «своих» людей на предприятие конкурента или их «вербовка».

Как видно из рис. 3.1, одна из важнейших ролей защиты информационных ресурсов компании находится в сфере принятия организационных решений. В любом случае, сохранение информации имеющей коммерческую ценность, в современных условиях жесткой конкурентной борьбы, представляется одной из важнейших задач любого руководителя, независимо от формы собственности организации. Важнейшая роль в этом вопросе принадлежит *должной организации конфиденциального делопроизводства.*

3.2. Два взгляда на организацию конфиденциального делопроизводства

Вопрос организации конфиденциального делопроизводства можно рассматривать с нескольких точек зрения, например как непосредственную организацию делопроизводства, т.е. аналог секретного делопроизводства в государственных органах, заключающегося исключительно в учете, хранении и проверки конфиденциальных документов, но можно рассматривать этот вопрос и значительно шире, так как его решение сложилось в крупных *коммерческих* организациях России.

Именно здесь сложилась практика подразумевать под организацией конфиденциального делопроизводства, не непосредственно сам процесс делопроизводства, а *комплексную задачу обеспечения безопасности информационных ресурсов компании.* Одним из важнейших

вопросов безопасности, является организационная защита информационных ресурсов компании, т.е. установление режима коммерческой тайны и обеспечение контроля за соблюдением такого режима.

В понятие установления и контроля за соблюдением режима коммерческой тайны на предприятии входит ряд вопросов, главные из них — *установление режима коммерческой тайны на предприятии*, разработка регламентирующих документов, основными из которых являются инструкция по конфиденциальному делопроизводству и перечень сведений, относящихся к коммерческой тайне и иным конфиденциальным сведениям, это вопросы учета, хранения, уничтожения конфиденциальных документов, вопросы проведения проверок соблюдения режима коммерческой тайны, вопросы проведения экспертиз передаваемых в другие организации и в средства массовой информации документов на предмет содержания в них сведений, содержащих коммерческую тайну и иные конфиденциальные сведения (рис. 3.2).



Рис. 3.2. Основные задачи конфиденциального делопроизводства

В наиболее крупных организациях конфиденциальное делопроизводство, как составной элемент обеспечения безопасности предприятия, возложен на Отделы защиты информационных ресурсов, организационно входящий в Управление информационной безопасности, которое в свою очередь входит в состав *службы безопасности* организации.

■ Структура взаимодействия подразделений обеспечивающих сохранение конфиденциальной информации



Рис. 3.3. Организационная структура взаимодействия подразделений, обеспечивающих сохранение конфиденциальной информации

3.3. Основные термины, понятия и определения

Перед тем как приступить непосредственно к вопросам конфиденциального делопроизводства, целесообразно определиться в основных терминах, понятиях и определениях, они зафиксированы в действующем законодательстве, прежде всего в Федеральном законе от 29.07.2004 № 98-ФЗ «О коммерческой тайне», а также в ряде других нормативных правовых документах.

Расшифруем некоторые из формулировок.

Персональные данные — любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес,

семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Служебная информация — любая не являющаяся общедоступной информация об эмитенте и выпущенных им эмиссионных ценных бумагах, которая ставит лиц, обладающих в силу своего служебного положения, трудовых обязанностей или договора, заключенного с эмитентом, такой информацией, в преимущественное положение по сравнению с другими субъектами рынка ценных бумаг.

Профессиональная тайна — общее название группы охраняемых законом тайн, необходимость соблюдения которых вытекает из доверительного характера отдельных профессий. К персональной тайне относятся, в частности, адвокатская тайна, врачебная тайна, нотариальная тайна. Ее следует отличать от служебной тайны, обязанность соблюдения которой вытекает из интересов службы.

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. Также коммерческой тайной именуют саму информацию, которая составляет коммерческую тайну, то есть, научно-техническую, технологическую, производственную, финансово-экономическую или иную информацию, в том числе составляющую секреты производства (ноу-хау), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны. Обладатель информации имеет право отнести ее к коммерческой тайне, если эта информация отвечает вышеуказанным критериям и не входит в перечень информации, которая не может составлять коммерческую тайну (ст. 5 Федерального закона «О коммерческой тайне»). Чтобы информация получила статус коммерческой тайны, ее обладатель должен исполнить установленные процедуры (составление перечня, нанесение грифа и некоторые другие). После получения статуса коммерческой тайны информация начинает охраняться законом.

За разглашение (умышленное или неосторожное), а также за незаконное использование информации, составляющей коммерческую

тайну, предусмотрена ответственность — дисциплинарная, гражданско-правовая, административная и уголовная.

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

Обладатель информации, составляющей коммерческую тайну, — лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании, ограничило доступ к этой информации и установило в отношении ее режим коммерческой тайны.

Доступ к информации, составляющей коммерческую тайну, — ознакомление определенных лиц с информацией, составляющей коммерческую тайну, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации;

Передача информации, составляющей коммерческую тайну, — 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.

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

Предоставление информации, составляющей коммерческую тайну, — передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем органам государственной власти, иным государственным органам, органам местного самоуправления в целях выполнения их функций.

Разглашение информации, составляющей коммерческую тайну, — действие или бездействие, в результате которых информация, со-

ставляющая 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.

Информационная безопасность — защищенность информации от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации.

Защита информации — это комплекс мероприятий, направленных на обеспечение информационной безопасности.

Гриф конфиденциальности — специальная отметка, свидетельствующая о принадлежности сведений к коммерческой или государственной тайне, проставляемая на носителе сведений и/или в сопроводительной документации.

Конфиденциальные сведения — (от лат. *confidentia* — доверие) сведения, составляющие коммерческую, производственную, личную тайну, не подлежащие широкому оглашению.

3.4. Виды тайн и их классификация

В законодательстве РФ на основе анализа более 90 законов сегодня упоминается более 30 видов тайн, которые выступают в виде прямых ограничений при реализации информационных прав и свобод. Если проанализировать подзаконные нормативные правовые акты, то перечень тайн будет пополнен и составит уже более 40 видов тайн.

В последние годы предпринималось несколько попыток их упорядочивания. Так в утратившем силу Федеральном законе от 20.02.1995 № 24-ФЗ «Об информации, информатизации и защите информации» (ст. 9) вся информация с ограниченным доступом была подразделена на государственную тайну и конфиденциальную информацию. При этом из многочисленных видов конфиденциальной информации в законе были упомянуты лишь личная, семейные тайны, персональные данные, тайна переписки, телефонных, почтовых, телеграфных и иных сообщений. Но уже в принятом в 1996 г. Федеральном законе «Об участии в международном информационном об-

мене» (ст. 8) государственная тайна определена как один из видов конфиденциальной информации. Эта путаница сохраняется во многих законах, где ссылки «на иные охраняемые секреты» предполагают продолжение списка видов информации с ограниченным доступом, и делает перечень открытым.

В настоящее время Перечень сведений конфиденциального характера утвержден Указом Президента РФ от 06.03.1997 № 188. Это:

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, сведения о лицах, в отношении которых в соответствии с Федеральными законами от 20.04.1995 № 45-ФЗ «О государственной защите судей, должностных лиц правоохранительных и контролирующих органов» и от 20.08.2004 № 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства», другими нормативными правовыми актами РФ принято решение о применении мер государственной защиты, а также сведения о мерах государственной защиты указанных лиц, если законодательством РФ такие сведения не отнесены к сведениям, составляющим государственную тайну;

3) служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом РФ и федеральными законами (служебная тайна);

4) сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ 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 РФ и федеральными законами (коммерческая тайна);

6) сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них;

7) сведения, содержащиеся в личных делах осужденных, а также сведения о принудительном исполнении судебных актов, актов других органов и должностных лиц, кроме сведений, которые являются общедоступными в соответствии с Федеральным законом от 02.10.2007 № 229-ФЗ «Об исполнительном производстве».

Глава 4. Структура защищенного документооборота

4.1. Структура защищенного документооборота

Всю информацию в фирме (организации) можно разделить на две большие группы: открытую; с ограниченным доступом (рис. 4.1).



Рис. 4.1. Виды информации и документов

В свою очередь информация с ограниченным доступом может быть: государственной тайной; конфиденциальной информацией. А, следовательно, и документы, содержащие ту или иную информацию подразделяются на секретные и конфиденциальные. Причем, секрет-

ные документы могут быть с грифом «Секретно», «Совершенно секретно», «Особой важности». Конфиденциальные документы соответственно с грифами «Коммерческая тайна», «Банковская тайна» и т.д. В настоящее время видов конфиденциальной информации (а, следовательно, и возможных грифованных документов) насчитывается более 30. Что в целом не создает благоприятной атмосферы в смысле обеспечения их безопасности. По этой причине количество видов конфиденциальной информации в перспективе, надо полагать, уменьшится. Каждый вид конфиденциальных документов имеет реквизиты. По своей природе (рис. 4.2) конфиденциальные документы бывают: нормативно-методические (НМД); руководящие (РД); распорядительные (РПД); информационно-справочные (ИСД); организационные (ОД); финансово-бухгалтерские (ФБД); кадровые (по личному составу) КД.

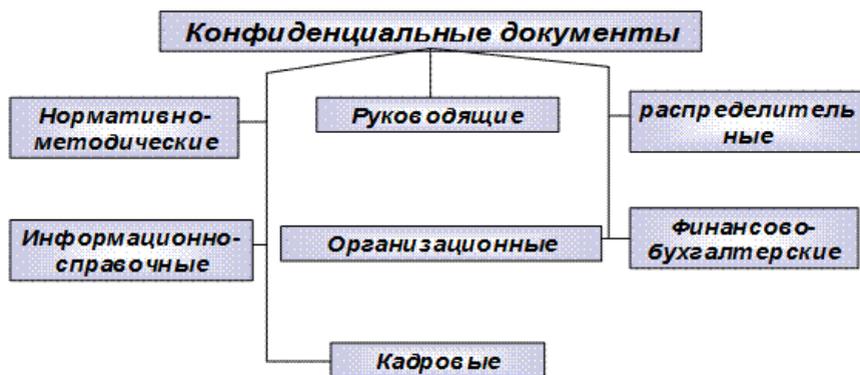


Рис. 4.2. Виды конфиденциальных документов

Правила оформления реквизитов регламентированы ГОСТ «Унифицированная система организационно-распорядительной документации. Требования к оформлению документов». (ГОСТ Р 6.30—2003). Конфиденциальные документы, содержащие коммерческую тайну, должны иметь гриф ограничения доступа к документу. Он располагается в правом верхнем углу, например: коммерческая тайна (или сокращенно КТ). Дополняется гриф номером экземпляра.

Конфиденциальные документы должны обрабатываться в конфиденциальном делопроизводстве фирмы, либо в общем делопроиз-

водстве, специально назначенным должностным лицом, ответственным за конфиденциальные документы. Конфиденциальные документы должны храниться в отдельном помещении в запираемых и опечатываемых шкафах. Допускается хранение конфиденциальных документов в общем делопроизводстве. Но обязательно они должны находиться отдельно от других дел делопроизводства.

В зависимости от назначения конфиденциальные документы подразделяются на: входящие; исходящие; внутренние. Прием входящих конфиденциальных документов (рис. 4.3) осуществляется сотрудником конфиденциального делопроизводства.

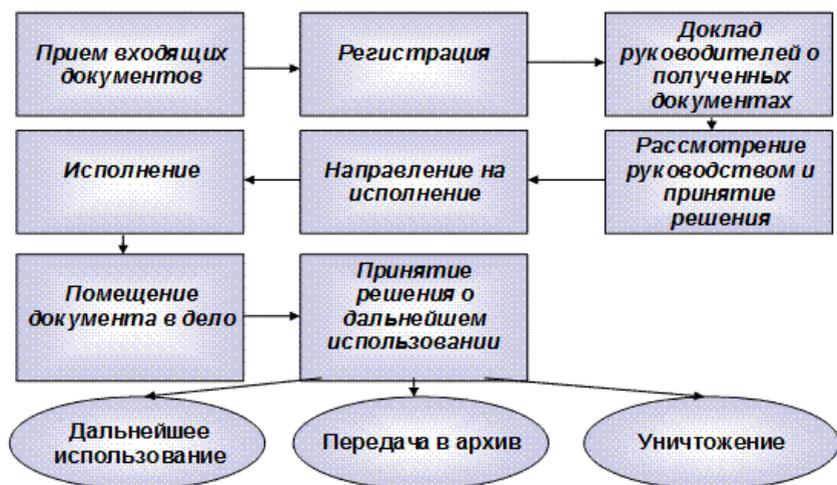


Рис. 4.3. Порядок работы с входящими конфиденциальными документами

Работа с конфиденциальными исходящими документами включает следующие этапы (рис. 4.4):

- разработка проекта документа;
- согласование документа;
- подписание документа;
- регистрация документа;
- отправка документа.

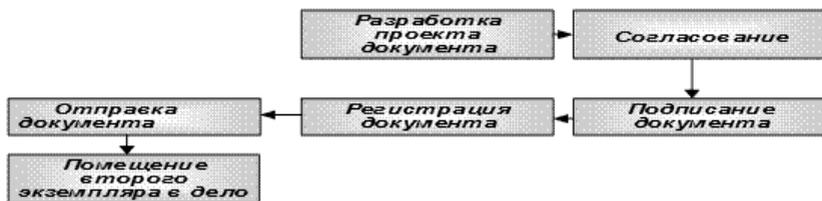


Рис. 4.4. Порядок работы с конфиденциальными исходящими документами

Проект исходящего конфиденциального документа разрабатывается исполнителем документа в двух экземплярах и по необходимости согласовывается с другими специалистами фирмы. Далее проект документа предоставляется на подпись руководителю фирмы. После подписания документа, он регистрируется сотрудником конфиденциального делопроизводства в журнале (карточке) регистрации исходящих конфиденциальных документов. Рассылка конфиденциальных документов осуществляется согласно подписанным руководителем списков с обязательным указанием учетных номеров отправленных документов. Порядок работы с конфиденциальными внутренними документами показан на рис. 4.5.

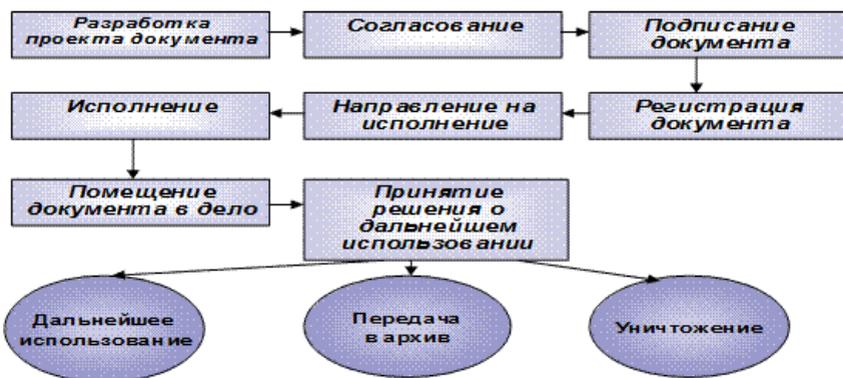


Рис. 4.5. Порядок работы с конфиденциальными внутренними документами

Организация конфиденциального документооборота должна строиться на основе следующих принципов: разрешительной системы доступа к конфиденциальным документам; исключения несанкцио-

нированного доступа к конфиденциальным документам; целенаправленного регулирования процессов движения конфиденциальных документов; исключения инстанций прохождения конфиденциальных документов и действий с ними, не обусловленных характером и порядком исполнения документов; фиксированной передачи конфиденциальных документов; обеспечения своевременного и качественного исполнения конфиденциальных документов; персональной и обязательной ответственности за выдачу неправомερных разрешений на ознакомление с конфиденциальными документами и на их отправление.

4.2. Сущность, задачи и особенности конфиденциального делопроизводства

По уровню доступности документы подразделяются на две категории: общедоступные и с ограниченным доступом. Общедоступными являются открытые документы. К документам с ограниченным доступом относятся документы, работа с которыми может производиться по специальному разрешению уполномоченных на то лиц. Документирование открытой информации и организация работы с открытыми документами входят в сферу действия открытого делопроизводства. Документы с ограниченным доступом относятся к сфере деятельности не одного, а нескольких типов делопроизводства, в зависимости от того, к какому виду тайны относится содержащаяся в документах информация. Нормативными документами установлено 6 видов тайны: государственная, коммерческая, служебная, личная, семейная и профессиональная.

Документы, содержащие государственную тайну, относятся к сфере секретного делопроизводства. Документы, содержащие личную и различные подвиды профессиональной тайны, являются предметом соответствующих типов специального делопроизводства. Конфиденциальное делопроизводство, как уже было отмечено, распространяется на документы, содержащие коммерческую и служебную тайну. При этом к документам, составляющим служебную тайну, отнесены только документы с грифом «Для служебного пользования», так как документы, содержащие коммерческую тайну других субъектов, должны обрабатываться и защищаться в режиме коммерческой тайны. Объединение

конфиденциальных документов, содержащих коммерческую и служебную тайну, одним делопроизводством обусловлено тем, что эти документы почти полностью идентичны по технологическим процедурам составления, обработки, обращения, хранения и защиты. Конфиденциальное делопроизводство следует определять как деятельность, обеспечивающую документирование конфиденциальной информации, организацию работы с конфиденциальными документами и защиту содержащейся в них информации. При этом под документированием информации понимается процесс подготовки и изготовления документов, под организацией работы с документами — их учет, размножение, прохождение, исполнение, отправление, классификация, систематизация, подготовка для архивного хранения, уничтожение, режим хранения и обращения, проверки наличия. 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 сфере деятельности открытое делопроизводство распространяется на управленческие действия и включает в основном управленческие документы.

Конфиденциальное делопроизводство в силу условий работы с конфиденциальными документами распространяется как на управленческую, так и на различные виды производственной деятельности, включает не только управленческие, но и научно-технические документы (научно-исследовательские, проектные, конструкторские, технологические и др.). Кроме того, конфиденциальное делопроизводство распространяется не только на официальные документы, но и на их проекты, различные рабочие записи, не имеющие всех необходимых реквизитов, но содержащие информацию, подлежащую защите. По видам работ конфиденциальное делопроизводство отличается от открытого, с одной стороны, большим 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 и от утраты, и от утечки. Термин «утечка конфиденциальной информации», вероятно, не самый благозвучный, однако он более емко, чем другие термины, отражает суть явления, к тому же он давно уже закрепился в научной литературе и нормативных документах. *Утечка конфиденциальной информации* представляет собой неправомерный, т.е. неразрешенный выход такой информации за пределы защищаемой зоны ее функционирования или установленного круга лиц, имеющих право работать с ней, если этот выход привел к получению информации (ознакомлению с ней) лицами, не имеющими к ней санкционированного доступа, независимо от того, работают или не работают такие лица на данном предприятии и обусловлены уязвимостью информации.

Уязвимость информации следует понимать как ее доступность для дестабилизирующих воздействий, т.е. таких воздействий, которые нарушают *установленный статус информации*. Нарушение статуса любой документированной информации включается в нарушение ее физической сохранности (вообще либо у данного собственника в полном или частичном объеме), логической структуры и содержания, доступности для правомочных пользователей. Нарушение статуса конфиденциальной документированной информации дополнительно включает нарушение ее конфиденциальности (закрытости для посторонних лиц). Уязвимость документированной информации — понятие собирательное. Она не существует вообще, а проявляется в различных формах. К таким *формам, выражающим результаты дестабилизирующего воздействия на информацию*, относятся (в скобках указаны существующие варианты названий форм):

- хищение носителя информации или отображенной в нем информации (кража);
- потеря носителя информации (утера);
- несанкционированное уничтожение носителя информации или отображенной в нем информации (разрушение);
- искажение информации (несанкционированное изменение, несанкционированная модификация, подделка, фальсификация);
- блокирование информации;
- разглашение информации (распространение, раскрытие).

Термин «разрушение» употребляется главным образом применительно к информации на машинных носителях. Существующие вари-

анты названий: модификация, подделка, фальсификация — не совсем адекватны термину «искажение», они имеют нюансы, однако суть их одна и та же — несанкционированное частичное и полное изменение состава первоначальной информации. Блокирование информации в данном контексте означает блокирование доступа к ней правомочных пользователей, а не злоумышленников.

Разглашение информации является формой проявления уязвимости только конфиденциальной информации. Та или иная форма уязвимости документированной информации может реализоваться в результате преднамеренного или случайного дестабилизирующего воздействия различными способами на носитель информации или на саму информацию со стороны источников воздействий. Такими источниками могут быть люди, технические средства обработки передачи информации, средства связи, стихийные бедствия и др. Способами дестабилизирующего воздействия на информацию являются копирование (фотографирование), записывание, передача, съем, заражение программ обработки информации вирусом, нарушение технологии обработки и хранения информации, вывод (или выход) из строя и нарушение режима работы технических средств обработки и передачи информации, физическое воздействие на информацию и др. Реализация форм проявления уязвимости документированной информации приводит или может привести к двум видам уязвимости — утрате или утечке информации.

К *утрате* документированной информации приводят хищение и потеря носителей информации, несанкционированное уничтожение носителей информации или только отображенной в них информации, искажение и блокирование информации. Утрата может быть полной или частичной, безвозвратной или временной (при блокировании информации), но в любом случае она наносит ущерб собственнику информации.

К *утечке* конфиденциальной документированной информации приводит ее разглашение. В литературе и даже в нормативных документах термин «утечка конфиденциальной информации» нередко заменяется или отождествляется с терминами: «разглашение конфиденциальной информации», «распространение конфиденциальной информации». Такой подход не является правомерным. Разглашение или распространение конфиденциальной информации означают не-

санкционированное доведение ее до потребителей, не имеющих права доступа к ней. При этом такое доведение должно осуществляться кем-то, исходить от кого-то. Утечка происходит при разглашении (несанкционированном распространении) конфиденциальной информации, но не сводится только к нему. Утечка может произойти и в результате потери носителя конфиденциальной документированной информации, а также хищения носителя информации либо отображенной в нем информации при сохранности носителя у его собственника (владельца). «Может произойти» не означает, что произойдет. Потерянный носитель может попасть в чужие руки, а может быть и «прихвачен» мусороуборочной машиной и уничтожен в установленном для мусора порядке. В последнем случае утечки конфиденциальной информации не происходит. Хищение конфиденциальной документированной информации также не всегда связано с получением ее лицами, не имеющими к ней доступа. Имелось немало случаев, когда хищение носителей конфиденциальной информации осуществлялось у коллег по работе допущенными к этой информации лицами с целью «подсидки», причинения вреда коллеге. Такие носители, как правило, уничтожались лицами, похитившими их. Но в любом случае потеря и хищение конфиденциальной информации если и не приводят к ее утечке, то всегда создают угрозу утечки. Поэтому можно сказать, что к утечке конфиденциальной информации приводит ее разглашение и могут привести хищение и потеря. Сложность состоит в том, что зачастую невозможно определить, во-первых, сам факт разглашения или хищения конфиденциальности информации при сохранности носителя информации у ее собственника (владельца), во-вторых, попала ли информация вследствие ее хищения или потери посторонним лицам.

Суммируя соотношение форм и видов уязвимости защищаемой информации, можно констатировать:

1. Формы проявления уязвимости информации выражают результаты дестабилизирующего воздействия на информацию, а виды уязвимости — конечный суммарный итог реализации форм проявления уязвимости.

2. Утрата информации включает в себя, по сравнению с утечкой, большее число форм проявления уязвимости информации, но она не поглощает утечку, так как не все формы проявления уязвимости ин-

формации, которые приводят или могут привести к утечке, совпадают с формами, приводящими к утрате.

3. Наиболее опасными формами проявления уязвимости конфиденциальной документированной информации являются потеря, хищение и разглашение — первые две одновременно могут привести и к утрате, и к утечке информации, вторая (хищение информации при сохранности носителя) и третья могут не обнаружиться, со всеми вытекающими из этого последствиями.

4. Неправомерно отождествлять, как это нередко делается в научной литературе и нормативных документах, включая законы, виды и отдельные формы проявления уязвимости информации (утрата = потеря, утрата = хищение, утечка = разглашение (распространение), а также формы проявления уязвимости информации и способы дестабилизирующего воздействия на нее.

5. Необходимо уделять одинаковое внимание предотвращению как утраты защищаемой документированной информации, так и ее утечки, так как ущерб собственнику информации наносится в любом случае.

Защита конфиденциальной документированной информации от утраты и утечки осуществляется в определенной мере в рамках и первой, второй составляющих конфиденциального делопроизводства, так как она взаимоувязана, «переплетена» с ними: документирование конфиденциальной информации и организация работы с конфиденциальными документами должны производиться в условиях обеспечения их защиты, и вместе с тем многие вопросы защиты решаются в ходе и путем осуществления систематических операций по учету и обработке документов. Однако защитные мероприятия охватывают не только сами документы, но и другие объекты, так или иначе связанные с защищаемыми документами (помещения, технические средства обработки и передачи информации и др.). Поэтому в определении конфиденциального делопроизводства защита документированной информации выделена в самостоятельную составляющую. 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:

1) документационное обеспечение всех видов конфиденциальной деятельности;

2) защита документированной информации, образующейся в процессе конфиденциальной деятельности.

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

Достоверность документной информации заключается, во-первых, в ее соответствии объективному состоянию того или другого вопроса и, во-вторых, в ее юридической силе, характеризующейся наличием и правильностью оформления соответствующих реквизитов. Своевременность документной информации означает, что за время обработки и передачи информации не изменилось состояние вопроса, к которому она относится. Организация исполнения документов включает в себя и оперативное доведение их до исполнителей, и обеспечение своевременного и качественного решения содержащихся в документах вопросов. Организация использования документов состоит в обеспечении как текущего, оперативного, так и последующего, ретроспективного использования документной информации. Вторая задача имеет своей целью обеспечение сохранности и конфиденциальности документированной информации, что требует создания и поддержания специальных условий хранения, обработки и обращения документов, гарантирующих надежную защиту, как самих документов, так и содержащейся в них информации.

Сущность конфиденциального делопроизводства обуславливает его организационные и технологические особенности, к числу основных из которых относятся:

— письменное нормативное закрепление общей технологии документирования, организации работы с документами и их защиты;

— жесткое регламентирование состава издаваемых документов и содержащейся в них информации, в том числе на стадии подготовки черновиков и проектов документов; обязательный поэкземплярный и листный учет всех, без исключения, документов, проектов и черновиков; максимально необходимая полнота регистрационных данных о каждом документе;

— фиксация прохождения и местонахождения каждого документа;

— проведение систематических проверок наличия документов; разрешительная система доступа к документам и делам, обеспечивающая правомерное и санкционированное ознакомление с ними; жесткие требования к условиям хранения документов и обращения с ними, которые должны обеспечивать сохранность и конфиденциальность документированной информации;

— регламентация обязанностей лиц, допущенных к работе с конфиденциальной документированной информацией, к ее защите;

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

Особенностью конфиденциального делопроизводства является и своеобразное переплетение некоторых функций, которые, на первый взгляд, как бы взаимоисключают друг друга. В частности, функциями по реализации задачи документационного обеспечения конфиденциальной деятельности являются создание документов, необходимых и достаточных для такой деятельности, предоставление каждому пользователю всех документов, требующихся для выполнения должностных обязанностей, параллельными им функциями по реализации задачи защиты конфиденциальной информации — предотвращение необоснованного издания и рассылки документов, исключение необоснованного ознакомления с документами. На самом деле применительно к документированию это означает, что конфиденциальная деятельность должна обеспечиваться минимальным количеством документов при сохранении полноты и достоверности информации, применительно к организации документооборота — предоставление пользователям всех необходимых документов, но только тех, которые действительно требуются для выполнения должностных обязанностей. Особенности конфиденциального делопроизводства одновременно выступают и в качестве требований к нему.

4.3. Система доступа к конфиденциальным документам

Конфиденциальные документы являются документами ограниченного доступа. Это означает, что знакомиться и работать с ними могут только лица, получившие на то соответствующие разрешения. Порядок получения и оформления таких разрешений устанавливается на каждом предприятии системой доступа к конфиденциальным документам, которая представляет собой совокупность норм и правил, определяющих, кто из руководителей предприятия и структурных подразделений, кому из пользователей и с какими категориями конфиденциальных документов может давать разрешение на ознакомление, а также, каким образом оформляются такие разрешения в зависимости от вида учета документов.

При разработке системы доступа к конфиденциальным документам необходимо руководствоваться следующими подходами.

1. Доступ к конфиденциальным документам может предоставляться только лицам, имеющим оформленный в установленном порядке (контрактом, приказом) допуск к соответствующему виду тайны и давшим письменное обязательство (в контракте или специальной подписке) о неразглашении ставших им известными конфиденциальных сведений. Допуск к соответствующему виду тайны является основанием для доступа к конкретным документам в пределах этого вида тайны.

2. Доступ к конфиденциальным документам должен быть обоснованным и правомерным, т.е. базироваться на служебной необходимости ознакомления с конкретным документом именно данного лица.

3. Система доступа должна давать возможность обеспечивать пользователей всеми необходимыми им в силу служебных обязанностей конфиденциальными документами, но только теми, которые действительно необходимы для выполнения конкретных видов работ.

К сожалению, этот подход не всегда четко соблюдается. С одной стороны, стремясь максимально сократить количество лиц, допускаемых к конфиденциальным документам, на некоторых предприятиях не знакомят часть пользователей с необходимой им для служебной деятельности информацией и тем самым снижают качество этой деятельности, с другой стороны — знакомят пользователей с конфиденциальными документами, не связанными напрямую с их функцио-

нальными обязанностями, но, как выражаются, необходимыми им «для общего развития» или «расширения кругозора», что приводит к разглашению информации, т.е. неправомерному доведению информации до лиц, которые не должны ее знать.

4. Доступ к конфиденциальным документам должен быть санкционированным, т.е. осуществляться только по соответствующему разрешению.

5. Доступ к конфиденциальным документам могут предоставлять только уполномоченные на то должностные лица, при этом соответствующее должностное лицо может давать разрешение на ознакомление с входящими в сферу его деятельности конфиденциальными документами только установленному кругу лиц и только по служебной необходимости.

6. Доступ должен оформляться письменно по каждому конкретному конфиденциальному документу. При необходимости ознакомления пользователя только с частью документа в разрешении на ознакомление должны быть указаны разделы, пункты или страницы, с которыми можно знакомить пользователя. Составители (исполнители) документов и лица, которые визировали, согласовывали, подписывали, утверждали документы, а также лица, указанные в тексте распорядительных документов, допускаются к таким документам без оформления дополнительных разрешений, если они продолжают выполнять те же функциональные обязанности. В первом случае это обусловлено тем, что перечисленные лица как бы автоматически в силу своего служебного положения уже получили доступ к документам на стадии их подготовки, во втором — тем, что с поручением, содержащимся в распорядительном документе, исполнитель должен быть ознакомлен обязательно, чтобы знать, что ему поручено, поэтому оформление дополнительного доступа теряет всякий смысл.

Поскольку система доступа к конфиденциальным документам содержит в себе значительное количество правовых положений, а нарушение ее требований, приводящее, как правило, к разглашению конфиденциальной информации, влечет за собой дисциплинарную, гражданско-правовую и в некоторых случаях уголовную ответственность виновных лиц, то ее следует закреплять в специальном нормативном документе, который обычно называется «Положение о системе доступа к конфиденциальным документам».

Положение должно основываться на вышеизложенных подходах и может включать в себя следующие разделы.

1. Общие положения.

2. Полномочия должностных лиц по разрешению доступа к конфиденциальным документам.

3. Порядок оформления разрешений на доступ к конфиденциальным документам.

В первом разделе указываются: назначение Положения; нормативные документы, на которых оно базируется; сфера его распространения; основные задачи и принципы системы доступа; на кого возлагается ответственность за невыполнение требований положения; кем осуществляется контроль за соблюдением норм положения. При этом следует отразить, что ответственность за невыполнение требований положения несут все должностные лица, имеющие право давать разрешение на доступ к конфиденциальным документам, а также все пользователи конфиденциальных документов. Контроль за выполнением норм положения должен возлагаться на руководителей службы безопасности, подразделения конфиденциального делопроизводства и управленческо-производственных подразделений в пределах их компетенции. Во втором разделе должны быть перечислены все должностные лица, которые могут давать разрешение на доступ к конфиденциальным документам, с указанием, какой категории пользователей и к какому составу документов.

Основополагающими подходами при этом должны быть следующие:

— руководитель предприятия имеет право давать разрешение на доступ к соответствующим конфиденциальным документам всем категориям пользователей;

— заместители руководителя предприятия по отдельным направлениям имеют право давать разрешение на доступ к соответствующим конфиденциальным документам всем пользователям, но в пределах своей сферы деятельности;

— руководителям подразделений дается право разрешать доступ к конфиденциальным документам всем сотрудникам своих подразделений по тематике работы подразделений; для осуществления доступа к конфиденциальным документам данного подразделения сотрудников других подразделений необходимо разрешение соответствующим

щего заместителя руководителя предприятия или руководителя предприятия;

— первые заместители руководителей, а также должностные лица, временно исполняющие ту или иную должность, могут, как правило, разрешать доступ к конфиденциальным документам в объеме всех прав, предусмотренных для замещаемых ими лиц.

В третьем разделе определяется порядок оформления разрешений на доступ к конфиденциальным документам, зарегистрированным по различным видам учета. Разрешение на ознакомление с конфиденциальными документами должно оформляться: по поступившим и изданным документам в форме резолюции на документе; по документам, зарегистрированным по учету документов выделенного хранения, в форме резолюции на документе или подписанного соответствующим руководителем списка пользователей на внутренней стороне обложки документа, титульном листе либо в карточке учета выдачи документа. Разрешение на доступ к конфиденциальным делам оформляется в номенклатуре дел.

Отдельным разделом положения может быть предусмотрен порядок доступа к конфиденциальным документам лиц, не работающих на данном предприятии (при выполнении совместных работ и др.).

При этом следует иметь в виду, что сотрудники органов государственной власти, иных государственных органов и органов местного самоуправления имеют право на доступ к конфиденциальной информации в пределах компетенции, определенной для этих органов законодательством РФ, поэтому предприятия обязаны не только знакомить сотрудников таких органов с конфиденциальными документами, но и предоставлять документы в распоряжение органов в случаях, установленных законодательством. В соответствии с законодательством названные органы обязаны обеспечить защиту полученных ими документов от разглашения и неправомерного использования должностными лицами и иными служащими этих органов, которые ознакомились с документами в связи с выполнением служебных обязанностей. За разглашение или неправомерное использование содержащейся в документах конфиденциальной информации данные органы несут предусмотренную законодательством ответственность. Положение может разрабатываться подразделением конфиденциального делопроизводства или постоянно действующей экзаменационной ко-

миссией (ПДЭК). Оно подписывается разработчиками, визируется всеми лицами, имеющими право давать разрешение на доступ к конфиденциальным документам, и утверждается приказом руководителя предприятия. В приказе определяются и мероприятия по введению положения в действие (порядок изучения положения пользователями, технология осуществления контроля за его выполнением и др.). С утвержденным положением должны быть ознакомлены под расписку все сотрудники предприятия, работающие с конфиденциальными документами.

Глава 5. Организация исполнения конфиденциальных документов

5.1. Организация исполнения конфиденциальных документов

В соответствии с утвержденным положением о системе доступа к конфиденциальным документам после учета документов осуществляется их рассмотрение и передача для исполнения. При большом объеме поступающих документов целесообразно осуществлять их предварительное распределение по уровням принятия решений по ним. С этой целью разрабатывается перечень поступивших документов, направляемых на исполнение без рассмотрения руководителем предприятия. В этом перечне полномочия по принятию решений по исполнению документов делегируются на соответствующий уровень управления. В перечень включаются конкретные наименования поступающих документов, имеющих, как правило, типовой и повторяющийся характер, которые адресуются заместителям руководителя предприятия, руководителям подразделений или непосредственным исполнителям без рассмотрения этих документов руководителем предприятия. Перечень может иметь следующую форму:

№ п/п	Наименование адресуемых документов	Инициалы, фамилии лиц, которым адресуются документы	Инициалы, фамилии лиц, которым адресуются документы при временном отсутствии основных адресатов
1	2	3	4

Разработку перечня целесообразно возлагать на ПДЭК. При подготовке перечня необходимо учитывать требования Положения о системе доступа к конфиденциальным документам в части обеспечения правомерности доступа к документам в процессе делегирования полномочий по их рассмотрению. Перечень подписывается председателем и членами ПДЭК и вводится в действие приказом руководителя предприятия. В приказе определяется и должностное лицо, которому предоставляется право адресования документов, включенных в перечень. Им может быть руководитель подразделения конфиденциального делопроизводства, руководитель службы безопасности или помощник (референт) руководителя предприятия. Это лицо в соответствии с перечнем лишь адресует документы без указания порядка и сроков их исполнения, поскольку при адресовании документов руководителям различных уровней эти руководители в резолюции определяют характер и сроки исполнения документов, а при адресовании документов непосредственным исполнителям последние знают, что нужно сделать по исполнению документа и в какие сроки, так как такие документы являются типовыми и характер их исполнения однотипен. Перечень позволяет сократить путь и время движения документов до непосредственных исполнителей, а следовательно, ускорить процесс их исполнения, освободить руководителей различного ранга от рассмотрения вопросов, которые могут быть решены непосредственными исполнителями документов, уменьшить трудозатраты на рассмотрение, исполнение и обработку документов, обеспечить выполнение требований системы доступа к поступившим документам. Не включенные в перечень поступившие документы, а также изданные документы и документы выделенного хранения, подлежащие рассмотрению непосредственно руководителем предприятия, передаются ему под подпись в «Журнале передачи конфиденциальных документов», если они не рассматриваются в присутствии сотрудника подразделения конфиденциального делопроизводства, ответственного за их учет. Журнал имеет следующие графы:

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

При одновременном получении и возврате нескольких документов может проставляться одна подпись за все документы. Если после рассмотрения документов в присутствии сотрудника подразделения конфиденциального делопроизводства у руководителя остается часть их, то в журнал передачи конфиденциальных документов вносится только эта часть. В процессе рассмотрения документов на них пишутся резолюции.

В состав резолюции входят следующие элементы: инициалы, фамилия исполнителя (исполнителей), содержание поручения (предписываемое действие), срок исполнения (при необходимости), подпись, дата, например: «И. В. Бородину, Н. И. Самойловой. Прошу подготовить проект договора к 18.04.2017. Личная подпись 09.04.2017».

Текст поручения должен быть конкретным и кратким. Не должны быть резолюции типа: «Прошу зайти», «Прошу переговорить» и т.п. Если для принятия решения необходим разговор с исполнителем, то приглашение исполнителя должно оформляться не резолюцией, а записью на отдельном прикрепляемом к документу листе или другим способом. После разговора с исполнителем должна быть оформлена резолюция на документе. В случаях, когда поручение дается двум и более лицам, ответственным исполнителем является лицо, указанное первым. Ему предоставляется право координации работы соисполнителей. Если ответственным исполнителем назначается лицо, указанное в резолюции не первым, то рядом с его фамилией в скобках или через тире проставляется «отв.». На документах, не требующих указаний по исполнению и срокам исполнения, эти данные не проставляются. Резолюция пишется на площади между адресатом и текстом. Если она не помещается на этой площади, то ее можно писать на свободном месте первого листа, за исключением полей.

Допускается оформление резолюции на отдельном листе с указанием на нем учетного номера и даты документа, к которому относится резолюция, однако не следует вводить это в систему, так как резолюция является составной частью документа и поэтому должна, как правило, оформляться на нем. На документах, требующих контроля исполнения, может проставляться на левом поле, на уровне заголовка реквизит «Отметка о контроле», который обозначается буквой «К» либо словом или штампом «Контроль». Целью отметки является напоминание исполнителю об обязанности исполнения документа в ус-

тановленный срок и указание подразделению конфиденциального производства о взятии документа на контроль. После рассмотрения и написания резолюций на документах они, как и документы, адресованные исполнителям в соответствии с Перечнем поступивших документов, направляемых на исполнение без рассмотрения руководителем предприятия, а также требующие исполнения внутренние документы, передаются исполнителям под подпись в соответствующих учетных формах. Обязательность подписи за получение и возврат конфиденциальных документов независимо от занимаемой должности необходима и для обеспечения сохранности документов, и потому, что при безрасписочном получении документов в случаях их утраты пользователи, как правило, заявляют, что они утраченный документ не получали, и вся вина за утрату ложится на сотрудника подразделения конфиденциального делопроизводства. Подпись за получение документов проставляется в графе 10 журнала учета поступивших документов с заполнением граф 8, 9, 1, 6, в графе 8 журнала учета изданных документов с заполнением граф 6, 7 (в графе 5 делается прочерк), в графе 2 карточки учета выдачи конфиденциального документа выделенного хранения с заполнением графы 1.

Если исполнителей несколько, то документ в первую очередь передается ответственному исполнителю, указанному в резолюции, а при отсутствии указания — поставленному в резолюции первым. При получении документа исполнитель должен проверить соответствие учетного номера документа и количества его листов (с просчетом) записям в учетных формах. Передача документов между исполнителями должна производиться через подразделение конфиденциального делопроизводства или (при возврате в течение рабочего дня) по разовой расписке, минуя подразделение конфиденциального делопроизводства. При карточном способе учета при изменении местонахождения документа в контрольном журнале карандашом проставляется новое местонахождение документа, а карточка перемещается в соответствующую ячейку картотеки. Если документ одновременно выдается по частям нескольким исполнителям, то при карточном способе учета подписи за получение документа проставляются на основной карточке, которая ставится в ячейку картотеки под фамилией 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 лишь содержать сведения об учетном номере документа, фамилии соответствующего исполнителя, количестве полученных им листов (экземпляров).

Документы, требующие подготовки ответа или принятия решения, подлежат контролю. Организация контроля должна обеспечивать качественное и своевременное исполнение документов. Ответственность за качество исполнения документов несут исполнители и руководители подразделений, в которых работают исполнители. Контроль за сроками исполнения документов осуществляет наряду с руководителями соответствующих структурных подразделений подразделение конфиденциального делопроизводства. Если исполнение документа поставлено на контроль, то для его осуществления при карточном способе учета используются дополнительные экземпляры учетных карточек, в которых для перенесения резолюции руководителя и контрольных отметок используются графы, отражающие движение документов в ходе их исполнения. При журнальном способе учета для осуществления контроля исполнения документов изготавливаются специальные контрольные карточки, имеющие следующие графы:

Учетный номер и гриф конфиденциальности документа	Дата документа	Вид и заголовок документа
1	2	3
Резолюция	Контрольные отметки	Отметка о снятии документа с контроля
4	5	6

В контрольных карточках не должны содержаться конфиденциальные сведения. При контроле документов, пункты которых имеют самостоятельного исполнителя и свой срок исполнения, на каждый из пунктов заполняется отдельный экземпляр карточки учета (контрольной карточки).

Из карточек контролируемых документов формируется контрольная картотека по срокам исполнения документов. В пределах каждого срока карточки могут систематизироваться по видам учета документов, исполнителям, видам документов и др. При автоматизи-

рованном контроле исполнения документов соответствующие данные вводятся в компьютер. В процессе контроля исполнения документа подразделение конфиденциального делопроизводства должно периодически (в установленные на предприятии сроки) напоминать исполнителю о контролируемом документе, о чем в графе «Контрольные отметки» контрольной карточки проставляется соответствующая дата. О нарушении срока исполнения документа подразделение конфиденциального делопроизводства извещает соответствующего руководителя. После исполнения документа исполнитель проставляет на нем отметку об исполнении документа и направлении его в дело, которая включает следующие данные: ссылку на дату и номер документа, свидетельствующего об исполнении данного документа, или при отсутствии такого документа краткую справку об исполнении; слово «В дело»; номер (индекс) дела, в которое должен быть подшит документ; подпись исполнителя или руководителя структурного подразделения, в котором исполнен документ; дату. Например: «Исполнен 14.04.2016. № 9К. В дело 0210, подпись, 15.04.2016» или «Запрашиваемые материалы включены в сводную заявку, предприятию сообщено по телефону (В. М. Бушуеву). В дело 1402, подпись, 16.04.2016».

Исполненный документ вместе с документом-ответом (при наличии) сдается в подразделение конфиденциального делопроизводства. Сотрудник подразделения должен проверить правильность произведенной отметки об исполнении документа, соответствие вида и заголовка документа заголовку дела, в которое он направляется, просчитать количество листов документа и проверить соответствие их учетным данным, расписаться за получение документа в соответствующих графах учетных журналов (карточек). Контролируемый документ по решению соответствующего руководителя снимается с контроля, контрольная карточка (дубликат учетной карточки) или уничтожается, или помещается в справочную картотеку. Основная учетная карточка (при карточном способе учета) перекладывается в картотеку исполненных документов, в которой карточки располагаются в последовательности их номеров. Если конфиденциальный документ не требует исполнения, а адресован лишь для ознакомления, то он может не выдаваться на рабочее место исполнителя, а ознакомление с ним производится в подразделении конфиденциального делопроизводства

(комнате для исполнителей). При этом если ознакомление производится в присутствии сотрудника подразделения конфиденциального делопроизводства, ответственного за учет документа, то подпись в учетной форме за получение документа может не проставляться. Подписи об ознакомлении с документами с проставлением даты производятся на самих документах, а подписи об ознакомлении с распорядительными документами могут проставляться на специальном листе ознакомления. В комнате для исполнителей или устанавливаемых в подразделении конфиденциального делопроизводства кабинках производится и исполнение документов, если на рабочих местах в служебных комнатах исполнителей нет необходимых условий, обеспечивающих сохранность документов и содержащейся в них информации. После исполнения поступившего документа или ознакомления с ним соответствующих должностных лиц негрифованные приложения, не подлежащие совместному хранению с основным конфиденциальным документом, передаются в службу открытого делопроизводства с заполнением граф 8—10 журнала учета поступивших документов и с отметкой о передаче на основном документе (сопроводительным письмом).

5.2. Отправление конфиденциальных документов

Отправление конфиденциальных документов на другие предприятия производится в законвертованном виде. Конверты (пакеты) должны быть светонепроницаемыми. Если они светопроницаемы, то вложения обертываются светонепроницаемой бумагой. Если одному адресату направляются несколько документов, то они помещаются в один пакет. В правом верхнем углу пакета проставляются: гриф конфиденциальности, соответствующий наивысшему грифу конфиденциальности документов, подлежащих вложению в пакет, ниже при необходимости пометка «Лично». На пакете пишется адрес и наименование предприятия-получателя, а при наличии пометки «Лично» дополнительно должность, инициалы и фамилия адресата. Под адресатом перечисляются учетные номера документов, которые будут вложены в пакет (если документ отправляется с сопроводительным письмом, то на пакете проставляется только номер сопроводительного письма без указания номеров приложений). При направлении до-

кументов в двух и более экземплярах на пакете рядом с номером документа в скобках указываются номера экземпляров. Ниже проставляются адрес и наименование предприятия-отправителя. Для постоянных корреспондентов при большом объеме переписки целесообразно иметь пакеты с заранее воспроизведенными на них типографским способом адресами и наименованиями предприятий-получателей и отправителя. При необходимости на пакете в центре верхнего поля может проставляться пометка «Срочно».

Перед помещением конфиденциальных документов в подготовленные пакеты проверяется соответствие данных на документах и пакетах, просчитывается количество листов и соответствие их учетным данным. При наличии сопроводительного письма проверяется, кроме того, соответствие названия, учетного номера, грифа конфиденциальности, номера экземпляра, количества листов приложения (с просчетом листов) записям в сопроводительном письме. Со стороны клапана в пакет помещается прокладка. Пакет заклеивается силикатным клеем и прошивается крест-накрест через середину нитками или металлическими скрепками с захватом всех клапанов либо, если вложения нельзя прокалывать, через четыре края с тугим охватом краев вложений. Нитки завязываются в центре оборотной стороны пакета, на узел прошивки накладывается бумажная наклейка из папиросной или другой тонкой, но не расслаивающейся бумаги с оттиском каучуковой печати предприятия. Наклейка должна быть на 34 мм больше размера оттиска печати. Наклейка накладывается так, чтобы захватывала все клапаны пакета в середине, концы ниток не находились под наклейкой, а узел прошивки был ею закрыт. При прошивке металлическими скрепками бумажная наклейка накладывается на загнутые концы скрепок. Наклейка сверху покрывается тонким слоем силикатного клея, чтобы образовалась стекловидная прозрачная пленка. Размер пленки должен быть на 12 мм больше бумажной наклейки.

Пакеты с конфиденциальными документами могут доставляться через спецсвязь или почтовое отделение связи либо, минуя их, непосредственно адресату. Возможно отправление пакетов и фельдъегерской связью. Пересылка пакетов фельдъегерской и специальной связью осуществляется на договорной основе. Через почтовое отделение связи пакеты пересылаются ценными или заказными отправлениями в соответствии с почтовыми правилами. При этом виде отправления

гриф конфиденциальности может проставляться на пакете не в правом верхнем углу, а рядом с номером документа аббревиатурой. Часть реквизитов на пакет допускается наносить маркировальной машиной. При отправлении конфиденциальных пакетов через почтовое отделение связи в целях сокрытия их конфиденциальности они могут помещаться в другие пакеты, на которые наносятся только реквизиты, предусмотренные почтовыми правилами для открытых ценных и заказных отправлений. При таком способе конвертования пакеты поступают в подразделение открытого делопроизводства предприятия-получателя и после вскрытия наружного пакета передаются под расписку в подразделение конфиденциального делопроизводства. При пересылке корреспонденции фельдъегерской или специальной связью составляется в необходимом количестве экземпляров реестр, последний экземпляр которого остается на предприятии. Передача пакетов осуществляется в соответствии с правилами этих служб связи.

Доставка конфиденциальных пакетов на другие предприятия, минуя органы связи, может осуществляться с разрешения руководителя предприятия сотрудником подразделения конфиденциального делопроизводства либо другим работником предприятия, допущенным к конфиденциальной информации, на служебном транспорте. Пакеты передаются по реестру или взамен разовой расписки, в которых, кроме подписи о получении пакетов, должна быть проставлена печать предприятия-получателя. Реестры и полученные расписки не должны иметь гриф конфиденциальности. Их валовая нумерация производится раздельно в течение года. Об отправленных документах производятся соответствующие отметки в учетных формах: в журнале учета изданных документов в графах 12—14, в журнале учета документов выделенного хранения в графах 8—10. При этом если документ отправлен без сопроводительного письма, то в графе «Наименование, номер и дата сопроводительного документа» пишется «реестр», «расписка», «квитанция», 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 учета поступивших документов, то отметка об отправлении проставляется в графе 14 (Примечание) журнала. В ней указываются количество отправленных листов,

куда они направлены, наименование, номер и дата сопроводительного документа, например: «3 листа отправлены в АООТ “Изумруд” по реестру № 6 от 24.03.2016».

Глава 6. Организация конфиденциального делопроизводства

6.1. Подразделения конфиденциального делопроизводства

Организация конфиденциального делопроизводства означает создание необходимых условий для изготовления и получения конфиденциальных документов, организации работы с ними и предотвращения утраты и утечки документированной конфиденциальной информации.

Организация конфиденциального делопроизводства включает создание подразделения, обеспечивающего изготовление, учет, хранение, обработку и использование конфиденциальных документов, установление его статуса, структуры, численного и должностного состава, разработку положения о подразделении и должностных инструкций сотрудников, выделение для подразделения служебного помещения, обеспечение необходимых условий труда, разработку или приобретение нормативных документов и методической литературы по организации и ведению конфиденциального делопроизводства, создание постоянно действующей экспертной комиссии, оформление допуска сотрудников к коммерческой и служебной тайне и обучение их правилам работы с конфиденциальными документами.

Конфиденциальное делопроизводство в силу небольшого по сравнению с открытым делопроизводством объема документов и в целях обеспечения условий для сохранности и конфиденциальности документов должно быть централизованным, т.е. сосредоточенным в едином подразделении предприятия. Подразделение конфиденциального делопроизводства может быть самостоятельным структурным подразделением предприятия, подчиненным непосредственно руководителю предприятия, или входить в состав других подразделений, как правило, осуществляющих защиту конфиденциальной информации: службу безопасности, службу защиты информации и др. В п. 2.2

Положения о порядке обращения со служебной информацией ограниченного распространения» (утвержденном постановлением Правительства РФ от 03.11.1994 № 1233) указано, что прием и учет (регистрация) документов, содержащих служебную информацию ограниченного распространения, осуществляются, как правило, структурными подразделениями, которым поручен прием и учет несекретной документации, однако это целесообразно лишь при незначительном объеме таких документов и при отсутствии документов, содержащих коммерческую тайну.

Наименование подразделения конфиденциального делопроизводства, статус и при необходимости структуру определяет руководитель предприятия, исходя из объема конфиденциального делопроизводства и общей структуры предприятия. Подразделение конфиденциального делопроизводства является составной частью системы защиты коммерческой и служебной тайны, органом, осуществляющим, координирующим и контролирующим работу с конфиденциальными документами. Оно должно рассматриваться как структурное подразделение, непосредственно участвующее в основной деятельности предприятия. 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, например: Укрупненные нормативы времени на работы по делопроизводственному обслуживанию, утвержденные постановлением Госкомтруда СССР и Секретариата ВЦСПС от 20.05.1987 № 327/17-42; Межотраслевые укрупненные нормативы времени на работы по документационному обеспечению управления, утвержденные постановлением Минтруда России от 25.11.1994 № 72, и др. 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. Обоснованное определение численности сотрудников подразделения конфиденциального делопроизводства на основе нормирования их

труда обеспечивает оптимальную загрузку сотрудников, что влечет за собой повышение оперативности и качества работы. Должностной состав сотрудников подразделения конфиденциального делопроизводства должен определяться характером и сложностью выполняемой работы.

Для более многообразной и более сложной работы следует устанавливать и более высокие должности. При определении должностей следует руководствоваться Общероссийским классификатором профессий рабочих, должностей служащих и тарифных разрядов (ОК 016-94), регламентирующим наименования должностей, а также использовать Квалификационный справочник должностей руководителей, специалистов и других служащих, утвержденный постановлением Минтруда России от 21.08.1998 № 37, в котором содержатся квалификационные требования к должностям.

При незначительном объеме конфиденциального делопроизводства специальное подразделение конфиденциального делопроизводства может не создаваться. В этом случае издание, обработка и хранение конфиденциальных документов возлагается на специально назначенных приказом руководителя предприятия нескольких либо одного сотрудник других подразделений, как правило, службы безопасности или, как было сказано, службы открытого делопроизводства, если документы содержат сведения, составляющие только служебную тайну. На этих лиц распространяются все задачи, функции, права и ответственность, возлагаемые на подразделение конфиденциального делопроизводства. Если ведение конфиденциального делопроизводства возложено на одного сотрудника, то для выполнения отдельных делопроизводственных операций, в которых требуется участие двух лиц (проверки наличия, уничтожение документов), необходимо привлекать (лучше на постоянной основе) второго сотрудника данного или другого подразделения, имеющего доступ к этим документам. Такое привлечение оформляется приказом по предприятию. Следует подчеркнуть, что в целях более надежного обеспечения сохранности и конфиденциальности документов на подразделение конфиденциального делопроизводства или на специально выделенных для ведения конфиденциального делопроизводства сотрудников должны быть возложены все операции по печатанию, учету, размножению, хранению, передаче, отправлению, систематизации, проверке наличия и

уничтожению конфиденциальных документов. Функции исполнителей и пользователей конфиденциальных документов в сфере изготовления и обработки документов ограничиваются подготовкой документов и их исполнением. Допустимо и печатание документов исполнителями, если оно осуществляется в специально предназначенном для этого помещении подразделения конфиденциального делопроизводства.

6.2. Организационно-правовые документы, регламентирующие статус подразделения и каждого из его сотрудников. Требования к помещениям и режиму работы

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. В должностных инструкциях устанавливаются и квалификационные требования к сотрудникам — образование и стаж работы на аналогичной должности. Положение о подразделении конфиденциального делопроизводства и должностные инструкции сотрудников являются организационно-правовыми документами, регламентирующими статус подразделения в целом и каждого из его сотрудников. При определении задач и функций подразделения конфиденциального делопроизводства необходимо исходить из того, что оно должно не только организовывать и осуществлять документационное обеспечение конфиденциальной управленческой и производственной деятельности предприятия, но и участвовать во всех мероприятиях по предотвращению утраты конфиденциальных документов и утечки содержащейся в них информации. Это участие не ограничивается разработкой и осуществлением соответствующих мероприятий только в рамках подразделения конфиденциального делопроизводства. Утрата и утечка конфиденциальной информации в большинстве случаев происходят по вине исполнителей и пользователей конфиденциальных документов, нарушающих по разным причинам правила обращения с такими документами.

Поэтому значительная часть функций подразделения конфиденциального делопроизводства связана с обучением исполнителей и пользователей прав работы с конфиденциальными документами и осуществлением контроля за их выполнением. Этим обусловлены и соответствующие права подразделения конфиденциального делопроизводства, в том числе такие: участие в подборе кадров для работы с конфиденциальной информацией, внесение предложений об отстранении от конфиденциальных работ, поощрении и привлечении к ответственности исполнителей и пользователей конфиденциальных документов, участие в проведении расследований по фактам утраты и утечки конфиденциальной информации. В целом комплекс задач, функций, прав и ответственности подразделения конфиденциального делопроизводства вытекает из содержания его работ, изложенных в последующих главах.

При разработке должностных инструкций следует учитывать, во-первых, необходимость специализации сотрудников по отдельным видам работ, что ускоряет их выполнение и повышает качество, и, во-вторых, нормативы времени на работы с тем, чтобы все сотрудники были загружены равномерно в соответствии с должностью и не было перезагруженности, которая отрицательно сказывается на качестве работы, и установлении квалификационных требований к должностям (необходимо иметь в виду сложность выполнения некоторых видов работ, требующих специальной подготовки). На соответствующие таким работам должности следует, как правило, назначать специалистов с высшим или средне-специальным образованием в области защиты информации. В соответствии с законодательством сотрудники подразделения конфиденциального делопроизводства несут дисциплинарную, административную либо гражданско-правовую ответственность за утрату конфиденциальных документов или разглашение содержащейся в них информации, поэтому в должностных инструкциях должна быть установлена персональная ответственность сотрудников за сохранность конфиденциальных документов и содержащейся в них информации. В случаях особой конфиденциальности документов назначение сотрудников на соответствующие должности в подразделение конфиденциального делопроизводства целесообразно осуществлять после проведения в отношении их полномочными органами проверочных мероприятий при письменном согласии на это сотрудников.

Все сотрудники, принимаемые на работу в подразделение конфиденциального делопроизводства, а также при отсутствии подразделения, специально назначенные для ведения конфиденциального делопроизводства лица должны дать письменное обязательство по соблюдению режима конфиденциальности. Это обязательство фиксируется в трудовом договоре (контракте) или специальном соглашении. Сотрудники могут допускаться к работе только после изучения в части, их касающейся, требований действующих на предприятии нормативно-методических документов по вопросам организации и ведения конфиденциального делопроизводства, обеспечения режима конфиденциальности проводимых работ и проверки знаний этих требований соответствующим руководителем. Подразделение конфиденциального делопроизводства должно быть обеспечено служебным помещением (при необходимости — несколькими помещениями) для хранения конфиденциальных документов и работы сотрудников подразделения, а также помещением для исполнителей, если работа с конфиденциальными документами не разрешена в служебных комнатах исполнителей.

В служебном помещении следует создавать и поддерживать необходимые условия труда, включающие совокупность компонентов, обеспечивающих работоспособность и здоровье сотрудников. Эти условия можно подразделить на три группы: состояние служебного помещения, организация трудового процесса, поддержание здорового микроклимата в коллективе. Служебное помещение должно обеспечивать необходимую площадь на каждое рабочее место, быть оснащено удобной мебелью, а также оборудованием и техническими средствами, включая ЭВМ, для оперативного изготовления, размножения, обработки документов, надежного их хранения, быстрого поиска. Благоприятная окраска стен помещения и цветовая гамма интерьера, нормальное освещение, поддержание чистоты, необходимой влажности и температуры воздуха, снижение уровня шума, возникающего при работе некоторых технических средств, оказывают существенное положительное влияние на самочувствие сотрудников и стимулируют их работоспособность. Оснащение служебного помещения должно предусматривать и изготовление необходимых учетных журналов (карточек), бланков документов, печатей, штампов, а также приобретение расходных материалов (бумаги, копировальной

ленты, спецблокнотов, тетрадей и др.). В служебном помещении необходимо иметь средства противопожарной защиты.

Организация трудового процесса включает: разработку технологии выполнения работ, рациональное размещение рабочих мест сотрудников, установление правильного режима труда и отдыха, обеспечение техники безопасности.

Технология выполнения работ складывается из описания содержания работ в последовательности их выполнения. Она может закрепляться в инструкции по конфиденциальному делопроизводству, технологических картах, картах организации трудового процесса или других документах. Рациональное размещение рабочих мест сотрудников предполагает их соответствие технологии выполнения работ, последовательности прохождения документов, взаимосвязям между сотрудниками. Оно должно способствовать и обеспечению персональной ответственности за сохранность документов.

Правильный режим труда и отдыха требует рационального распределения нагрузки в течение рабочего дня, чередования труда и отдыха, проведения при необходимости, психофизической разгрузки. Установление и поддержание здорового микроклимата в коллективе также способствует повышению производительности труда и сохранению здоровья сотрудников. Микроклимат зависит не только от взаимоотношений сотрудников, но и от отношения руководителя к сотрудникам. Непредвзятость со стороны руководителя, равномерная нагрузка сотрудников, оказание им помощи, внимание к их бытовым проблемам, своевременное устранение конфликтных ситуаций создают благоприятную почву для хорошего настроения сотрудников и нормальных, доброжелательных взаимоотношений. Каждый сотрудник подразделения конфиденциального делопроизводства должен быть обеспечен нормативно-методическими документами, регулирующими процесс его деятельности и технологию выполнения работ. К ним относятся документы, перечисляемые в различных главах данной книги, а также методическая литература: книги, брошюры, журналы, которые позволяют найти ответы на вопросы, не отраженные в нормативных документах. На рабочих местах следует иметь и необходимые справочники, включая телефонные.

6.3. Постоянно действующая экспертная комиссия и ее задачи

Важной составной частью организации конфиденциального делопроизводства является создание *постоянно действующей экспертной комиссии* (ПДЭК). Задачами такой комиссии должны быть: разработка перечней сведений, составляющих коммерческую и служебную тайну; разработка перечней издаваемых предприятием конфиденциальных документов; снижение или снятие степени конфиденциальности сведений и грифа конфиденциальности документов; разработка положения о системе доступа к конфиденциальным документам; экспертиза ценности конфиденциальных документов с целью установления сроков их хранения и отбора документов на основе этих сроков для архивного хранения и уничтожения; проведение аналитической работы по предотвращению утечки и утраты конфиденциальной информации.

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 пред-

приятии 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.

Порядок изготовления конфиденциальных документов, режим обращения с ними требуют определенных знаний, которые должны быть приобретены до начала работы с документами и постоянно пополняться. С этой целью необходимо организовывать различные формы обучения сотрудников: техническую учебу, семинары, самостоятельную подготовку со сдачей зачетов и др. Для проведения занятий следует привлекать не только сотрудников подразделения конфиденциального делопроизводства, но и руководителей соответствующих подразделений предприятия, а также специалистов по конфиденциальному делопроизводству, работающих в соответствующих научно-исследовательских и учебных заведениях.

Глава 7. Определение состава конфиденциальных документов

7.1. Определение состава конфиденциальных документов

Документирование конфиденциальной информации включает определение состава внутренних и отправляемых документов и их изготовление. Документирование конфиденциальной информации является важнейшей составной частью конфиденциального делопроизводства, поскольку от количества, состава и правильности оформления документов зависят качество и эффективность управленческой и производственной деятельности, достоверность и юридическая сила документов, трудоемкость их обработки и качество организации. Объем и характер создаваемых документов влияют и на организацию работы по их защите. Кроме того, в процессе документирования создается документальная база, раскрывающая историю предприятия. Ранее было отмечено, что одной из особенностей конфиденциального

делопроизводства является жесткое регламентирование состава издаваемых документов. Обусловлено это тем, что документ является потенциально существующим источником утечки содержащейся в нем информации, т.е. попадания ее в руки тех, кому она не предназначена. Поэтому конфиденциальные документы должны издаваться только при действительной необходимости в письменном удостоверении наличия и содержания управленческих, производственных и иных действий. При этом решение задач конфиденциальной деятельности должно обеспечиваться минимальным количеством документов при сохранении полноты необходимой информации. Но установление состава издаваемых конфиденциальных документов направлено не только на предотвращение необоснованного их издания и на исключение избыточной конфиденциальной информации, но определение количества их экземпляров, адресатов, которым они должны направляться, так как не вызванная действительной необходимостью рассылка конфиденциальных документов также приводит к утечке информации. На стадии определения состава издаваемых документов решается вопрос и о придании им необходимой юридической силы путем установления должностных лиц, которые должны визировать, подписывать и утверждать тот или другой документ.

В конечном итоге *регламентация состава издаваемых конфиденциальных документов* преследует цель не только исключения необоснованного, но и неконтролируемого их издания. Состав документированной конфиденциальной информации зависит от компетенции и функции предприятия, характера его деятельности, взаимосвязей с другими предприятиями, порядка разрешения вопросов. Такой состав закрепляется перечнями издаваемых предприятием конфиденциальных документов, раздельно по документам, отнесенных к коммерческой тайне, и документам, отнесенным к служебной тайне. Но эти перечни должны разрабатываться на основе и в рамках перечней сведений, составляющих коммерческую и служебную тайну. Вызвано это тем, что по существующим нормам сначала определяются сведения, составляющие тот или другой вид тайны. Эти сведения могут быть зафиксированы как в документах, так и в других носителях: памяти человека, базе данных ЭВМ, выпускаемой продукции, технологических процессах, физических полях и др. Поэтому только после определения состава всех конфиденциальных сведений можно уста-

новить те из них, которые должны документироваться. Таким образом, определение состава издаваемых конфиденциальных документов должно начинаться с разработки перечней сведений, составляющих коммерческую и служебную тайну.

7.2. Перечень сведений, составляющих коммерческую тайну

Перечень сведений, составляющих коммерческую тайну, разрабатывается для каждого предприятия самим предприятием — *обладателем информации*. Это вытекает из действующего законодательства, которым установлено, что состав и объем таких сведений определяется собственником информации.

Таким образом, *право предпринимателя на состав коммерческой тайны является безусловным*. Никто не может диктовать ему, какие сведения относить к коммерческой тайне, за исключением сведений, которые не могут составлять коммерческую тайну согласно государственным нормативным актам. Следовательно, состав сведений, относимых к коммерческой тайне, должен устанавливаться и изменяться индивидуально, на уровне их обладателя. В этой связи следует обратить внимание на имеющиеся в научной литературе попытки разработки неких типовых перечней сведений, составляющих коммерческую тайну любой коммерческой структуры независимо от сферы и специфики ее деятельности. Такие попытки не могут иметь успех, поскольку состав конфиденциальной информации в коммерческой сфере определяется исходя из специфики деятельности данного конкретного предприятия: типа предприятия, характера его деятельности, технологии изготовления продукции, объема и себестоимости продукции, состава и количества поставщиков сырья, условий рынка сбыта, направленности интересов конкурентов и т.д. То, что для одних предприятий является коммерческой тайной, для других может не быть таковой и даже использоваться в рекламных целях.

В целом тенденции развития коммерческой тайны направлены на сохранение значения производственной тайны, связанной с новизной и совершенствованием технологических процессов, т.е. с элементами творческой деятельности, и на падение значения тайны финансово-торговой, связанной не с элементами новизны, а с элементами индивидуальности и большей или меньшей степенью исключительности.

Правовым основанием для установления состава сведений, относимых к коммерческой тайне, являются, упоминавшиеся ранее законы (см. стр. 8—9), а также определение понятия «коммерческая тайна», которыми предусмотрено, что сведения, составляющие коммерческую тайну, могут быть в любой сфере предпринимательской деятельности, следовательно, коммерческая тайна может распространяться на все направления и вид деятельности предприятия.

Разработкой перечня сведений, составляющих коммерческую тайну должна заниматься ПДЭК.

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

На втором этапе определяется, какая из установленной информации должна быть конфиденциальной, и отнесена к коммерческой тайне. Базовым критерием при этом является возможность получения преимуществ от использования информации за счет неизвестности ее третьим лицам. Этот критерий имеет как бы две составляющие: неизвестности информации третьим лицам и получение преимуществ в силу этой неизвестности. Данные составляющие взаимосвязаны и взаимообусловлены, поскольку, с одной стороны, неизвестность информации третьим лицам сама по себе ничего не значит, если не обеспечивает преимуществ; с другой — преимущества можно получить только за счет такой неизвестности.

Конфиденциальность является правовой формой и одновременно инструментом обеспечения неизвестности информации. Преимущества от использования информации, не известной третьим лицам, могут состоять в получении выгоды или предотвращении ущерба в зависимости от областей и видов деятельности, экономические, моральные и другие характеристики, выражаться количественными и качественными показателями.

В сфере коммерческой деятельности ценность информации обусловлена, прежде всего, рыночной потребностью в информации как

источнике получения прибыли, поэтому отнесение информации к коммерческой тайне позволяет получить прибыль и предотвратить убытки. Конфиденциальность такой информации создает для ее обладателя преимущества в конкурентной борьбе и выступает как средство защиты от не добросовестной конкуренции. Названный критерий является объективным показателем возможности отнесения информации к коммерческой тайне, мерилom придания информации статуса конфиденциальной. Это означает, что при отсутствии данного критерия нет оснований для перевода информации в категорию конфиденциальной. Но это не означает, что при его наличии информация во всех случаях может и должна быть отнесена к коммерческой тайне.

Законодательством введены два ограничения на отнесение информации к коммерческой тайне (рис. 7.1). Первое ограничение состоит в том, что к коммерческой тайне не может быть отнесена информация, составляющая государственную тайну. Второе ограничение заключается в том, что к коммерческой тайне нельзя относить информацию, которая должна быть общедоступной в целях предупреждения сокрытия правонарушений и предотвращения нанесения ущерба законным интересам государства, физических или юридических лиц.



Рис. 7.1. Сведения, которые не могут составлять коммерческую тайну

Перечни такой информации содержатся в Федеральных законах «Об информации, информатизации и защите информации», «О благотворительной деятельности и благотворительных организациях» и др.

Эти перечни в значительной мере дублируют друг друга и имеют различную правовую основу. В Федеральном законе «О коммерческой тайне» имеется специальная ст. 5 «Информация, которая не может составлять коммерческую тайну». В этой статье обобщены и дополнены сведения, содержащиеся в ранее изданных нормативных актах. Запрещение относить к коммерческой тайне ту или иную информацию не означает, что всю ее может получить по требованию любое юридическое или физическое лицо. Часть ее, затрагивающая законные интересы этих лиц, безусловно, должна им предоставляться, а часть предоставляется лишь соответствующим органам власти, наделенным законодательством правом контроля такой информации.

Должно быть и третье ограничение, которое хотя и не предусмотрено законодательством, но диктуется здравым смыслом. Оно состоит в том, что при переводе информации в разряд коммерческой тайны необходимо учитывать сопутствующие этому затраты на ее защиту. Если эти затраты превышают достигаемые в результате защиты количественные и качественные показатели, то придание информации статуса конфиденциальной теряет всякий смысл. Следует иметь в виду, что в перечень сведений, составляющих коммерческую тайну, может включаться не только информация, создаваемая данным предприятием, но и информация, полученная им без использования неправомερных средств при проведении исследований по собственной инициативе, систематических наблюдений и сбора сведений. Такая информация считается полученной правоммерно и самостоятельно независимо оттого, что ее содержание может совпадать с содержанием коммерческой тайны другого юридического или физического лица. Кроме того, правоммерно полученной считается конфиденциальная информация, полученная от ее обладателя на основании договора или в результате правопреемства.

Предприятие, правоммерно и самостоятельно получившее информацию, одновременно являющуюся коммерческой тайной другого юридического или физического лица, становится обладателем этой коммерческой тайны со всеми предусмотренными законодательством правами. После установления состава конфиденциальной 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. В практике работы предприятий применяются от одной до нескольких степеней конфиденциальности информации с различными их наименованиями. Наиболее распространенным является деление информации на две степени: конфиденциально и строго конфиденциально. Однако Законом «О коммерческой тайне» установлена одна степень конфиденциальности с названием «Коммерческая тайна», свидетельствующая лишь о принадлежности информации к коммерческой тайне. Правда, в проекте Закона это названо не степенью, а грифом коммерческой тайны, но суть дела от этого не меняется, поскольку, по определению, гриф конфиденциальности — это реквизит, свидетельствующий о степени конфиденциальности сведений, содержащихся в их носителе, проставляемый на самом носителе и (или) в сопроводительной документации на него. Наименование грифа должно соответствовать наименованию степени конфиденциальности. Установление одной степени (одного грифа) конфиденциальности информации, составляющей коммерческую тайну, обусловлено, вероятно, тем, что степень конфиденциальности определяется собственниками информации, которые могут иметь (а зачастую так, и бывает) разные подходы к степени конфиденциальности однотипной по содержательной части информации. В этом случае при рассмотрении в судебном порядке дел о неправомерном получении коммерческой тайны сложно определить, кто из собственников установил правильную степень конфиденциальности информации, так как критерии отнесения информации к той или другой степени конфиденциальности выбирает ее собственник. В то же время сведение информации, требующей разного уровня закрытости, к одной степени конфиденциальности не позволяет выделить наиболее значимую информацию с целью установления для нее более жесткого, по сравнению с менее значимой, режима защиты. Но закон есть закон, а в Федеральном законе «О коммерческой тайне» сохраняется одна степень конфиденциальности, выход может быть в разделении информации по степеням конфиденциальности на внутреннюю и отправляемую. Информация, не подлежащая отправлению на другие предприятия, может иметь несколько степеней и наименований конфиденциальности, а отправляемая — одну степень «Коммерческая тайна». При использовании на предпри-

ятии одной степени конфиденциальности этот этап работы ПДЭК выпадает.

Следующий этап — определение конкретных сроков конфиденциальности информации либо обстоятельств и событий, при наступлении которых конфиденциальность снимается. Продолжительность конфиденциальности информации должна соответствовать срокам действия условий, необходимых и достаточных для признания данной информации конфиденциальной в соответствии с законодательством. Результаты работы оформляются перечнем сведений, составляющих коммерческую тайну, который может иметь следующую форму:

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

Если сведениями установлена одна степень конфиденциальности, то графа 3 опускается. При значительном объеме конфиденциальных сведений они классифицируются в перечне по разделам, соответствующим сферам деятельности предприятия. Перечень подписывается председателем и всеми членами ПДЭК, утверждается и вводится в действие приказом руководителя предприятия. В приказе должны быть определены мероприятия по обеспечению функционирования перечня и контролю его выполнения. С приказом и перечнем необходимо ознакомить под расписку всех сотрудников предприятия, работающих с конфиденциальной информацией. Копии перечня или выписки из него должны быть направлены конфидентам (владельцам) данной коммерческой тайны. Ими являются физические или юридические лица, которым в силу служебного положения, договора либо на ином законном основании известна коммерческая тайна ее обладателя. Дополнения и изменения состава, включенных в перечень сведений, а также изменение степени их конфиденциальности могут осуществляться с разрешения руководителя предприятия и вноситься в перечень за подписями руководителя подразделения по принадлежности сведений и руководителя службы безопасности. При существенном изменении состава сведений перечень должен составляться заново. Об изменениях в составе коммерческой тайны обладатель

информации обязан в письменной форме известить конфидентов данной информации.

Что касается состава информации, являющейся служебной тайной, то следует иметь в виду, что такая информация предусмотрена для органов государственной и муниципальной власти и подведомственных им предприятий, в коммерческих структурах она используется главным образом лишь *при переписке с органами власти*. В «Положении о порядке обращения со служебной информацией ограниченного распространения» сказано, что руководитель федерального органа исполнительной власти в пределах своей компетенции определяет категории должностных лиц, уполномоченных относить служебную информацию к разряду ограниченного распространения, а эти лица несут персональную ответственность за обоснованность такого отнесения. Как видно из этой нормы, она не содержит технологии определения состава информации, относимой к служебной тайне. На практике, которая существует уже несколько десятилетий, используются обычно два варианта определения состава такой информации. В первом варианте министерства и ведомства разрабатывают единые для отрасли перечни сведений ограниченного распространения и направляют их на подведомственные предприятия. Во втором варианте полномочия по разработке перечней передаются руководителям подведомственных предприятий, и перечни разрабатываются применительно к каждому конкретному предприятию. Иногда используется и третий, комбинированный вариант, при котором перечни разрабатывают и министерства (ведомства), и на основе этих перечней — подведомственные предприятия. Технология разработки перечней сведений ограниченного распространения практически не отличается от технологии разработки перечней сведений, составляющих коммерческую тайну. Служебная тайна может быть в любой области деятельности органа власти или предприятия, однако в упомянутом Положении определен состав сведений, которые не могут быть отнесены к служебной информации ограниченного распространения.

7.3. Критерии документирования информации

Сведениям, составляющим служебную тайну, установлена одна степень конфиденциальности: «Для служебного пользования». Пере-

чень таких сведений имеет форму перечня сведений, составляющих коммерческую тайну, без графы 3. Перечни сведений, составляющих коммерческую и служебную тайну, раскрывают тематическое содержание включенных в них сведений. Но эти сведения, как уже отмечалось, фиксируются в различном виде на различных носителях и могут быть как документированными, так и не документированными.

В сферу конфиденциального делопроизводства входит только документированная информация (документы), поэтому из всей совокупности информации, включенной в перечни сведений, отнесенных к коммерческой и служебной тайне, нужно выделить состав документируемой информации и установить виды документов, в которых она должна быть зафиксирована. Определение состава конфиденциальных документов должно осуществляться также ПДЭК.

При этом следует руководствоваться определенными критериями документирования информации. К ним относятся:

- необходимость документированной информации для правового обеспечения деятельности предприятия, регламентирующего статус предприятия, права, обязанности и ответственность его сотрудников;
- необходимость документированной информации для производственной деятельности: научно-исследовательской, конструкторской, проектной, технологической и др.;
- необходимость документированной информации для управленческой деятельности;
- необходимость документированной информации как доказательного источника на случаи возникновения конфликтных ситуаций;
- необходимость передачи информации в официальном виде;
- важность информации как исторического источника, раскрывающего направления и особенности деятельности предприятия.

В рамках критериев документирования *определение состава документируемой информации* увязывается с решением конкретных задач. В зависимости от назначения документируемой информации определяются конкретные виды документов, в которых эта информация должна быть зафиксирована. В процессе определения необходимых конфиденциальных документов следует проводить работу по сокращению их количества за счет разработки интегральных документов, в которые можно включить показатели нескольких документов, в том числе путем замены разовых первичных документов нако-

пительными. Однако объединение документов должно осуществляться с таким расчетом, чтобы в итоге не создавалась возможность необоснованного ознакомления со всем документом лиц имеющих доступ только к части содержания (показателей) документа. Виды конфиденциальных документов необходимо устанавливать с учетом оптимального объема содержащейся в них информации, исключающего избыточную, в том числе дублетную информацию, поскольку избыточная информация — это конфиденциальные данные, утечка которых может нанести ущерб предприятию. После установления состава документов определяются круг лиц, имеющих право составлять, визировать и подписывать (утверждать) тот или другой вид документа, а также предприятия, которым данный документ должен направляться. Перечни издаваемых конфиденциальных документов составляются раздельно по каждому виду тайны и могут иметь следующую форму:

№ п/п	Наименования документов	Гриф конфиденциальности	Срок конфиденциальности	Инициалы и фамилии лиц, имеющих право составлять документы	Инициалы и фамилии лиц, визирующих документы	Инициалы и фамилии лиц, имеющих право подписывать и утверждать документы	Количество изготовляемых экземпляров документов	Куда направляются	Примечания
1	2	3	4	5	6	7	8	9	10

Грифы и сроки конфиденциальности документов должны соответствовать степеням и срокам конфиденциальности включаемых в документы сведений, определенным перечнями сведений, составляющих коммерческую и служебную тайну. При установлении таким сведениям одной степени конфиденциальности графа «Гриф конфиденциальности» опускается. Если документ подлежит утверждению, то в графе 7 сначала проставляются инициалы и фамилия лица (лиц), подписывающего документ, затем после слова «утв.» — инициалы и

фамилия лица, утверждающего документ. При значительном количестве утверждаемых документов Графа 7 может быть разделена на две графы: «Инициалы и фамилии лиц, имеющих право подписывать документы» и «Инициалы и фамилии лиц имеющих право утверждать документы».

К числу документов, *подлежащих утверждению* в соответствии с существующими нормативными актами, относятся: уставы, положения о представительствах, филиалах и структурных подразделениях предприятия, структура, штатное расписание, должностные инструкции, акты проверок (ревизий), сметы, расценки на проведение работ и оказание услуг, и некоторые другие. Если при направлении документов другим предприятиям каждый адресат не должен знать, кому еще направлен данный документ, то в графе 9 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 10 следует использовать (при необходимости) для указания периодичности составления документов, а также для пометки о проставлении оттиска печати на соответствующих документах.

Перечни издаваемых документов подписываются председателем и всеми членами ПДЭК и утверждаются руководителем предприятия. С перечнями под расписку должны быть ознакомлены все лица, наделенные правом составлять, визировать, подписывать и утверждать соответствующие документы. Внесение возможных последующих частичных уточнений или изменений в перечни может быть возложено на руководителя службы безопасности. При изменении перечней сведений, составляющих коммерческую и служебную тайну, соответствующие изменения вносятся и в перечни издаваемых конфиденциальных документов. О снятии грифа конфиденциальности с отправленных документов должны быть письменно оповещены предприятия-адресаты.

В случаях возникновения необходимости *издания разовых документов*, не включенных в перечни, или дополнительных экземпляров документов, не предусмотренных перечнями, их изготовление может производиться по совместному разрешению руководителей соответствующего подразделения и службы безопасности (или подразделе-

ния конфиденциального делопроизводства). Одновременно определяется целесообразность включения таких документов (дополнительных экземпляров) в соответствующий перечень.

Глава 8. Подготовка и издание конфиденциальных документов

8.1. Оформление и учет носителей конфиденциальной информации

Проекты конфиденциальных документов, как и проекты открытых документов, печатаются или с черновика, на котором они составлены, или с текста, нанесенного на иной носитель информации, или без использования того и другого. Черновики и проекты (беловики) открытых документов не регистрируются, *регистрируется уже готовый подписанный (утвержденный) документ, а его черновик (при наличии) уничтожается исполнителем* (составителем) документа без отражения в регистрационных формах факта уничтожения. На некоторых предприятиях поступают таким же образом и с черновиками конфиденциальных документов, в лучшем случае в учетных формах производится отметка об уничтожении черновика, представленного исполнителем, как это предусмотрено «Положением о порядке обращения со служебной информацией ограниченного распространения». Однако это нередко приводит к тому, что при составлении нескольких вариантов черновика с отметкой в учетных формах уничтожается только вариант, с которого печатался проект документа, остальные варианты просто выбрасываются в мусорную корзину или хранятся у исполнителя.

Случается, что и единственный вариант черновика по ошибке выбрасывается вместе с черновиками открытых документов. Это может привести и приводит к тому, что *безучетные*, а потому и *бесконтрольные черновики* попадают в чужие руки. Но эти черновики содержат конфиденциальную информацию, и в результате такого обращения с ними происходит утечка информации, что наносит ущерб ее собственнику. Поиск неучтенных черновиков зачастую не достигает положительных результатов. Поэтому все носители, предназначенные

для составления черновиков и проектов конфиденциальных документов, следует *учитывать предварительно, до внесения в них записей.*

Все сказанное в равной степени относится и к отпечатанным проектам конфиденциальных документов независимо от того, с черновика они печатались или без его использования, поскольку может быть несколько вариантов проекта, отдельные листы проекта могут перепечатываться, может меняться и количество экземпляров проекта, безучетное циркулирование вариантов, перепечатанных листов, экземпляров проекта также создает возможность для утечки содержащейся в них информации. Следовательно, должны учитываться и проекты конфиденциальных документов на стадии их изготовления. Учет черновиков и проектов позволяет предотвращать неправомерное обращение с ними и, кроме того, обеспечивать контроль за подготовкой документов и их соответствием перечням издаваемых конфиденциальных документов. Учет носителей, используемых для составления конфиденциальных документов, осуществляется подразделением конфиденциального делопроизводства.

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

Бумажными носителями могут быть: для текстовых документов — спецблокноты, отдельные листы бумаги, типовые формы документов, стенографические и рабочие тетради; для чертежно-графических документов — ватман, калька, миллиметровка (координатная бумага). Спецблокнот предназначен для составления черновиков документов. Он представляет собой сброшюрованные и пронумерованные листы бумаги с линией отрыва и контрольным листом, в котором проставляются номера листов блокнота. Стенографическая тетрадь используется для стенограмм, рабочая тетрадь (сброшюрованные листы бумаги без линии отрыва) — как правило, для различных рабочих справочных записей, хотя в ней допускается составлять черновики отдельных больших по объему документов. Остальные носители могут использоваться как для составления черновиков, так и для печатания или рукописного изготовления проектов документов. При этом типовые формы документов — бланки с трафаретным текстом — должны содержать только открытую информацию и иметь в соответствующих местах пропуски для последующего внесения конфиденциальной информации, как пра-

вило, количественного характера. Перед взятием на учет носители должны быть оформлены следующим образом. На обложках спецблокнотов сотрудник подразделения конфиденциального делопроизводства пишет или проставляет штампом (если не проставлено типографским способом) слово «Спецблокнот» и в правом верхнем углу гриф конфиденциальности. Если листы спецблокнота не пронумерованы типографским способом, то они нумеруются сотрудником подразделения конфиденциального делопроизводства. На обложках рабочих и стенографических тетрадей указываются вид носителя, гриф конфиденциальности, инициалы и фамилия исполнителя. Листы тетрадей нумеруются, на обороте последнего листа составляется, подписываемая сотрудником подразделения конфиденциального делопроизводства, завершительная надпись с указанием количества листов в тетради. Листы типовых форм документов нумеруются исполнителем, на первом листе проставляется гриф конфиденциальности.

На отдельных листах бумаги, ватмана, миллиметровки, кальки в соответствующих графах основных надписей штампов или других установленных местах исполнителем проставляются: на всех носителях — гриф конфиденциальности, номера листов; дополнительно на носителях, предназначенных для чертежно-графических документов — количество листов, подразделение и фамилия исполнителя. На любом носителе предназначенном для составления одного конкретного документа, указывается наименование этого документа. Бумажные носители учитываются в журналах или карточках, имеющих следующие графы:

Учетный номер и гриф конфиденциальности носителя	Дата регистрации	Виды носителя	Наименование или назначение носителя	Количество листов	Фамилия лица, получившего носитель	Подпись за получение и дата	Подпись за возврат и дата	Отметка об уничтожении носителя
1	2	3	4	5	6	7	8	9

При взятии носителей на учет заполняются графы 1—5. В графе 1 рядом с номером носителя начальными буквами (аббревиатурой) проставляется его гриф конфиденциальности: КТ (коммерческая тайна), ДСП (для служебного пользования). Если издаваемые документы имеют только один гриф конфиденциальности, то в наименовании графы 1 слова «и гриф конфиденциальности» опускаются, рядом с номерами носителей гриф не проставляется. В графе 2 дата проставляется арабскими цифрами: в картонке 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 документа, который будет составляться на носителе, если носитель предназначен для составления конкретного документа, или назначение носителя, если в него будет вноситься различная информация, например, по спецблокноту — «для черновиков», по рабочей тетради — «для рабочих записей». Одновременно на самих носителях проставляется: — на спецблокнотах: в верхнем левом углу лицевой стороны обложки штамп с указанием учетного номера и количества листов, на каждом листе в верхнем левом углу — учетный номер; — на рабочих и стенографических тетрадях: в верхнем левом углу лицевой стороны обложки (а при невозможности — в верхнем левом углу форзаца) такой же штамп с указанием учетного номера и количества листов; — на отдельных листах бумаги, типовой формы документа, ватмана, кальки, миллиметровки: в верхней части левого поля первого листа такой же штамп с указанием учетного номера и количества листов (на носителях чертежно-графической информации — только учетного номера); на левом поле остальных листов штамп «К Уч. №» с указанием номера.

Уч.	№
Кол-во ли ст ов	

После взятия на учет носитель передается исполнителю с заполнением граф 6, 7 журнала учета бумажных носителей. При необходимости взятия 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 бумажных носителей за тем же номером, что и ранее взятые листы, отдельной строкой под ними (при этом заполняются графы 2,5), на левом поле каждого листа проставляется штамп «К Уч. №» с указанием номера, а на первом листе всего носителя прежнее количество листов зачеркивается и проставляется новое с учетом дополнительных листов. Исправление заверяется подписью сотрудника подразделения конфиденциального делопроизводства. Выдача дополнительных листов производится под отдельную подпись в графе 7 журнала учета бумажных носителей. Машинные носители информации необходимы при изготовлении проектов документов при помощи печатающих устройств ЭВМ (независимо от того, с черновика печатаются проекты или без его использования), поскольку распечатка документа производится с машинного носителя.

К *машинным носителям документированной информации* относятся: жесткие (твердые) магнитные диски; гибкие магнитные диски (дискеты); магнитные ленты; магнитооптические диски; оптические диски. ЭВМ, используемые для изготовления конфиденциальных документов учитываются службой безопасности предприятия. 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:

Учетный номер и гриф 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 отдельно. 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. 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.

8.2. Изготовление и учет проектов конфиденциальных документов

Проекты конфиденциальных документов могут изготавливаться рукописным способом, на пишущей машинке или при помощи печатающих устройств средств вычислительной техники. Рукописным способом допускается готовить отдельные текстовые внутренние документы, авторами которых являются должностные лица (докладные записки, справки и др.), а также вносить переменную часть в типовые формы документов. Проекты других текстовых документов изготавливаются печатным способом либо с черновика, либо с другого носителя, включая звуковоспроизводящие устройства, либо под диктовку, либо непосредственно исполнителем. Проекты чертежно-

графических документов могут изготавливаться как рукописным способом, так и печатным, с помощью компьютера. Печатание проектов конфиденциальных документов следует осуществлять в подразделении конфиденциального делопроизводства. Используемые для печатания средства вычислительной техники и электрические пишущие машинки должны быть защищены от перехвата излучаемых ими сигналов. При любом способе изготовления (рукописном, печатном) проект документа должен иметь все необходимые и правильно оформленные реквизиты. 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 быть 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 стенографической или рабочей тетради — проверить наличие листов тетради и соответствие их количества заверительной надписи.

Если проект печатается с другого документа, то просчитывается количество листов и того документа. В предыдущем подразделе было отмечено, что проекты конфиденциальных документов должны учитываться на стадии их изготовления, и сказано, чем это вызвано. Поэтому после приема носителя (черновика) производится присвоение учетного номера проекту документа, который будет напечатан с этого носителя. Поскольку номер, присвоенный проекту, становится и номером документа после оформления проекта, учетные номера проектов проставляются в журналах (карточках) учета изданных конфиденциальных документов, которые ведутся отдельно по документам, составляющим коммерческую и служебную тайну, и имеют следующие графы:

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

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 предприятием документы не переводятся на учет документов выделенного хранения, 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 носителя, и аббревиатурой его гриф конфиденциальности. Внутренние документы и документы, подлежащие отправлению на другие предприятия, учитываются по единой валовой нумерации. В графе 5 проставляются учетный 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 подразделения конфиденциального делопроизводства и даты, например:

№ п/п	Учетные номера документов	Подпись, дата		№ п/п	Учетные номера документов	Подпись, дата
1	4			2		
2				6		
2	8			.		
.				.		
.				.		
2				.		
5				5		
				0		

Спецблокнот возвращается исполнителю, а за получение отдельных листов бумаги, типовой формы документа, стенографической или рабочей тетради, документа, с которого должен печататься проект, сотрудник подразделения конфиденциального делопроизводства выдает разовую расписку по следующей форме (бланки расписок тиражируются в необходимом количестве экземпляров):

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

При печатании проекта документа, в том числе при производстве распечаток, на каждом листе каждого экземпляра документа проставляется учетный номер, присвоенный проекту по журналу учета из-

данных документов, в порядке, который будет изложен в следующем подразделе. После печатания проекта документа заполняются графы 8—7 журнала учета 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 подразделения конфиденциального делопроизводства и уничтожается. При необходимости перепечатывания отдельных листов проекта документа без изменения общего количества листов от исполнителя принимаются по разовой расписке все экземпляры подлежащих перепечатыванию листов. Вновь отпечатанные листы передаются исполнителю взамен разовой расписки.

При необходимости перепечатывания проекта документа с изменением количества листов перепечатывание производится за новым учетным номером. От исполнителя принимаются правленный 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 первоначального проекта, при этом в графе 5 указывается «С № ____» с проставлением номера перепечатываемого проекта без указания номеров листов в нем. При изготовлении дополнительных экземпляров проекта документа (в случае возникновения необходимости в них) в графе 6 журнала учета изданных документов под ранее произведенной записью через знак «+» проставляется количество дополнительно изготовленных экземпляров. Нумерация дополнительных экземпляров проекта 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 бумажных носителей, или сразу по журналу учета изданных документов. В последнем случае заполняются графы 1, 3, 7 (в графе 5 пишется слово «рукопись»). Если проект документа был отпечатан как открытый, а в процессе визирования или подписания принято решение о переводе его в разряд конфиденциальных, то исполнителем должны быть представлены в подразделение конфиденциального 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 предприятия 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 предприятия для принятия соответствующих решений. Фактически представленные экземпляры проекта документа и черновик регистрируются в журнале учета изданных документов в графах 1, 3, 7. В графе 5 при наличии черновика пишется «засекречено ____ л.» с указанием количества листов черновика, на черновике проставляется гриф конфиденциальности и учетный номер проекта документа. При отсутствии черновика в графе 5 указывается «б/ч» (без черновика). Проект документа оформляется в соответствии с правилами, предъявляемыми к конфиденциальным документам, и выдается вместе с черновиком (при наличии) исполнителю под подпись в графе 8.

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

Сотрудник подразделения конфиденциального делопроизводства расписывается за получение документа (проекта) и черновика в графе 9 журнала учета изданных документов, одновременно проставляя в графе 2 дату документа, которая должна соответствовать дате его подписания (утверждения). Черновик, проект (как неподписанный, так и перепечатанный), лишние экземпляры документа разрываются и помещаются в находящуюся в подразделении конфиденциального делопроизводства урну. В графе 10 журнала учета изданных документов пишется слово или проставляется штамп «Уничтожен», заве-

ряемый подписью сотрудника подразделения конфиденциального делопроизводства с проставлением даты. В графе 11 при уничтожении проекта документа пишется слово или проставляется штамп «Проект уничтожен», а при уничтожении лишних экземпляров документа — «Экз. № _____ уничтожены» с указанием номеров экземпляров. Эти отметки заверяются подписью сотрудника подразделения конфиденциального делопроизводства с проставлением даты. В графе 9 журнала учета бумажных носителей производится отметка об уничтожении носителя (кроме спецблокнотов) в качестве черновика изданного документа (проекта). Отметка оформляется следующим образом: «Уничтожен как черновик документа № _____» с указанием номера изданного документа (проекта).

Если носитель не являлся черновиком, а уничтожается по каким-либо другим причинам, то он помещается в урну, а в графе 9 журнала учета бумажных носителей пишется слово или проставляется штамп «Уничтожен». И в первом, и во втором варианте отметка об уничтожении заверяется подписями двух сотрудников подразделения конфиденциального делопроизводства с указанием даты. Испорченные, не являющиеся черновиком листы спецблокнота, если он предназначен для использования несколькими исполнителями, должны изыматься из спецблокнота и помещаться в урну после возврата спецблокнота каждым исполнителем с отметкой об уничтожении в контрольном листе спецблокнота, заверяемой подписью сотрудника подразделения конфиденциального 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 проверяется наличие отметок и подписей о номерах документов или уничтожении испорченных листов, обложка спецблокнота с корешками и изъятыми листами и с испорченными листами, если они не были уничтожены ранее, помещается в урну, а в графе 9 журнала

учета бумажных носителей пишется слово или проставляется штамп «Уничтожен», заверяемый подписями двух сотрудников подразделения конфиденциального делопроизводства, с указанием даты.

Испорченные листы бумаги, ватмана, кальки, миллиметровки уничтожаются как листы черновика. Кроме того, в урну должны помещаться без проставления отметок об уничтожении отдельные перепечатанные листы проекта документа, а также использованные при печатании документов копировальная бумага, красящая лента, прокладки, так как в них отображена конфиденциальная информация. Содержимое урны (макулатура) в последующем уничтожается двумя сотрудниками подразделения конфиденциального делопроизводства путем сжигания. 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. Об уничтожении макулатуры следует составлять акт по следующей форме:

<p>Мы, нижеподписавшиеся, _____ (должности, инициалы, фамилии сотрудников подразделения конфиденциального делопроизводства) составили настоящий акт в том, что нами "____"_____20... г. произведено уничтожение путем сжигания макулатуры, образовавшейся в процессе изготовления конфиденциальных документов за период с "____"_____20... г. по "____"_____20... г., находившейся в урне, опечатанной печатью № _____</p> <p>_____.</p> <p>_____.</p> <p>(подписи)</p>

Макулатура может уничтожаться и с помощью бумагорезательной машины, как правило, также после проведения квартальной проверки наличия документов. При этом листы должны быть разрезаны на куски, гарантирующие невозможность восстановления текста. При уничтожении таким способом тоже следует составлять акт об уничтожении с заменой в тексте слова «сжигания» на слова «измельчения машиной».

8.3. Оформление издаваемых конфиденциальных документов

Изготовленный проект чертежно-графического документа оформляется исполнителем в соответствии с требованиями по оформлению и после подписания соответствующими лицами передается в подразделение конфиденциального делопроизводства с погашением подписи исполнителя по месту регистрации: в графе 8 журнала учета бумажных носителей или графе 9 журнала учета изданных документов. Если изданный конфиденциальный документ подлежит отправлению с сопроводительным письмом, то оно составляется и оформляется в изложенном выше применительно к текстовым документам порядке, регистрируется за самостоятельным учетным номером, на нем проставляется гриф конфиденциальности, соответствующий грифу конфиденциальности приложения, независимо от того, содержит или нет само сопроводительное письмо конфиденциальные данные. При наличии нескольких приложений с разными грифами конфиденциальности гриф конфиденциальности сопроводительного письма устанавливается по наивысшему грифу приложений.

Регистрация сопроводительного письма за самостоятельным учетным номером обусловлена тем, что сопроводительное письмо, как правило, составляется и печатается не одновременно с приложениями, а позже, тогда как каждому конфиденциальному документу учетный номер присваивается на стадии его печатания. К тому же с сопроводительным письмом могут быть отправлены не только документы, зарегистрированные по журналу учета изданных документов, но и по другим видам учета. Необходимость проставления на сопроводительном письме грифа конфиденциальности вызвана тем обстоятельством, что без соблюдения этого требования подавляющее большинство сопроводительных писем будут не конфиденциальными, а открытыми, но поскольку документы отправляются за номерами сопроводительных писем, то формально и конфиденциальные приложения окажутся открытыми, со всеми вытекающими последствиями для их сохранности и конфиденциальности. При этом следует исходить из того, что сопроводительные письма необходимы лишь в случаях, когда в них содержатся какие-либо пояснения к прилагаемому документу. Подразделение конфиденциального делопроизводства наряду с руководителями соответствующих подразделений должно

осуществлять контроль за соответствием документов перечням издаваемых конфиденциальных документов. Необходимость такого контроля обусловлена тем, что составители документов нередко допускают отступления от перечней.

Эти отступления осуществляются по следующим направлениям:

— завышение или занижение грифа конфиденциальности документов;

— проставление грифа конфиденциальности на документах, не содержащих конфиденциальных сведений; — необоснованное включение конфиденциальной информации в документы и превращение тем самым открытых документов в конфиденциальные;

— неправильное адресование документов;

— непоставление грифа конфиденциальности на документах, содержащих конфиденциальную информацию.

Завышение или занижение грифа конфиденциальности документов осуществляется составителями документов механически или из-за плохого знания перечней издаваемых конфиденциальных документов. Проставление грифа конфиденциальности на документах, не содержащих конфиденциальной информации, т.е. необоснованное засекречивание документов, также иногда осуществляется по указанным причинам, но чаще всего происходит с целью избежать гласности, оградить себя от критики, скрыть недостатки и даже преступные деяния. Делается это и для придания «веса» документу, обеспечения дополнительной гарантии его сохранности при пересылке.

Засекречивание документов за счет включения в них не вызываемой необходимостью конфиденциальной информации осуществляется либо с целью получения перечисленных в предыдущем абзаце преимуществ, либо для перестраховки составителя документа, старающегося оградить себя от возможных претензий и поэтому включающего избыточную информацию на всякий случай, либо в силу слабой компетенции составителя в излагаемом вопросе, незнания, какой информацией располагает корреспондент. Следует иметь в виду, что засекречивание документов производится иногда по формальному признаку — при ответах или ссылках на конфиденциальные документы, что также необоснованно, так как гриф конфиденциальности должен определяться степенью конфиденциальности информации, содержащейся только в издаваемом документе (за исключением сопроводительных писем).

Неправильное адресование документов происходит также из-за плохого знания перечней или невнимательности и заключается в предоставлении в документе адресата, к которому документ не имеет отношения, а следовательно, не должен ему направляться, либо в перечислении на каждом экземпляре документа всех адресатов, которым направляете документ, в случаях, когда одни адресаты не должны знать, что данный документ направлен другим адресатам, и поэтому требуется их раздельное проставление на соответствующих экземплярах документа.

Непроставление грифа конфиденциальности на документах, содержащих конфиденциальную информацию, тоже чаще всего имеет своей причиной невнимательность или плохое знание перечней издаваемых конфиденциальных документов, хотя бывают случаи сознательного необоснованного незасекречивания документов. Поскольку такие документы создаются в подразделении открытого делопроизводства, контроль за их изданием должен возлагаться не на подразделение конфиденциального делопроизводства, а на другие подразделения службы безопасности. Необходимо иметь в виду, что перечисленные направления нарушения конфиденциальности документов могут быть вызваны и недостаточной полнотой и конкретностью перечней издаваемых конфиденциальных документов, поэтому следует проводить систематический анализ их качества.

Глава 9. Общие требования к учету документов

9.1. Общие требования к учету конфиденциальных документов

Учет конфиденциальных документов является одной из важнейших составных частей конфиденциального делопроизводства. В открытом делопроизводстве вместо термина «учет» употребляется термин «регистрация», которая, согласно Типовой инструкции по делопроизводству в федеральных органах исполнительной власти, представляет собой «запись учетных данных о документе по установленной форме, фиксирующая факт его создания, отправления или получения». Основная цель регистрации — построение поисковой системы по документам. В конфиденциальном делопроизводстве запись

учетных данных о документе не сводится только к фиксации факта его создания, отправления или получения и является не только основой построения поисковой системы по документам, хотя и то, и другое относится к целям записи.

Важнейшая цель записи учетных данных состоит в обеспечении сохранности конфиденциальных документов и предотвращении таким образом утечки содержащейся в документах информации. Для достижения этого в регистрационных формах необходимо фиксировать не только данные о самом документе, включая количество его экземпляров и листов, поскольку утрата экземпляра или отдельных листов при безучетном их хранении зачастую приводит и к утечке конфиденциальной информации, но и любое движение и местонахождение документа, что позволяет, помимо расширения справочно-поисковых данных о документе, обеспечивать персональную ответственность за его сохранность и качественно проводить проверки наличия документов с целью своевременного обнаружения их возможных утрат. Поэтому применительно к конфиденциальным документам употребляется термин «учет», так как он является более емким и не сводится только к фиксации данных о реквизитах документа. Учет конфиденциальных документов осуществляется подразделением конфиденциального делопроизводства.

В «Положении о порядке обращения со служебной информацией ограниченного распространения» записано, что при небольшом объеме документов с грифом (пометкой) «Для служебного пользования» их учет разрешается вести совместно с несекретными документами. Однако формы учета несекретных документов не отражают всех показателей, необходимых для учета документов с грифом «Для служебного пользования», что создает условия для утраты документов. К тому же при совместном учете усложняется работа по регистрации, проведению проверок наличия, поиску, систематизации документов, содержащих служебную тайну. Поэтому оптимальным вариантом является раздельный учет несекретных и с грифом «Для служебного пользования» документов. Учет документов, содержащих коммерческую тайну, осуществляется отдельно от документов, содержащих служебную тайну. Учету подлежат все без исключения изготовленные на предприятии и полученные им конфиденциальные документы.

Учет конфиденциальных документов подразделяется на три вида: изданных документов, поступивших документов и документов выделенного хранения.

Учет изданных документов охватывает документы, изготовленные на данном предприятии рукописным, машинописным способами или с использованием печатающих устройств ЭВМ, независимо от того, направляются эти документы на другие предприятия или являются внутренними.

Учет поступивших документов охватывает документы, поступившие от других предприятий, за исключением тех из них, которые без присвоения им регистрационного номера по этому виду учета сразу переводятся на учет документов выделенного хранения.

Учет документов выделенного хранения охватывает все документы, не подлежащие подшивке в дела. В открытом делопроизводстве нет такого вида учета. Документы, которые по различным причинам не подшиваются в дела, передаются в библиотеку, технический архив или соответствующие производственные подразделения.

В конфиденциальном делопроизводстве в силу того, что оно распространяется не только на управленческую, но и на научно-техническую документацию и учет этой документации осуществляется в одном подразделении, документы, не подлежащие подшивке в дела, ставятся или переводятся на учет документов выделенного хранения. Эти документы можно разделить на две категории.

К первой относятся документы, которые по производственным условиям нецелесообразно подшивать в дела. Например, различного рода технологические инструкции, с которыми параллельно работают несколько исполнителей. При подшивке их в дело исполнитель, взявший дело, лишает остальных исполнителей возможности пользоваться необходимыми им инструкциями.

Ко второй категории относятся документы, которые по их внешним особенностям невозможно или нецелесообразно подшивать в дела (большого формата, сброшюрованные, чертежно-графические и т.д.). На этот вид учета могут ставиться документы на стадии их создания или получения либо переводиться документы, уже взятые на Учет изданных или поступивших документов. Независимо от вида учета конфиденциальные документы можно учитывать в журналах или карточках. При большом объеме документов целесообразно использовать карточный способ учета, так как он сокращает время на поиск документов за счет помещения карточек в соответствующие рубрики картотек, дает возможность осуществлять ручной контроль

исполнения документов без изготовления специальных контрольных карточек, ускоряет и повышает качество проведения проверок наличия документов. При карточном способе учета документов (как и носителей) необходимо вести контрольный журнал, предназначенный для регистрации карточек и обеспечения последовательности представления их номеров, контроля за местонахождением документов, находящихся в обращении, ускорения их поиска, а также для представления отметок о проверках наличия документов.

Контрольный журнал заводится по каждому виду карточного учета документов. Он имеет следующую форму:

Учетные номера документов	Местонахождение документов	Отметки о проведении проверок наличия документов
1	2	3

В графе 2 напротив соответствующего номера проставляются карандашом фамилия сотрудника, получившего документ, или другое местонахождение документа. При изменении местонахождения документа предыдущая отметка зачеркивается или вытирается и проставляется новая, при этом карточка учета данного документа каждый раз помещается в соответствующую рубрику картотеки. При отработке документа (переводе на другой вид учета, отправлении, подшивке в дело, уничтожении, передаче на архивное хранение) соответствующий номер в контрольном журнале округляется без указания окончательного местонахождения документа. Карточка помещается в картотеку отработанных документов по порядку номеров. В графе 3 напротив соответствующего номера проставляется дата проведения квартальной проверки наличия документа. Вместо контрольного журнала допустимо вести валовую картотеку, формируемую из вторых экземпляров учетных карточек, в которую вносятся данные, предусмотренные для контрольного журнала, но реальные затраты при этом возрастают за счет изготовления вторых экземпляров карточек. Журналы или картотеки учета изданных и поступивших документов ведутся по годно; не исполненные в текущем году документы подлежат переводу на учет следующего года (кроме распорядительных документов и протоколов) с отметкой об этом в учетных формах теку-

шего года, оформляемой по аналогии с отметкой о перерегистрации носителей: по изданным документам в графе 16, по поступившим — в графе 14.

Журнал (картотека) учета документов выделенного хранения 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 документов и созданию сложностей для их пользователей. Порядок оформления учетных форм документов и внесения исправлений в произведенные в них записи является таким же, как и для учетных форм носителей.

9.2. Учет изданных конфиденциальных документов

В предыдущей главе было сказано, что учет изданных конфиденциальных документов осуществляется на стадии подготовки их проектов. Там же была изложена технология учета и дана форма журнала (карточки) учета. Издаваемые на предприятии конфиденциальные распорядительные документы (постановления, приказы, распоряжения), а также протоколы, помимо учетного номера, должны иметь *раздельную по видам тайны ежегодную порядковую нумерацию* в пределах каждого из этих видов документов. Для обеспечения последовательности проставления таких номеров, ускорения поиска документов необходимо вести журналы учета изданных конфиденциальных распорядительных документов и протоколов по каждому их виду отдельно. Журнал имеет следующие графы:

Порядковый номер и гриф конфиденциальности	Дата	Учетный номер	Заголовков	Количество экземпляров	Количество листов в экземпляре	Отметка о местонахождении
1	2	3	4	5	6	7

Если документы издаются с одним грифом конфиденциальности, то в наименовании графы 1 слова «и гриф конфиденциальности» опускаются, рядом с номерами документов гриф не проставляется. В

графе 3 проставляется учетный номер документа, присвоенный ему по журналу учета изданных документов. Графы 1,4 обязательны, целесообразность включения граф 5,7 должна определяться главным образом объемом и характером справочной работы по документам.

9.3. Учет поступивших конфиденциальных документов

Конфиденциальные документы должны пересылаться (доставляться) между предприятиями в соответствующим образом оформленных запечатанных пакетах. Все поступающие пакеты в момент их получения целесообразно учитывать для того, чтобы можно было обнаружить их возможную утрату до регистрации содержащихся в них документов. Для этого следует вести журнал учета поступивших конфиденциальных пакетов, который предназначен, кроме того, для проставления отметок о взятии поступивших документов на различные виды учета, а также о возврате ошибочно присланных документов. Журнал имеет следующие графы:

Дата поступления пакетов	Откуда поступили	Количество пакетов	Подпись лица, доставившего пакеты	Порядковые номера пакетов	Номера и грифы конфиденциальности вложенных в пакеты документов	Учетные номера документов, зарегистрированных по учету поступивших документов	Учетные номера документов, зарегистрированных по учету документов выделен	Учетные номера возвращенных документов и носителей	Отметка о возврате ошибочно присланных документов
1	2	3	4	5	6	7	8	9	10

При получении пакетов сотрудник подразделения конфиденциального делопроизводства должен:

- проверить на пакете наличие грифа конфиденциальности, соответствие адресата, проставление номеров документов и предприятия-отправителя, целостность упаковки, сохранность прошивки и оттиска печати;

— убедиться, что содержимое пакета не просматривается;
— проверить на пакете и сопроводительном документе на него (реестре и соответствии наименований адресата и отправителя, номеров документов, номеров экземпляров (если указаны), грифа конфиденциальности; — расписаться в сопроводительном документе за принятые пакеты с проставлением даты (при необходимости и времени) и печати или специального штампа подразделения конфиденциального делопроизводства. Если на пакетах указан другой адресат, то они не принимаются.

При нарушении оформления пакетов, несоответствии данных на пакете и в сопроводительном документе, повреждении упаковки составляется в двух экземплярах акт, который подписывается сотрудником подразделения конфиденциального делопроизводства и лицом, доставившим пакеты. Второй экземпляр акта направляется отделению связи, доставившему пакет, или предприятию-отправителю пакета, если пакет доставлен минуя отделение связи. Если повреждение пакета дает возможность изъять документ или прочесть его, то об этом сообщается руководителю предприятия, который определяет, принимать пакет или нет. После проставления подписи за принятые пакеты сотрудник подразделения конфиденциального делопроизводства заполняет графы 13 журнала учета поступивших пакетов, при этом в графе 3 количество пакетов указывается прописью, а лицо, доставившее пакеты, заверяет эти данные своей подписью в графе 4. Это дает возможность обнаружить возможную пропажу пакета за период с момента его регистрации до вскрытия. Затем до вскрытия пакетов заполняются графы 5,6 журнала.

Порядковые номера пакетов ежедневно начинаются с № 1 или проставляются последовательно в течение года. Рядом с номером пакета, имеющего пометку «Лично», пишется слово «лично». Номера и грифы конфиденциальности вложенных в пакет документов проставляются напротив номера соответствующего пакета (при наличии двух и более номеров — столбцом). Если на пакете рядом с номером документа указаны номера экземпляров, то они переносятся в журнал. Вызвано это тем, что номера экземпляров на пакете проставляются, когда их два и более, и если их не переносить в журнал, то в случае утраты какого-то экземпляра в период после вскрытия пакета до регистрации документа обнаружить утрату будет невозможно. При

вскрытии пакетов проверяется соответствие на пакете и документе отправителя и адресата, грифа конфиденциальности, номеров документов, номеров экземпляров документа (если указаны на пакете). Пакеты должны быть развернуты таким образом, чтобы убедиться, что в них не осталось вложений. В документах проверяется наличие листов, а в документах, имеющих приложения, кроме того, соответствие учетных номеров, грифа конфиденциальности, номеров экземпляров, количества листов приложения записям в отметке о наличии приложения, содержащейся в основном документе (сопроводительном письме).

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

При несоответствии на пакете и документе или на документе и приложении учетных номеров, недостатке или излишке листов и экземпляров документа, а также в случае, если документ направлен на данное предприятие ошибочно, руководителем подразделения конфиденциального 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 недостатке листов или экземпляров сообщается, кроме того, руководителю данного предприятия. Ошибочно присланные документы, лишние листы и экземпляры вместе с актом направляются с сопроводительным письмом в новом пакете отправителю. В графе 10 журнала учета поступивших пакетов производится отметка о возврате с указанием, сколько листов или какие экземпляры и почему возвращаются, номера и даты сопроводительного письма, например: «Три листа (экз. № ___) возвращены как лишние с № 14КТ от 24.05.20__» или (при возврате документа полностью) «Документ возвращен как ошибочно присланный с № 17 ДСП от 26.05.20__». Ошибочно присланные документы могут по согласованию с предприятием-отправителем пересылаться по назначению за их учетными номерами в новых пакетах с вложением в них лицевой стороны пакета предприятия-отправителя. В этом случае в графе 10 журнала учета поступивших пакетов дела-

ется отметка о пересылке с указанием предприятия, которому направлен документ, номера и даты сопроводительного письма. О несоответствии на пакете и документе или на документе и приложении грифа конфиденциальности или номеров экземпляров отправителю сообщается письмом.

После вскрытия пакета и проверки правильности вложений поступившему документу присваивается очередной номер, проставляемый в графе 7 журнала учета поступивших пакетов. Одновременно данные о документе заносятся в журнал или карточку учета поступивших конфиденциальных документов, имеющих следующие графы:

Учетные номер и гриф конфиденциальности документа	Дата поступления	Вид и заголовков документа	Откуда поступил	Номер и дата издания	Количество листов основного документа	Количество листов приложений
1	2	3	4	5	6	7

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

В момент регистрации заполняются графы 1—7. В графе 1 проставляются очередной порядковый номер, присвоенный документу, и аббревиатурой гриф конфиденциальности документа, В графе 5 указываются номер, присвоенный документу на предприятии, издавшем документ, 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 грифа конфиденциальности, то количество их листов проставляется через + к листам конфиденциальных приложений, например: 8+4 н/с.

При поступлении документа в двух и более экземплярах проставляется общее количество листов всех экземпляров. На самом документе *в правом углу нижнего поля первого листа* проставляется отметка о поступлении, которая содержит учетный номер, присвоенный документу, гриф конфиденциальности, дату поступления, количество листов. При наличии *сопроводительного письма* указывается отдельно количество листов сопроводительного письма и через знак «+» общее количество листов всех конфиденциальных приложений. При наличии открытых (не конфиденциальных) приложений количество их листов отражается отдельно через знак «+» с добавлением аббревиатуры «н/с» (несекретные), например:

Уч.	№
47КТ	19.04.200
3	л.л.
1+20+6 н/с	

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

Уч. №	
Дата	
Кол-во листо в	

При наличии приложений, кроме отметки о поступлении документа, на первом листе каждого приложения (как конфиденциально, так и открытого) в правом углу нижнего поля проставляется штампом или от руки отметка «К Уч. №__» с указанием номера, присвоенного документу в целом, и аббревиатурой его грифа конфиденциальности. Эта отметка необходима для того, чтобы в случаях получения исполнителем отдельных приложений без сопроводительного письма было видно, что они являются частью поступившего документа, а не изданным данным предприятием документом. В сброшюрованных документах отметки о поступлении можно проставлять

на титульном листе. Документы, присланные в пакетах с пометкой «Лично», по усмотрению лица, вскрывшего пакет, или передаются для учета сотруднику подразделения конфиденциального делопроизводства, или регистрируются последним в учетных формах со слов лица, вскрывшего пакет. При втором варианте регистрационные данные в штампе на документе проставляет лицо, вскрывшее пакет. Поступившие машинные носители после занесения их в журнал учета поступивших пакетов регистрируются в журнале учета машинных носителей в порядке, изложенном в подразделе выше. Если поступивший документ подлежит выделенному хранению, то ему следует сразу (без регистрации в журнале учета поступивших документов) присваивать очередной порядковый номер по журналу учета документов выделенного хранения. Этот номер проставляется на документе, в графе 8 журнала учета поступивших пакетов и в графе 1 журнала учета документов выделенного хранения с одновременным заполнением граф 2,7 этого журнала, при этом в графе 5 указывается: «П/ж № ___ за _____». с проставлением номера и даты поступления пакета, в котором находился документ. Если на предприятие возвращены без сопроводительного письма отправленные ранее без сопроводительного письма все или часть экземпляров документа, зарегистрированного по любому виду учета, или машинный носитель, то в графе 9 журнала учета поступивших пакетов напротив возвращенного номера вложенного в пакет документа (носителя) проставляется номер, ранее присвоенный документу на данном предприятии с добавлением перед ним индекса И (для изданных документов), П (для поступивших документов), В (для документов выделенного хранения), Н (для носителей). Одновременно в графе 15 журнала учета изданных документов или в графе 11 журнала учета документов выделенного хранения производится запись: «Экз. №___ возвращены, п/ж №___ за _____» с указанием номеров экземпляров, порядкового номера и даты поступления пакета, проставленных в журнале учета поступивших пакетов. 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, в котором находился возвращенный документ. Если документ (носитель) отправлялся и (или) возвращен с сопроводительным письмом, то он регистрируется за очередным номе-

ром в журнале учета поступивших документов. Документ, подлежащий выделенному хранению, переводится затем без сопроводительного письма на учет документов выделенного хранения, а носитель — на учет машинных носителей. Сопроводительное письмо подшивается в дело. Допустимо также в журнале учета поступивших документов регистрировать только сопроводительное письмо, а приложение оформлять как возврат ранее отправленного документа. В обоих случаях в справочных целях на сопроводительном письме следует делать отметку об учетном номере приложения.

9.4. Учет конфиденциальных документов выделенного хранения

Учет конфиденциальных документов, подлежащих выделенному хранению, осуществляется в журнале или карточках, имеющих следующие графы:

Учетный номер и гриф конфиденциальности документа	Дата регистрации	Вид и заголовок документа	Откуда поступил или каким подразделением разработан	С учетом каких учетных номеров	Номера экземпляров	Количество листов в экземпляре
8	9	10	11	12	13	14

Отправление			Отметка о возврате	Уничтожение		Передача на архивное хранение	
Куда отправлен	Номера экземпляров	Наименование, номер и дата сопроводительного документа		Номера экземпляров	Номер и дата об уничтожении	Номер экземпляра	Архивный шифр
8	9	10	11	12	13	14	15

При значительном объеме документов выделенного хранения чертежно-графические и текстовые документы могут учитываться раздельно, но в однотипных формах учета. В этом случае слова «чертежно-графические» или «текстовые» должны включаться в наименование журнала. В момент регистрации заполняются графы 1—7. При регистрации чертежно-графических документов в графе 3 проставляются вид носителя (калька, ватман, синька) и индекс (обозначение) документа.

При взятии на учет документа, переводимого с учета поступивших документов, в графе 4 указывается, откуда поступил документ, в графе 5— его учетный номер по журналу учета поступивших документов, одновременно в графе 13 журнала учета поступивших документов проставляются номер, присвоенный документу по журналу учета документов выделенного хранения, и количество листов, отметка о возврате, уничтожении, передача на архивное хранение, номера экземпляров, номер и дата акта об уничтожении, номер экземпляра, архивный шифр куда отправлены номера экземпляров, наименование, номер и дата сопроводительного документа, переведенных на выделанное хранение.

При взятии на учет документа, переводимого с учета изданных документов, в графе 4 указывается подразделение данного предприятия, разработавшее документ, в графе 5 — учетный номер документа по журналу учета изданных документов, в графе 17 журнала учета изданных документов проставляются номер, присвоенный документу по журналу учета документов выделенного хранения, и количество переведенных на выделенное хранение экземпляров.

Взятые на учет выделенного хранения текстовые документы помещаются в обложку и брошюруются (прошиваются), если не имели обложки и не были сброшюрованы, при этом после последнего листа документа помещается лист с заверительной надписью, в которой указывается прописью количество листов в документе, заверяемое подписью (с расшифровкой) лица, составившего заверительную надпись, с проставлением даты. Если в документе имеются литерные, пропущенные номера или вклеенные на листы фотоотпечатки, то они оговариваются в заверительной надписи.

На *текстовых документах* учетные номера, присвоенные по журналу учета документов выделенного хранения, проставляются в

верхнем левом углу обложки и титульного листа (при его наличии). В правом верхнем углу проставляются гриф конфиденциальности и под ним номер экземпляра.

На *чертежно-графических документах* учетные номера проставляются на каждом листе в местах, отведенных соответствующими стандартами. На присланных документах имеющиеся там номера зачеркиваются тушью тонкими линиями. На каждый документ заводится карточка учета выдачи по следующей форме:

КАРТОЧКА
учета выдачи конфиденциального документа выделенного хранения

(учетный номер, наименование документа и количество листов в нем)

Кому выдан	Подпись за получение и дата	Подпись за возврат и дата
---------------	--------------------------------	------------------------------

9.5. Размножение конфиденциальных документов

Размножение конфиденциальных документов должно производиться только при действительной служебной необходимости в их дополнительных экземплярах. Конфиденциальные документы могут размножаться в подразделении конфиденциального делопроизводства или в специальном множительном подразделении предприятия. Размножение (тиражирование) конфиденциальных документов в типографиях методом набора и печатания текста, как правило, не осуществляется главным образом из-за отсутствия потребности в большом тираже. Предназначенные для размножения документов технические средств (копировально-множительное оборудование, компьютеры, пишущие машинки) должны быть защищены от возможного перехвата возникающих при их работе электромагнитных излучений. Размножение конфиденциальных документов не должно производиться попеременно с размножением открытых документов. Во время размножения конфиденциальных документов все, что не имеет отношения к их размножению, должно быть убрано с рабочих мест, используемых при размножении, доступ посторонних лиц в помещение, в котором производится размножение, не разрешается. При возникно-

вании в процессе размножения листов брака они помещаются в специальную папку.

Разрешение на размножение документов могут давать по усмотрению руководителя предприятия руководители соответствующих структурных подразделений самостоятельно либо совместно с руководителем службы безопасности (подразделения конфиденциального делопроизводства) предприятия. Подписанный руководителем предприятия список лиц, имеющих право давать разрешение на размножение конфиденциальных документов, должен находиться в множительном подразделении. Документы, поступившие из других предприятий, могут размножаться только с письменного разрешения издавших их предприятий.

Размножение документов производится в форме изготовления дополнительных экземпляров, снятия копий с документов и производства выписок из документов. Разрешение на изготовление дополнительных экземпляров документов оформляется на обороте последнего листа экземпляра, с которого должно производиться размножение. Этот экземпляр не должен в последующем направляться на другие предприятия, он подшивается в дело или переводится на учет документов выделенного хранения. Разрешение оформляется следующим образом: «Размножить в _____ экз. Должность (должности) лиц, разрешающих размножение документа, подпись (подписи), дата». При размножении поступившего документа дополнительно делается ссылка на номер и дату разрешения. При невозможности оформления разрешения на размножение на самом документе оно оформляется в форме учета данного документа. При размножении документов в специальном множительном подразделении их передача на размножение производится специально назначенному для размножения конфиденциальных документов лицу под его подпись в форме учета или карточке выдачи документа. Подлежащие размножению документы регистрируются в подразделении конфиденциального делопроизводства или в специальном множительном подразделении (по месту размножения) в *журнале учета* размножения конфиденциальных документов, имеющего следующие графы:

Учетные номер, гриф конфиденциальности и дата документа	Количество или номера листов (пунктов)	Размножено экземпляров	Дата размножения	Учетные номера, присвоенные копиям и выпискам	Количество листов брака	Подпись об уничтожении бракованных листов, дата	Подпись сотрудника подразделения конфиденциального делопроизводства за получение изготовленных экземпляров, дата
1	2	3	4	5	6	7	8

При *поступлении документа* на размножение заполняются графы 1—2 журнала. В графе 1 гриф конфиденциальности проставляется аббревиатурой. В графе 2 указывается общее количество листов документа. Если размножается документ, изданный данным предприятием, в процессе размножения номер экземпляра документа, с которого осуществляется размножение, на размноженных экземплярах не воспроизводится.

При размножении *поступивших документов* номер экземпляра воспроизводится. Учетный номер, присвоенный документу, сохраняется на размноженных экземплярах. После размножения документа заполняются графы 3, 4 и (при наличии брака) 6, 7 журнала учета размножения конфиденциальных документов. В графе 3 указывается общее количество размноженных экземпляров без проставления их номеров. В графе 6 отражается общее количество листов брака без перечисления их номеров. Эти листы уничтожаются с помощью бумагорезательной машины или разрываются и помещаются в печатанную урну, после чего работник, производивший размножение документа и уничтожение бракованных листов, расписывается в графе 7 с проставлением даты. Графа 8 включается в журнал и заполняется в случаях, когда размножение производится в специальном множительном подразделении. Подпись за возврат документа, с которого производилось размножение, проставляется в учетной форме, по которой осуществлялась его передача в специальное множительное

подразделение. На размноженных экземплярах работник подразделения конфиденциального делопроизводства проставляет их номера.

При этом если документ был издан данным предприятием, то номера размноженных экземпляров продолжают номера ранее изготовленных экземпляров, если документ был издан другим предприятием, то на размноженных экземплярах их номера проставляются дробно: в числителе на всех экземплярах остается номер, присвоенный предприятием, издавшим документ, а в знаменателе на каждом экземпляре проставляется присвоенный ему порядковый номер, начиная с № 1. На каждом размноженном экземпляре в реквизите «Отметка об исполнителе» проставляется только учетный номер, присвоенный документу при его издании, независимо от места издания, фамилия, имя, отчество исполнителя и его рабочий телефон (если проставлен на размножаемом экземпляре). На экземпляре, с которого производилось размножение, под разрешением на размножение работник подразделения конфиденциального делопроизводства производит запись: «Размножено _____ экз. с № _____ по № _____», которая заверяется его подписью с проставлением даты. Если размноженные экземпляры не воспроизводят подпись, то они удостоверяются печатью предприятия или подразделения конфиденциального делопроизводства, которая проставляется с захватом части слова, обозначающего должность лица, подписавшего документ. При размножении документов, зарегистрированных в журнале учета изданных документов, количество размноженных экземпляров проставляется в графе 6 ниже ранее проставленных через знак «+». При размножении документов, зарегистрированных по журналу учета поступивших документов, отметка о размножении производится в графах 6, 7 ниже проставленных листов и оформляется следующим образом: «Размножено _____ экз.».

При размножении документов, зарегистрированных в журнале учета документов выделенного хранения, отметка о размножении производится в графе 6. Номера размноженных экземпляров проставляются следом за ранее проставленными номерами. Размноженные экземпляры отделяются от ранее проставленных знаком «+». Размножение конфиденциальных документов в форме снятия копий осуществляется в случаях, когда документы подшиты в дело и сняты с учета по журналам (карточкам) учета этих документов. Технология изготовления копий документов аналогична технологии изготовления до-

полнительных экземпляров, кроме следующих особенностей. Разрешение на изготовление копий оформляется записью: «Снять копию в _____ экз.».

Копии документа присваивается отдельный учетный номер — очередной порядковый номер по журналу учета изданных документов, независимо от того, по какому виду учета (изданных или поступивших документов) зарегистрирован документ, с которого снимается копия. Присвоенный копии учетный номер проставляется на всех листах копии посередине нижнего поля с добавлением аббревиатуры грифа конфиденциальности (на последнем листе — в реквизите «Отметка об исполнителе»). В реквизите «Дата и номер документа» на копии сохраняются прежние данные. На первом листе копии над реквизитом «Гриф ограничения доступа к документу» проставляется слово КОПИЯ. Реквизит «Отметка об исполнителе» оформляется полностью, как во вновь создаваемых документах. Ниже реквизита «Подпись» на копии документа проставляется слово «Верно», которое заверяется подписью лица, производившего снятие копии, с указанием его должности, инициалов и фамилии, а также даты заверения. Если копия пересылается на другие предприятия, то на ней дополнительно проставляется печать предприятия или подразделения конфиденциального делопроизводства.

Экземпляры копии имеют самостоятельную нумерацию, начиная с № 1. На экземпляре документа, с которого снималась копия, под разрешением на снятие копии работником подразделения конфиденциального делопроизводства производится запись «Снята копия в _____ экз. за уч. № _____», которая заверяется его подписью с проставлением даты. В журнале учета размножения конфиденциальных документов дополнительно заполняется графа 5. Заполнение граф журнала учета изданных документов при снятии копий производится аналогично заполнению на вновь создаваемые документы. Технология производства выписок из конфиденциальных документов имеет следующие особенности. Выписки могут производиться с документов, как не подшитых, так и подшитых в дела, а также с документов выделенного хранения. Разрешение на изготовление выписки оформляется записью: «Размножить л.л. (п.п.) _____ в _____ экз.».

Выпискам присваивается отдельный учетный номер — очередной порядковый номер по журналу учета изданных документов, неза-

висимо от того, по какому виду учета зарегистрирован документ, из которого производится выписка. Проставление учетного номера на выписке осуществляется аналогично проставлению его на копии. На первом листе выписки после заголовка документа проставляется слово **ВЫПИСКА**. Выписка имеет собственную нумерацию листов и экземпляров. Рек визит «Отметка об исполнителе» оформляется полностью. Отметки о производстве и заверении выписки оформляются, как и в копии, с заменой в отметке о производстве слов «Снята копия» на слова «Произведена выписка». В журнале учета размножения конфиденциальных документов в графе 2 перед производством выписки проставляются номера листов или пунктов, с которых производится выписка (например, л.л. 7-9 или п.п. 4 6 — 8), а в графе 5 после производства выписки — учетный номер выписки, остальные графы заполняются, как и при других формах размножения. Заполнение граф журнала учета изданных документов при производстве выписок осуществляется аналогично заполнению на вновь создаваемые документы.

Раздел III. Режим хранения, виды и принципы проверок конфиденциальных документов

Глава 10. Режим хранения конфиденциальных документов и обращения с ними

10.1. Режим хранения конфиденциальных документов

Для обеспечения физической сохранности конфиденциальных документов, дел и носителей, а также для предотвращения утечки содержащейся в них информации должен быть установлен специальный режим их хранения. Помещения подразделения конфиденциального делопроизводства, предназначенные для круглосуточного хранения конфиденциальных документов, в целях обеспечения дополнительных гарантий от постороннего проникновения в них должны, как правило, находиться не на первом и последнем этажах. Кроме того, они должны соответствовать нормам, установленным для хранения документов: удалены от помещений с пищевыми продуктами и химическими веществами, не иметь с ними вентиляционных каналов, отвечать требованиям пожарной безопасности, санитарным нормам, а также быть гарантированы от затопления. Вход в такие помещения необходимо строго регламентировать. Кроме руководителя предприятия и сотрудников, имеющих прямое отношение к обработке и хранению конфиденциальных документов, в помещения могут допускаться лица, обеспечивающие их обслуживание.

Уборка помещений, ремонт находящихся в них оборудования и технических средств, выполнение других работ, связанных с привлечением лиц, не имеющих доступа к хранящимся в помещениях документам, должны производиться только в присутствии сотрудников подразделения конфиденциального делопроизводства.

Окна помещений должны иметь надежные средства защиты, исключающие возможность проникновения в помещения посторонних лиц. Кроме того, на них должны быть защитная сетка или жалюзи, предотвращающие возможность выпадения документов, а также визуального просмотра документов и экранов видеомониторов с улицы. Если помещения расположены на первом или последнем этаже или

рядом с ними находятся пожарные лестницы, балконы, водосточные трубы, другие какие-либо пристройки, с помощью которых можно проникнуть в помещения, то для предотвращения проникновения окна дополнительно защищаются распашной металлической решеткой с замком.

Входные двери помещений должны быть обиты металлом и оборудованы замками, гарантирующими их надежное закрытие. По окончании рабочего дня двери необходимо не только запирать, но и опечатывать печатью подразделения (или сотрудника подразделения) конфиденциального делопроизводства. Печать проставляется на тонкий слой пластилина или специальной мастики таким образом, чтобы оттиск невозможно было снять и восстановить. Перед отпиранием двери проверяется сохранность оттиска печати и целостность запоров. При обнаружении попыток проникновения в помещения нужно немедленно поставить в известность службу охраны и доложить руководителю предприятия. До принятия решения руководителем предприятия помещения не открываются и обеспечиваются физической охраной. Для предотвращения несанкционированного входа в помещения в течение рабочего дня на дверях могут устанавливаться электромеханические или электронные замки.

Конфиденциальные документы в помещениях должны храниться в сейфах, металлических шкафах или металлических стеллажах, которые по окончании рабочего дня запираются и опечатываются сотрудниками, ответственными за учет и хранение документов. Хранение открытых документов вместе с конфиденциальными допускается только в случаях, когда они являются приложениями к конфиденциальным документам. Входные двери, окна помещений, а также сейфы, шкафы и стеллажи следует оснастить охранной сигнализацией, связанной со службой охраны предприятия или службой вневедомственной охраны. Помещения, в которых для фиксации, обработки, хранения, воспроизведения и передачи конфиденциальной документной информации используются электронно-вычислительные машины, электронные множительные аппараты, средства аудио— видеозаписывающей и воспроизводящей техники и другие технические средства, создающие электромагнитные излучения, необходимо оборудовать дополнительными средствами защиты, предотвращающими перехват соперником электромагнитных сигналов, несущих конфиден-

циальную информацию. В этих же целях целесообразно приобретать сертифицированные технические средства обработки информации, отвечающие требованиям по защите конфиденциальной информации от ее утечки, а средства иностранного производства предварительно подвергать спецпроверкам на предмет выявления возможных специальных электронных и программных закладок. Замки дверей помещений, распашных металлических решеток на окнах, сейфов, шкафов или стеллажей должны иметь рабочие и запасные экземпляры ключей.

Запасные экземпляры ключей могут храниться в опечатанных их владельцами пеналах или конвертах либо у руководителя предприятия, либо в службе охраны, либо (ключи от сейфов, шкафов, стеллажей, металлических решеток) в сейфе (шкафу) сотрудника подразделения конфиденциального делопроизводства, ответственного за хранение документов. Рабочие экземпляры ключей от сейфов, шкафов, стеллажей, решеток в нерабочее время могут храниться в опечатанном пенале (конверте) либо в службе охраны, либо в сейфе (шкафу) сотрудника подразделения конфиденциального делопроизводства, ответственного за хранение документов. В последнем случае по окончании рабочего дня ключ от этого сейфа вместе с рабочим экземпляром ключа от входной двери помещения передается в пенале, опечатанном печатью сотрудника подразделения конфиденциального делопроизводства, в службу охраны с внесением соответствующих данных в графы 1—6 журнала передачи-приема под охрану помещений и пеналов с ключами. Журнал может иметь следующую форму:

Наименование или номер помещения, передаваемого под охрану	Номер печати, которой опечатаны помещение и пенал с ключами	Дата и время передачи под охрану	Подпись и фамилия лица, передавшего помещение и пенал под охрану	Отметка о включении сигнализации	Подпись и фамилия лица, принявшего помещение и пенал под охрану	Дата и время получения пенала	Подпись и фамилия лица, получившего пенал	Отметка о выключении сигнализации
1	2	3	4	5	6	7	8	9

При получении пенала из охраны заполняются графы 7—9. Получение пенала с ключами из службы охраны и вскрытие помещений должно осуществляться только сотрудниками подразделения конфиденциального делопроизводства, ответственными за хранение конфиденциальных документов. При их отсутствии для вскрытия помещений назначается комиссия в составе не менее двух человек, которая составляет акт о вскрытии с указанием в нем должностей и фамилий лиц, вскрывших помещения, времени и причины вскрытия, номеров печатей, которыми были опечатаны помещения. Комиссионно с составлением акта вскрываются и сейфы, шкафы или стеллажи при отсутствии сотрудника, ответственного за хранение находящихся в них документов. В случае утраты рабочих или запасных экземпляров ключей об этом немедленно ставится в известность руководитель предприятия. При утрате ключа от сейфа, шкафа или стеллажа до замены замка или смены секрета замка хранить документы в этом сейфе (шкафу, стеллаже) не следует.

Для обеспечения выдачи конфиденциальных документов исполнителям (пользователям) помещения должны быть оборудованы специальными окошками, не выходящими в общий коридор, или внутри отгораживаться барьером. Исполнители могут работать с конфиденциальными документами или в специально выделенных помещениях подразделения конфиденциального делопроизводства, или в своих служебных комнатах, если эти комнаты отвечают требованиям обеспечения сохранности и конфиденциальности документов.

При работе с документами в служебных комнатах каждый исполнитель должен иметь постоянное рабочее место, сейф (металлический шкаф) или отдельную ячейку сейфа для хранения конфиденциальных документов и номерную металлическую печать. Ключи от сейфа и номерная печать выдаются исполнителю под подпись в личном счете. Рабочий экземпляр ключа и номерная печать хранятся постоянно у исполнителя. Запасные экземпляры ключей должны храниться в подразделении конфиденциального делопроизводства или службе охраны в опечатанном номерной печатью исполнителя конверте либо пенале. Все сейфы, шкафы и стеллажи, установленные в помещениях подразделения конфиденциального делопроизводства и в служебных комнатах исполнителей, в которых круглосуточно или в рабочее время хранятся конфиденциальные документы, а также ключи от них

должны учитываться подразделением конфиденциального делопроизводства по журналу учета хранилищ и ключей от них, имеющем следующую форму:

№ п/п	Наименование хранилища (сейф, металлический шкаф, металлический стеллаж)	Заводской инвентарный номер хранилища	Местонахождение хранилища (подразделение, номер комнаты)	Инициалы и фамилия ответственного за хранилище	Количество экземпляров ключей и их номера	Подпись ответственного за хранилище, за получение ключей, дата	Подпись сотрудника подразделения конфиденциального делопроизводства за возврат ключей, дата
1	2	3	4	5	6	7	8

При внесении в журнал данных о ключах от распашных металлических решеток графы 2-3 не заполняются. Ежегодно должна проводиться проверка фактического наличия ключей от хранилищ и номерных печатей исполнителей, Для эвакуации конфиденциальных документов при возникновении стихийных бедствий, пожара, аварии, грозящих затоплением, загоранием или другой формой уничтожения документов, в помещениях, предназначенных для их хранения, должно находиться необходимое количество тары (мешков, чемоданов, контейнеров и т.д.), в которой можно транспортировать документы.

При возникновении чрезвычайной ситуации сотрудники подразделения конфиденциального делопроизводства должны немедленно вызвать пожарную команду или соответствующую аварийную службу, уведомить руководителя предприятия, принять меры к ликвидации чрезвычайной ситуации, а при невозможности ликвидации обеспечить охрану документов собственными силами, а также силами службы охраны предприятия и начать эвакуацию документов в заранее определенное место. При возникновении чрезвычайной ситуации в нерабочее время проведение аналогичных действий должен организовать дежурный по предприятию, поставив в известность дополнительно руководителя подразделения конфиденциального делопроиз-

водства. О проведенном вскрытии (при необходимости) помещений, а также о вскрытии по согласованию с руководителем предприятия или подразделения конфиденциального делопроизводства сейфов, шкафов или стеллажей составляется акт, в котором указываются должности и фамилии лиц, производивших вскрытие, какие хранилища вскрыты, куда помещены документы, номера печатей на таре.

10.2. Порядок обращения с конфиденциальными документами

На каждом предприятии должен быть установлен строгий порядок обращения с конфиденциальными документами, который является составной частью внутриобъектового режима и направлен на обеспечение сохранности конфиденциальных документов и предотвращение утечки содержащейся в них информации. Выдача (передача) конфиденциальных документов может производиться только исполнителям (пользователям), имеющим санкционированный доступ к этим документам, и только под подпись в учетных формах или взамен разовой расписки. Выдача документов исполнителям и их возврат осуществляются в течение одного рабочего дня, но если исполнители работают с конфиденциальными документами в своих служебных комнатах, то документы (кроме дел) допускается выдавать им как на один рабочий день, так и на все время, необходимое для работы с ними. В последнем случае, помимо сейфа и номерной печати, исполнителю выдаются под подпись в лицевом счете специальный портфель (кейс), имеющий устройство для опечатывания, и форма «Описи документов, находящихся у исполнителя», в которую исполнитель должен вносить каждый документ в момент получения и вычеркивать после передачи в подразделение конфиденциального делопроизводства. Опись может иметь следующие графы:

№ п/п	Номер и гриф конфиденциальности				Количество листов
	Изданного документа	Поступившего документа	Документа выделенного хранения	Носителя	
1	2	3	4	5	6

Опись предназначена для осуществления самоконтроля за наличием документов. С этой целью перед сдачей спецпортфеля с документами в подразделение конфиденциального делопроизводства ис-

полнитель должен проверить наличие находящихся у него документов и их соответствие описи. При отсутствии каких-либо документов или части их немедленно ставится в известность подразделение конфиденциального делопроизводства и организуется их поиск. После проверки документы вместе с описью помещаются в спецпортфель, который опечатывается личной печатью исполнителя и передается в подразделение конфиденциального делопроизводства. Не допускается хранить в спецпортфеле открытые документы, если они не являются приложением к конфиденциальным документам. Спецпортфели могут храниться у исполнителей только в течение рабочего дня. Их получение и возврат производятся в обмен на специально заготовленную расписку (жетон), удостоверение или пропуск сотрудника. При наличии большого числа исполнителей, работающих с конфиденциальными документами, на специальную расписку может наклеиваться фотокарточка исполнителя. При приеме-передаче спецпортфеля необходимо проверять соответствие номера и четкость оттиска печати. Должностные лица, которым разрешено в нерабочее время хранить конфиденциальные документы в личных сейфах при условии подключения сейфов к охранной сигнализации, по окончании рабочего дня помещают документы в сейф, опечатывают его и сдают под охрану по специальному журналу, ведущемуся службой охраны. По завершении работы с документами исполнители должны своевременно возвращать их в подразделение конфиденциального делопроизводства.

При увольнении, перед уходом в отпуск, отъездом в командировку исполнители сдают в подразделение конфиденциального делопроизводства все хранящиеся в их спецпортфелях конфиденциальные документы.

Рабочее место исполнителя должно быть организовано таким образом, чтобы исключалось обозрение (в том числе и через окна) находящихся из-за стола конфиденциальных документов лицами, не имеющими к ним отношения. На столе должны быть только те конфиденциальные документы, с которыми осуществляется работа. Все остальные должны находиться в сейфе, закрытом на ключ. Не разрешается хранение конфиденциальных документов в ящиках столов и других, не предназначенных для этого местах. При выходе исполнителя в течение рабочего дня из служебной комнаты документы уби-

раются в сейф, который опечатывается личной печатью. При выходе из комнаты всех исполнителей дверь комнаты должна быть закрыта на ключ. Крупноформатные конфиденциальные документы на чертежных досках (кульманах) на время отсутствия исполнителя должны закрываться специальными защитными чехлами, опечатываемыми его печатью. Подразделение конфиденциального делопроизводства обязано осуществлять периодический контроль за порядком хранения документов в служебных комнатах исполнителей и обращения с ними. Нарушения порядка обращения с конфиденциальными документами целесообразно учитывать с целью последующего анализа и принятия мер по их предотвращению. Учет может осуществляться в карточке (журнале), имеющей следующие графы:

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

О серьезных нарушениях, которые привели или могли привести к утрате документов или утечке содержащейся в них информации, подразделение конфиденциального делопроизводства должно докладывать руководителю предприятия и вносить предложения об отстранении от работы с конфиденциальными документами или привлечении к ответственности виновных лиц. При смене или временном отсутствии руководителя и сотрудников подразделения конфиденциального делопроизводства передача документов замещающим их лицам производится по актам или распискам с обязательной проверкой фактического наличия передаваемых документов.

Глава 11. Принципы проведения проверок наличия конфиденциальных документов

11.1. Назначение, виды и принципы проведения проверок наличия конфиденциальных документов

Проверки наличия конфиденциальных документов являются важной составной частью конфиденциального делопроизводства.

Цель проверок состоит в обеспечении контроля за сохранностью документов. Это достигается путем установления соответствия фактического наличия документов учетным данным на них, выявления отсутствующих документов и принятия мер по их розыску. Однако в процессе регистрации документов могут быть допущены ошибки, следствием которых становится искажение учетных данных о документах. Кроме того, часть зарегистрированных документов может быть отправлена, уничтожена, подшита в дела, возвращена после отправления, переведена на другой вид учета. При проставлении в учетных формах отметок о таком движении документов также могут случаться ошибки, которые при определенных обстоятельствах создают основу для утраты документов и (или) несвоевременного обнаружения утрат.

Поэтому проверки правильности регистрации документов и проставления отметок об их движении должны быть составными частями проверок наличия документов. Проверки направлены и на выявление неучтенных по каким-либо причинам конфиденциальных документов, установление этих причин и взятие таких документов на учет. «Положение о порядке обращения со служебной информацией ограниченного распространения» предусматривает проведение проверок наличия документов не реже одного раза в год, допуская тем самым возможность их проведения только один раз в год. Однако при такой периодичности резко снижается вероятность своевременного обнаружения утрат документов и их нахождения.

Чем чаще проводятся проверки, тем больше гарантий обеспечения сохранности документов. Проверками должны быть охвачены не только документы, но и дела, а также носители конфиденциальной информации. Проверки правильности регистрации и фактического наличия документов частично проводятся в процессе выдачи их ис-

полнителям и следующего возврата. Однако такие проверки не охватывают все документы и все необходимые проверочные операции. Поэтому следует осуществлять комплексные плановые проверки фактического наличия документов, дел и носителей и правильности отметок об их регистрации и движении. Наиболее оптимальными видами проверок и сроками их проведения являются:

- проверки правильности проставления регистрационных данных носителей, документов, дел и учетных журналов (картотек);
- сразу после регистрации;
- проверки правильности проставления отметок о движении носителей, документов и дел, независимо от времени их регистрации;
- сразу после проставления отметок или при невозможности проведения сразу после проставления отметок;
- по истечении каждого квартала;
- проверки фактического наличия всех носителей и всех не подшитых в дела и не переведенных на учет выделенного хранения изданных и поступивших документов, независимо от времени их регистрации;
- один раз в квартал по истечении квартала (квартальные проверки);
- проверка фактического наличия всех дел, документов выделенного хранения и учетных журналов (картотек), зарегистрированных в истекшем и предыдущих годах;
- один раз в год по истечении года (годовая проверка).

Эти виды проверок и сроки их проведения позволяют своевременно выявлять ошибки, допущенные при регистрации документов и производстве отметок об их движении, осуществлять систематический контроль за наличием документов, при этом более тщательный в отношении документов, не сброшюрованных и не подшитых в дела, а следовательно, подвергающихся большей опасности утраты. В то же время такой состав проверок и такая периодичность их проведения дают возможность избежать повтора проверочных операций, за исключением проверок фактического наличия части носителей и не подшитых в дела документов. Кроме того, существуют так называемые нерегламентные проверки фактического наличия документов, которые проводятся по мере возникновения необходимости в них. Проверочные операции может осуществлять сотрудник подразделе-

ния конфиденциального делопроизводства, регистрировавший документы и производивший отметки об их движении. Но для некоторых операций это не лучший вариант, поскольку у сотрудника притупляется внимание к записям, сделанным им самим. Этот вариант целесообразно использовать при проверках правильности проставления регистрационных данных носителей, документов, дел и учетных журналов (картотек), в том числе при проверках отметок о возврате ранее отправленных документов, так как регистрационные данные дополнительно проверяются в процессе передачи-приема носителей, документов и дел между исполнителями и подразделением конфиденциального делопроизводства.

Самым оптимальным вариантом для других видов проверок является проведение их одновременно двумя сотрудниками, одним из которых должен быть сотрудник, осуществлявший регистрацию документов, дел и носителей и проставлявший отметки о их движении. При этом каждый из сотрудников не дублирует проверочные операции, а выполняет определенную их часть. Например, один сотрудник называет учетные данные на документе, другой проверяет их соответствие в учетных формах или один называет данные учетных форм, другой проверяет их соответствие в других учетных формах, сопроводительных документах, делах и т.д. Это повышает качество проверок и ускоряет их проведение. В целях обеспечения контроля за проведением всех необходимых проверочных операций и избежания их дублирования необходимо проставлять соответствующие отметки о проверках. Отметки о проверках правильности регистрации носителей, документов, дел и учетных журналов (картотек), а также правильности записей о возврате документов проставляются условным обозначением. Отметки о проверках фактического наличия носителей, документов, дел и учетных журналов (картотек) целесообразно проставлять датами проверок, поскольку, как уже отмечалось, такие проверки частично повторяются и по дате можно отличить одну проверку от другой. Отметки допускается производить карандашом, чтобы при необходимости можно было их вытереть, например, с целью освобождения места для проставления последующих отметок. Проверки правильности производства отметок о движении носителей, документов и дел заверяются подписями с проставлением даты. При

проведении проверок необходимо руководствоваться следующими принципами:

— охват проверочными операциями всех подлежащих проверке документов, дел и носителей, всех учетных форм, в которых зафиксированы проверяемые реквизиты, и всех необходимых сопроводительных (оправдательных) материалов о движении документов;

— проведение проверок наличия документов по схеме: сначала документ, потом учетные данные на него (от документа к формам учета), что обеспечивает большую возможность обнаружения неучтенных конфиденциальных документов;

— фиксация конечных результатов проверок. Технологии проведения названных видов проверок различаются между собой, поэтому целесообразно рассмотреть их по каждому виду.

11.2. Проверка правильности проставления регистрационных данных конфиденциальных носителей, документов, дел и учетных журналов (карточек)

Для проверки правильности проставления регистрационных данных бумажных носителей должны привлекаться журнал учета бумажных носителей и носители. В журнале и на носителе проверяется соответствие записей об учетном номере и грифе конфиденциальности носителя, дате регистрации, виде, наименовании или назначении носителя, количестве листов. В носителе проверяется правильность нумерации листов. Отметка о проверке проставляется в журнале рядом с номером носителя. Если бумажные носители в момент их заведения регистрируются не в журнале учета бумажных носителей, а в журнале учета документов выделенного хранения (рабочие тетради, калька и др.), то для проверки правильности их регистрации привлекаются Журнал учета документов выделенного хранения и носители. В журнале и на носителе проверяется соответствие записей об учетном номере и грифе конфиденциальности носителя, дате регистрации, виде и наименовании носителя, наименовании подразделения, номерах экземпляров, количестве листов в экземпляре. В носителе проверяется правильность нумерации листов. Отметка о проверке проставляется в журнале рядом с номером носителя. Для проверки правильности проставления регистрационных данных машинных но-

сителей должны использоваться журнал учета машинных носителей и носители. В журнале и носителе проверяется соответствие вида и типа носителя, его учетного номера и грифа конфиденциальности. Отметка о проверке проставляется в журнале рядом с номером носителя. Для проверки правильности проставления регистрационных данных изданных документов привлекаются журнал учета изданных документов, документы и черновики. В журнале и на документе проверяется соответствие записей об учетном номере, грифе конфиденциальности, дате, виде и заголовке документа, фамилии исполнителя (на документе — в реквизите «Отметка об исполнителе»), количестве экземпляров (в документе — по их фактическому наличию и в реквизите «Отметка об исполнителе»), количестве листов в экземпляре. В документе проверяется правильность нумерации листов, проставление учетных номеров на каждом листе документа, проставление номера экземпляра на каждом экземпляре. В журнале и на черновике проверяется соответствие номера носителя и номеров листов черновика. Отметка о проверке проставляется в журнале рядом с номером документа.

Наиболее сложной является *проверка правильности проставления регистрационных данных поступивших документов*, поскольку в их состав входят документы, зарегистрированные по журналу учета поступивших документов, журналу учета документов выделенного хранения, а также возвращенные документы, которые ранее были зарегистрированы по разным видам учета. Для проверки правильности проставления регистрационных данных документов, зарегистрированных по журналу учета поступивших документов, привлекаются журнал учета поступивших пакетов, журнал учета поступивших документов и документы. В журнале учета пакетов проверяется соответствие количества поступивших пакетов (графа 3) количеству зарегистрированных (графа 5). В журнале учета пакетов и журнале учета поступивших документов проверяется соответствие данных о присвоенном учетном номере, дате поступления документа, номере, за которым документ направлен, предприятию-отправителю. В журнале учета поступивших документов и на документе проверяется соответствие присвоенного учетного номера, грифа конфиденциальности, даты поступления, вида и заголовка документа, предприятия-отправителя, номера, за которым документ направлен, даты докумен-

та, количества листов (с просчетом их в документе). В документе, имеющем приложения, дополнительно проверяется соответствие учетных номеров, грифов конфиденциальности, номеров экземпляров, количества листов в экземпляре данным, содержащимся в реквизите «Отметка о наличии приложения». Отметки о проверке проставляются в журнале учета пакетов (в графе 7) и в журнале учета поступивших документов (рядом с номером документа). Для проверки правильности присвоения регистрационных данных поступивших документов, взятых сразу на учет документов выделенного хранения без промежуточной регистрации их в журнале учета поступивших документов, привлекаются журнал учета поступивших пакетов, журнал учета документов выделенного хранения и документы. В журналах учета пакетов и документов проверяется соответствие данных о присвоенном номере, дате поступления (регистрации), номере, за которым документ направлен (графа 6 журнала учета пакетов и графа 5 журнала учета документов выделенного хранения), предприятии-отправителе. В журнале учета документов выделенного хранения и на документе проверяется соответствие присвоенного учетного номера, грифа конфиденциальности, даты регистрации, вида и заголовка документа, предприятия — отправителя, номера, за которым документ направлен, номеров экземпляров, количества листов в экземпляре (с просчетом их в каждом экземпляре). Отметки о проверке проставляются в журнале учета пакетов (в графе 8) и в журнале учета документов выделенного хранения (рядом с номерами документов).

Для проверки правильности проставления отметок о возврате ранее отправленных документов привлекаются журнал учета поступивших пакетов, соответствующие журналы учета документов и документы. В соответствующем журнале учета проверяется наличие отметки о возврате документа и ее соответствие записи в графе 9 журнала учета пакетов. В журналах учета изданных документов, документов выделенного хранения и на документах проверяется, кроме того, соответствие номеров возвращенных экземпляров. Отметки о проверке проставляются в журнале учета пакетов (в графе 9 рядом с номерами возвращенных документов). Для проверки правильности проставления отметок о возврате ранее отправленных машинных носителей используются журнал учета поступивших пакетов, журнал учета машинных носителей и носители. В графе 8 журнала учета ма-

шинных носителей проверяется наличие отметки о возврате носителя и ее соответствие записи в графе 9 журнала учета пакетов. Отметки о проверке проставляются в графе 9 журнала учета пакетов рядом с номерами возвращенных носителей.

Для проверки правильности проставления регистрационных данных дел и учетных журналов (картотек) привлекаются номенклатура дел, дела и учетные журналы (картотеки). В номенклатуре и на обложке дела (журнала) или наклейке на картотеке проверяется соответствие индекса (номера) дела (журнала, картотеки), грифа конфиденциальности, заголовка (наименования), срока хранения и номеров статей по перечню. По учетным журналам, кроме того, проверяется соответствие количества листов. Отметка о проверке проставляется в номенклатуре рядом с индексом (номером) дела, журнала или картотеки.

11.3. Проверки правильности проставления отметок о движении конфиденциальных документов, дел и носителей

Для проверки правильности проставления отметок **об отправлении документов** привлекаются учетные журналы, в которых зарегистрированы отправленные документы, и сопроводительные материалы, по которым отправлены документы (реестры, расписки, квитанции, сопроводительные письма). В журнале и сопроводительном документе проверяется соответствие записей о номере, грифе конфиденциальности, виде и наименовании документа, адресате, номерах отправленных экземпляров (по документам, зарегистрированным в журнале учета поступивших документов, вместо номеров экземпляров проверяется количество отправленных листов), наименовании, номере и дате сопроводительного документа. Подписи о проверке проставляются в графе 14 журнала учета изданных документов, графе 10 журнала учета документов выделенного хранения или в графе 14 журнала учета поступивших документов.

Для проверки правильности проставления отметок **об отправлении (возврате) ошибочно присланных документов** привлекаются журнал учета поступивших пакетов и копии, сопроводительных писем, с которыми отправлены документы. В журнале и сопроводительном письме проверяется соответствие записей о номере и грифе

конфиденциальности документа, адресате, номере и дате сопроводительного письма. Подписи о проверке проставляются в графе 10 журнала учета пакетов.

Для проверки правильности проставления отметок *об отправлении машинных носителей* привлекаются журнал учета машинных носителей и сопроводительные документы, по которым отправлены носители. В журнале и сопроводительном документе проверяется соответствие записей о виде, номере, грифе конфиденциальности носителя, адресате, номере и дате сопроводительного документа. Подписи о проверке проставляются в графе 7 журнала учета машинных носителей.

Для проверки правильности проставления отметок *об отправлении дел* привлекаются номенклатура дел и сопроводительные документы, по которым отправлены дела. В номенклатуре дел и сопроводительном документе проверяется соответствие записей об индексе (номере) и грифе конфиденциальности дела, заголовке дела, номере тома, количестве листов в томе, адресате, номере и дате сопроводительного документа. Подписи о проверке проставляются в графе 9 номенклатуры дел.

Для проверки правильности проставления отметок *об отправлении документов, изъятых из дел*, привлекаются дела, из которых изъяты документы, и сопроводительные документы, по которым отправлены изъятые документы. В сопроводительном документе, описи документов дела и справке-заместителе проверяется соответствие записей о номере, грифе конфиденциальности и количестве листов документа, адресате, номере и дате сопроводительного документа. Подписи о проверке проставляются в графе 7 описи документов дела. Кроме того, в процессе проверок правильности проставления отметок об отправлении в сопроводительном документе (за исключением сопроводительных писем) проверяется наличие подписи лица за получение пакетов и оттиска печати (штампа).

Для проверки правильности проставления отметок *об уничтожении документов выделенного хранения* привлекаются журнал учета документов выделенного хранения и акты об уничтожении дел и документов. В журнале и акте проверяется соответствие записей об учетном номере, грифе конфиденциальности, виде и заголовке документа, номерах экземпляров, количестве листов в экземпляре, номере

и дате акта об уничтожении. Подписи о проверке проставляются в графе 13 журнала учета документов выделенного хранения.

Для проверки правильности проставления отметок *об уничтожении дел и учетных журналов (картотек)* привлекаются номенклатура дел и акты об уничтожении дел и документов. В номенклатуре и акте проверяется соответствие записей об индексе (номере) и грифе конфиденциальности дела (журнала, картотеки), его заголовке, номере тома, количестве листов в томе (по картотеке — вместо номера тома и количества листов проверяется количество карточек), номере и дате акта об уничтожении. Подписи о проверке проставляются в графе 9 номенклатуры дел.

Для проверки правильности проставления отметок *об уничтожении документов, изъятых из дел*, привлекаются дела, из которых изъяты документы, и акт об уничтожении дел и документов. В акте, описи документов дела и справке-заместителе проверяется соответствие записей о номере, грифе конфиденциальности и дате документа, количестве листов, номере и дате акта об уничтожении. Подписи о проверке проставляются в графе 7 описи документов дела. Кроме того, в процессе проверок правильности проставления отметок об уничтожении документов и дел в акте об уничтожении проверяется наличие отметок о физическом уничтожении документов и дел, заверенных подписями лиц, производивших уничтожение.

Для проверки правильности проставления отметок *о переводе изданных и поступивших документов на учет документов выделенного хранения* привлекаются журналы учета изданных, поступивших документов и документов выделенного хранения и переведенные на учет выделенного хранения документы. В журнале и документе проверяется соответствие учетного номера, присвоенного при издании или поступлении документа, учетному номеру, присвоенному по журналу учета документов выделенного хранения, грифа конфиденциальности, вида, заголовка и номеров экземпляров документа, количества листов в экземпляре с просчетом листов. Подписи о проверке проставляются в графе 17 журнала учета изданных документов или в графе 13 журнала учета поступивших документов. В журнале учета документов выделенного хранения рядом с номером документа проставляется отметка о проверке правильности регистрации.

Для проверки правильности проставления отметок *о подшивке документов в дела* привлекаются дела, в которых подшиты документы, и журналы учета, в которых зарегистрированы документы. В деле и журнале проверяется соответствие учетного номера, грифа конфиденциальности, вида и наименования документа, индекса (номера) дела, количества листов в документе, номеров листов дела. Кроме того, в описи документов дела и документе проверяется соответствие даты, номера, грифа конфиденциальности, вида и наименования документа, отправителя (по поступившим документам) или адресата (по отправленным документам), номеров листов дела. Подписи о проверке проставляются в графе 16 журнала учета изданных документов или в графе 12 журнала учета поступивших документов.

Для проверки правильности проставления отметок *о перешивке документов в другие дела* привлекаются дела, из которых изъяты документы, и дела, в которые документы перешиты. В описи документов дела, в которое перешит документ, и на документе проверяется соответствие данных, перечисленных в предыдущем абзаце. В справке-заместителе и описи документов дела, из которого изъят документ, проверяется наличие данных о новом местонахождении документа и их соответствие данным описи документов дела, в которое подшит документ. Подписи о проверке проставляются в графе 7 описи документов дела, из которого изъят документ.

Для проверки правильности проставления отметок *об изъятии из дела документов*, с которых снят гриф конфиденциальности, привлекаются дела и акт передачи документов в службу открытого делопроизводства. В описи документов дела, справке-заместителе и акте проверяется соответствие данных о номере, дате и количестве листов документа, дате и номере акта о передаче. Подписи о проверке проставляются в графе 7 описи документов дела. При любом изъятии документов из дел в учетных формах, в которых документы были зарегистрированы, отметки о новом местонахождении или уничтожении документов не производятся.

Для проверки правильности проставления отметок *о передаче на архивное хранение дел и документов выделенного хранения* привлекаются номенклатура дел, журнал учета документов выделенного хранения и описи дел и документов, переданных на архивное хранение. В описи и номенклатуре проверяется соответствие индекса (но-

мера), грифа конфиденциальности, заголовка дела, номера тома дела, количества листов в томе, архивного шифра (номеров фонда, описи, единицы хранения). Подписи о проверке проставляются в графе 9 номенклатуры дел. В журнале учета документов выделенного хранения и описи проверяется соответствие номера, грифа конфиденциальности, вида и заголовка документа, номера экземпляра, количества листов в экземпляре, архивного шифра. Подписи о проверке проставляются в графе 15 журнала учета документов выделенного хранения.

Для проверки правильности проставления отметок *о передаче в службу открытого делопроизводства дел и документов выделенного хранения*, с которых снят гриф конфиденциальности, привлекаются номенклатура дел, журнал учета документов выделенного хранения и акт передачи. В номенклатуре и акте проверяется соответствие индекса (номера), заголовка дела, номера тома, количества листов, номера и даты акта. Подписи о проверке проставляются в графе 9 номенклатуры дел. В журнале учета документов выделенного хранения и акте проверяется соответствие учетного номера, вида и заголовка документа, номеров экземпляров, количества листов в экземпляре, номера и даты акта. Подписи о проверке проставляются в графе 10 журнала учета документов выделенного хранения.

Глава 12. Виды проверок наличия конфиденциальных документов

12.1. Квартальные проверки фактического наличия конфиденциальных носителей и документов

Для проверки наличия *бумажных носителей*, независимо от времени их регистрации, привлекаются носители и журнал учета бумажных носителей. На носителе и в журнале проверяется соответствие учетного номера и количества листов (с просчетом листов в носителе). В стенографических и рабочих тетрадах просчет листов можно не производить, соответствие количества листов записям в журнале проверяется по заверительной надписи в тетрадах.

Для проверки наличия *машинных носителей*, независимо от времени их регистрации, привлекаются носители и журнал учета ма-

шинных носителей. На носителе и в журнале проверяется соответствие учетного номера. Для проверки наличия *не подшитых в дела и не переведенных на выделенное хранение изданных документов*, независимо от времени их регистрации, привлекаются документы и журнал учета изданных документов. На документе и в журнале проверяется соответствие учетного номера, количества экземпляров документа и количества листов в каждом экземпляре с их просчетом. Одновременно проверяется наличие подписи за уничтожение черновика (если он был). Если на момент проверки по каким-либо причинам черновик не уничтожен, то проверяется его наличие с просчетом листов и соответствие записям в графе 5 журнала.

Для проверки наличия *не подшитых в дела и не переведенных на выделенное хранение поступивших документов*, независимо от времени их регистрации, привлекаются документы и журнал учета поступивших документов. На документе и в журнале проверяется соответствие учетного номера, количества листов основного документа и приложений (при наличии приложений) с просчетом листов. Даты проверок фактического наличия носителей и документов проставляются при журнальном способе учета в соответствующем журнале рядом с номером носителя или документа, при карточном способе — в графе 3 контрольного журнала. Поскольку проверка фактического наличия носителей и документов должна проводиться по схеме от документа к учетному журналу (карточке) и они проверяются, как правило, не в последовательности учетных номеров, а по местонахождению, то по завершении проверки всех носителей и документов выявляются непроверенные носители и документы по отсутствию дат проверок.

Если к началу квартальной проверки носитель, изданный или поступивший документ сняты с учета (уничтожены, отправлены, переведены на учет документов выделенного хранения, подшиты в дела), то в форме учета проверяется наличие отметок и подписей о произведенных операциях с установлением (кроме магнитных носителей) соответствия количества зарегистрированных листов (а по изданным документам — и экземпляров) количеству снятых с учета. Учетный номер округляется как закрытый. При карточном способе учета карточка помещается в картотеку отработанных документов. Если в процессе или по итогам квартальной проверки выявится отсутствие от-

дельных зарегистрированных документов (носителей), то должны быть приняты меры по оперативному их поиску. При отсутствии положительных результатов необходимо приказом по предприятию создавать специальную комиссию для установления причин отсутствия документов, разработки версий об их возможном местонахождении и проведения поиска документов по каждой из этих версий. При любом исходе поиска комиссия должна составлять заключение о результатах своей работы. В случае нахождения документов в заключении отражаются причины отсутствия документов в установленных для них местах и предлагаются меры по устранению таких причин. Заключение утверждается руководителем предприятия, который принимает решение о мерах наказания виновных. В соответствующих учетных формах производятся отметки о списании документов со ссылкой на номер и дату заключения комиссии. Комиссия создается и при обнаружении в ходе проверок неучтенных конфиденциальных документов (носителей). В заключении комиссии отражается действительная степень конфиденциальности этих документов, причины издания их неучтенными и формулируются предложения, направленные на предотвращение неучтенного издания документов. Выявленные неучтенные документы регистрируются в соответствующих формах учета. По результатам произведенных в течение квартала проверок правильности проставления отметок о движении документов, дел, носителей и фактического наличия носителей и документов составляется акт.

12.2. Годовая проверка наличия конфиденциальных дел

Годовая проверка наличия дел должна проводиться после подшивки в дела истекшего года всех поступивших и изданных за этот год документов и после закрытия дел (просчета листов, составления заверительной надписи дела, его прошивки и опечатывания). Если отдельные документы требуют длительного исполнения и поэтому не могут быть подшиты в дела, то их следует перерегистрировать в журнал учета документов следующего года с целью закрытия соответствующего дела за истекший год, однако по документам постоянного срока хранения такая перерегистрация может допускаться как исключение.

Для проверки наличия всех дел, зарегистрированных в истекшем и предыдущих годах, привлекаются дела и номенклатуры дел за соответствующие годы. На обложке дела и в номенклатуре проверяется соответствие индекса (номера) дела, номера тома дела, количества листов в томе. Кроме того, в делах, зарегистрированных в истекшем году, проверяется соответствие данных о количестве листов на обложке дела и в заверительной надписи.

Для проверки наличия всех документов выделенного хранения, зарегистрированных в истекшем и предыдущих годах, привлекаются документы и журнал учета документов выделенного хранения. В документе и журнале проверяется соответствие учетного номера, номеров экземпляров, количества листов в экземпляре (в документе количество листов — по заверительной надписи, если не проставлено на обложке, если проставлено, то по заверительной надписи только в документах, зарегистрированных в истекшем году). Годовая проверка наличия учетных журналов (картотек) должна проводиться после выверки и закрытия журналов (картотек) учета носителей (при погодном их учете), изданных и поступивших за истекший год документов. В ходе выверки осуществляется проверка наличия округлений (закрытия) всех регистрационных номеров (снятия носителей и документов с учета по данным регистрационным номерам) и проверка наличия карточек в картотеке отработанных документов. При этом если отдельные документы и носители перерегистрированы в журналы учета следующего года, то в журналах учета документов (носителей) текущего и следующего годов проверяется соответствие учетных данных, а на документе (носителе) — наличие нового учетного номера. Правильность отметок о перерегистрации в журнале текущего года заверяется подписями проверяющих, а в журнале следующего года рядом с номером документа (носителя) проставляется отметка о проверке правильности регистрационных данных. В закрываемых учетных формах после последнего регистрационного номера в журнале или на отдельной карточке, помещаемой в конце картотеки, производится запись: «Все учетные номера журнала (картотеки) закрыты и проверены», заверяемая подписями проверявших с проставлением даты. При наличии незакрытых учетных номеров выявляются причины и принимаются меры по закрытию.

Для проверки наличия всех учетных журналов (картотек), заведенных в истекшем и предыдущих годах, привлекаются журналы (картотеки) и номенклатура дел. В журнале и номенклатуре проверяется соответствие учетного номера, номера тома (при наличии двух и более томов), количества листов (в журнале — по заверительной надписи). В картотеке и номенклатуре проверяется соответствие учетного номера, количества карточек (в картотеке по последнему номеру карточки). Даты проверок проставляются в номенклатуре дел рядом с индексом (номером) дела (журнала, картотеки), в журнале учета документов выделенного хранения — рядом с номером документа. Выявление отсутствующих дел, документов и журналов производится путем выверки дат проверок и подписей о снятии их с учета. По результатам годовой проверки составляется акт.

В результате проверки установлено: 1. Все подлежавшие проверке дела, документы выделенного хранения и учетные журналы (картотеки) находятся в наличии. 2. Все регистрационные номера в журналах (картотеках) учета закрыты. 3. _____ дел (документов выделенного хранения) не зарегистрированы по формам учета.

При наличии заключения комиссии по фактам утрат или выявления неучтенных дел, документов выделенного хранения и журналов учета оно прилагается к акту проверки с отражением в реквизите «Отметка о наличии приложения».

12.3. Нерегламентированные проверки наличия конфиденциальных носителей, документов и дел

Нерегламентированные проверки наличия конфиденциальных носителей, документов и дел проводятся при смене руководителя и сотрудников подразделения конфиденциального делопроизводства, их временном отсутствии (болезнь, командировка, отпуск), временном отсутствии исполнителей, нарушении оттисков печатей на хранилищах документов, ликвидации предприятия. Во всех случаях они осуществляются путем проверки соответствия фактического наличия носителей, документов и дел учетным данным на них.

При смене руководителя подразделения конфиденциального делопроизводства проводится проверка наличия всех носителей, доку-

ментов и дел, независимо от времени их регистрации. Проверка проводится комиссией, назначаемой приказом руководителя предприятия. Результаты проверки отражаются в общем акте приема-передачи дел. К акту прилагаются справки сотрудников подразделения конфиденциального делопроизводства, подтверждающие наличие носителей, документов и дел, находящихся у них на хранении.

При смене сотрудника подразделения конфиденциального делопроизводства проводится проверка наличия носителей, документов и дел, находящихся на ответственном хранении сотрудника. Проверка осуществляется сдающим и принимающим сотрудниками. Результаты проверки оформляются актом приема-передачи, подписываемым этими сотрудниками и утверждаемым руководителем подразделения конфиденциального делопроизводства. В случае отсутствия сменяемого сотрудника проверка проводится комиссией. На период временного отсутствия руководителя или сотрудника подразделения конфиденциального делопроизводства числящиеся за ними документы, носители и дела, необходимые для текущей работы, передаются замещающим их лицам по разовой расписке или по акту с проверкой соответствия их фактического наличия учетным данным. При отсутствии передающего лица проверка проводится комиссией. Носители, документы и дела, которые не требуются для работы на период временного отсутствия лица, не передаются. Они должны храниться в опечатанных металлических шкафах (сейфах). При этом составляется акт, в котором указываются номера хранилищ и номер печати, которой они опечатаны. Принимающее лицо не несет ответственности за находящиеся в этих хранилищах документы, если оттиск печати на них не будет нарушен. При нарушении оттиска печати, а также в случае проникновения в помещения, в которых хранятся носители, документы и дела, посторонних лиц со вскрытием хранилищ или нарушением оттиска печатей на них приказом руководителя предприятия назначается комиссия для проверки находящихся в хранилищах документов. Результаты проверки оформляются актом. При увольнении, переводе на другую работу, перед командировкой, отпуском исполнителя находящиеся в его спецпортфеле документы и носители передаются в подразделение конфиденциального делопроизводства со списанием их в учетных формах.

В случае внезапного отсутствия исполнителя (болезнь и др.) необходимые для работы документы, находящиеся в его спецпортфеле, изымаются комиссионно с проверкой соответствия фактического наличия изымаемых документов учетным данным. При этом составляется акт изъятия документов, в котором отражается, какие документы (с указанием учетного номера и количества листов каждого документа) изъяты. Спецпортфель с оставшимися документами опечатывается печатями двух членов комиссии (с отражением в акте номеров печатей), изъятые документы списываются с исполнителя в формах учета. При ликвидации предприятия проверка наличия носителей, документов и дел проводится комиссией, назначаемой руководителем организации. Результаты проверки оформляются актом, который приобщается к общему акту о ликвидации.

Глава 13. Режим секретности

13.1. Тайна и государственная тайна, режим секретности

Одно из значений слова тайна — «нечто скрываемое от других, известное не всем, секрет». Тайну можно понимать как информацию, не подлежащую разглашению, доступ к источникам которой должен быть ограничен ради защиты чьих-то интересов.

Государственная тайна — это информация, сведения, несанкционированный доступ к которым может причинить вред интересам страны, государства. В Законе РФ «О государственной тайне» дано такое определение: «государственная тайна — защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации».

Информация тесно связана с ее носителями — материальными объектами, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов.

Правовой основой режима секретности являются Конституция РФ, Федеральный закон «О безопасности», Закон РФ «О государст-

венной тайне», а также принятые на основе последнего закона акты Президента и Правительства РФ. Например, Указ Президента РФ от 24.01.1998 № 61 «О перечне сведений, отнесенных к государственной тайне», постановления Правительства РФ от 18.09.2006 № 573 «О предоставлении социальных гарантий гражданам, допущенным к государственной тайне на постоянной основе, и сотрудникам структурных подразделений по защите государственной тайны»; от 04.09.1995 № 870 «Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности». Нужно отметить, что Закон РФ «О государственной тайне» — первый в российской истории акт такого уровня по этому вопросу. Раньше эти вопросы решались подзаконными актами, которые к тому же сами были секретными, не публиковались. Принятие по этому вопросу открытого правового акта, к тому же имеющего высшую юридическую силу, — еще один штрих в развитии российской демократии, в повышении роли закона в административно-правовом регулировании.

Можно назвать такие признаки государственной тайны:

- 1) это очень важные сведения;
- 2) их разглашение может причинить ущерб государственным интересам;
- 3) перечень сведений, которые могут быть отнесены к государственной тайне, закрепляется федеральным законом;
- 4) она охраняется мерами уголовной ответственности (ст. 275, 276, 283 УК РФ) и иными принудительными средствами;
- 5) для ее охраны создан специальный административно-правовой режим — режим секретности.

Секретность — важное средство обеспечения государственной безопасности. С другой стороны, засекречивание сведений — это предусмотренное Конституцией ограничение закрепленного ее ст. 27 права граждан «свободно искать, получать, производить и распространять информацию любым законным способом».

Режим секретности — это установленный нормативными актами единый порядок обеспечения защиты сведений, составляющих государственную тайну, включающий систему административно-правовых, организационных, инженерно-технических и других мер. Таким образом, внутриобъектовый и пропускной режимы являются неотъемлемой частью комплекса мероприятий, направленных на защиту сведений, составляющих государственную тайну, и сохранность их носителей.

13.2. Роль и место внутриобъектового и пропускного режимов в системе защиты информации предприятия

13.2.1. Внутриобъектовый и пропускной режимы

Внутриобъектовый и пропускной режимы устанавливаются, как правило, на предприятиях, осуществляющих в предусмотренном законодательством Российской Федерации порядке работу со сведениями, составляющими государственную тайну. Вместе с тем нормы и правила внутриобъектового режима могут быть применимы в случаях, когда предприятие выполняет работы и с иными видами информации с ограниченным доступом (конфиденциальной информацией). Эти случаи в данной главе оговорены особо. Внутриобъектовый и пропускной режимы представляют собой основные элементы системы защиты информации предприятия.

Организация указанных режимов — обязательное требование нормативно-методических документов по защите государственной тайны, предоставляющих предприятию право на проведение работ, связанных с использованием сведений, составляющих государственную тайну.

Внутриобъектовый и пропускной режимы на предприятии организуются в целях исключения: проникновения посторонних лиц на охраняемую (режимную) территорию и объекты предприятия, а также в служебные помещения, в которых проводятся работы с использованием сведений, составляющих государственную тайну; посещения режимных помещений без служебной необходимости сотрудниками предприятия, не имеющими к ним прямого отношения, а также командированными лицами, которым не предоставлено право на их посещение (работу в них); вноса (ввоза) на территорию предприятия личных технических средств (кино-, фото-, видео-, звукозаписывающей аппаратуры и других технических средств); несанкционированного выноса (вывоза) с территории предприятия носителей сведений, составляющих государственную тайну; нарушений установленного регламента служебного времени, распорядка работы структурных подразделений по защите государственной тайны, а также установленного порядка и режима работы сотрудников предприятия и командированных лиц с носителями сведений, составляющих государ-

ственную тайну. Организация и обеспечение внутриобъектового и пропускного режимов на предприятии направлены на соблюдение всеми сотрудниками предприятия и командированными лицами надлежащего режима секретности.

В данной главе учебного пособия раскрыты основные положения организации внутриобъектового и пропускного режимов на предприятии, их цели и задачи, а также задачи, возлагаемые на должностных лиц и сотрудников предприятий. Более подробно вопросы организации внутриобъектового и пропускного режимов изложены в нормативно-методических документах, разрабатываемых федеральными органами исполнительной власти применительно к возложенным на них функциям и в соответствии с решаемыми ими задачами. Эти нормативно-методические документы, раскрывающие особенности формирования и функционирования систем защиты информации в органах государственной власти, на предприятиях и в организациях, содержание проводимых мероприятий, относятся к документам с ограниченным доступом и в данном учебном пособии не рассматриваются.

13.2.2. Работа по организации внутриобъектового режима. Основные подходы и принципы

Внутриобъектовый режим — комплекс мероприятий, направленных на обеспечение установленного режима секретности непосредственно в структурных подразделениях, на объектах и в служебных помещениях предприятия.

Основными направлениями работы по организации внутриобъектового режима на предприятии являются:

- определение общих требований режима секретности на предприятии в соответствии с положениями нормативных правовых актов и указаний вышестоящих органов государственной власти организаций);
- ограничение круга лиц, допускаемых к сведениям, составляющим государственную тайну, и их носителям;
- регламентация непосредственной работы сотрудников предприятия, а также командированных лиц, с носителями сведений, составляющих государственную тайну;

— планирование комплекса мероприятий, направленных на исключение утечки сведений, составляющих государственную тайну, и утрат носителей этих сведений;

— организация контроля со стороны должностных лиц предприятия и структурных подразделений по защите государственной тайны за выполнением требований по режиму секретности на предприятии;

— организация работы с персоналом предприятия, допущенным к сведениям, составляющим государственную тайну, а также вновь принимаемыми на работу гражданами.

Задачи по организации внутриобъектового режима на предприятии возлагаются, как правило, на заместителя руководителя предприятия, отвечающего за вопросы защиты государственной тайны. Заместитель руководителя предприятия работу по формированию системы внутриобъектового режима организует на основе всестороннего анализа возможных каналов утечки сведений, составляющих государственную тайну, при проведении предприятием всех видов работ.

В ходе выполнения этой работы руководством предприятия используются следующие основные подходы к организации внутриобъектового режима:

— определение ответственности руководителей подразделений должностных лиц за защиту государственной тайны;

— четкое разграничение функций, возлагаемых на соответствующие структурные подразделения предприятия (служба безопасности, режимно-секретное подразделение, подразделение противодействия иностранным техническим разведкам, служба охраны и др.);

— создание эффективной системы контроля за выполнением мероприятий по режиму секретности и обеспечению сохранности носителей сведений, составляющих государственную тайну.

Руководитель предприятия и соответствующие должностные лица должны обеспечить соблюдение *основных принципов формирования системы* внутриобъектового режима:

— принципа персональной ответственности руководителей структурных подразделений, других должностных лиц и сотрудников предприятия за выполнение задач в области защиты государственной тайны;

— принципа комплексного использования имеющихся сил и средств для решения задач по защите государственной тайны;

— принципа полного охвата всех направлений деятельности предприятия, в ходе работы по которым возможна утечка сведений, составляющих государственную тайну, или утрата носителей этих сведений.

13.2.3. Меры, которые предусматривает внутриобъектовый режим

Внутриобъектовый режим предусматривает следующие меры:

- выявление возможных каналов утечки сведений, составляющих государственную тайну, и реализация мер, направленных на закрытие этих каналов;
- отнесение сведений к государственной тайне, засекречивание и рассекречивание сведений и их носителей;
- лицензирование и сертификация деятельности в области защиты информации;
- подбор и изучение кандидатур лиц для назначения на должности, требующие допуска к государственной тайне, оформление необходимых документов;
- распределение обязанностей в области защиты государственной тайны между должностными лицами и сотрудниками предприятия;
- определение круга должностных лиц, имеющих право разрешать ознакомление (работу) персонала со сведениями, составляющими государственную тайну;
- создание структурных подразделений, решающих задачи по защите государственной тайны, и определение их функций;
- предоставление сотрудникам предприятия и командированным лицам только того объема информации, который необходим им для выполнения их должностных (функциональных) обязанностей;
- допуск и непосредственный доступ сотрудников предприятия к сведениям, составляющим государственную тайну (их носителям), ограничение круга лиц, допускаемых к данным сведениям;
- проведение работы среди сотрудников, допущенных к государственной тайне, по разъяснению требований режима секретности, повышению бдительности и персональной ответственности за сохранность доверенных сведений;

- учет, хранение, размножение, уничтожение носителей сведений, составляющих государственную тайну, установление режима и порядка работы сотрудников предприятия с этими носителями сведений;

- противодействие иностранным техническим разведкам и техническая защита информации;

- организация подготовки, переподготовки и повышения квалификации сотрудников предприятия, допущенных к государственной тайне;

- организация и проведение совещаний, в ходе которых обсуждаются вопросы, содержащие сведения, составляющие государственную тайну;

- защита государственной тайны в ходе сотрудничества предприятия с иностранными партнерами (фирмами), в том числе при подготовке и проведении приема иностранных делегаций на предприятии;

- защита государственной тайны при выполнении научно-исследовательских, опытно-конструкторских и других видов совместных работ, связанных с передачей сведений, составляющих государственную тайну, другим предприятиям;

- финансовое, материально-техническое и иные виды обеспечения защиты государственной тайны;

- исключение утечки сведений, составляющих государственную тайну, в ходе издательской (публикаторской) и рекламной деятельности предприятия;

- выделение и оборудование режимных помещений, осуществление контроля доступа персонала и посетителей в эти помещения, исключение возможности бесконтрольного доступа в них;

- проведение аналитической работы, выработка на основе ее результатов перспективных (прогнозных) оценок состояния дел в области защиты государственной тайны;

- определение внутреннего распорядка и регламента предприятия;

- контроль порядка использования технических средств передачи и обработки информации, средств размножения, копирования носителей сведений, составляющих государственную тайну, и иных технических средств и устройств;

- контроль эффективности решения задач по защите государственной тайны должностными лицами и структурными подразделениями предприятия;
- контроль наличия носителей сведений, составляющих государственную тайну.

13.2.4. Силы и средства, используемые при организации внутриобъектового режима

Важнейшую роль в организации внутриобъектового режима играют руководитель предприятия и его заместитель, в соответствии со своими должностными обязанностями непосредственно возглавляющий работу по защите государственной тайны. В соответствии с нормативными актами непосредственная ответственность за организацию и осуществление мероприятий по защите государственной тайны возлагается на руководителя предприятия. Руководитель предприятия, с учетом анализа состояния защиты государственной тайны и результатов контроля эффективности решения задач по защите государственной тайны должностными лицами и структурными подразделениями предприятия, определяет (уточняет) задачи этим должностным лицам и структурным подразделениям.

Руководитель предприятия обязан:

— проявлять высокую требовательность к должностным лицам и сотрудникам предприятия, принимать меры по недопущению разглашения сведений, составляющих государственную тайну, утрат носителей сведений, строго взыскивать с сотрудников предприятия, допускающих факты безответственности и халатности в работе со сведениями, составляющими государственную тайну;

— оценивать деятельность сотрудников предприятия в области защиты государственной тайны;

— направлять работу должностных лиц и сотрудников предприятия на строгое соблюдение требований режима секретности.

Заместитель руководителя предприятия отвечает за практическую деятельность структурных подразделений предприятия и должностных лиц по защите государственной тайны. В рамках деятельности по организации внутриобъектового режима он выполняет следующие основные функции:

- непосредственно руководит разработкой организационно-планирующих документов предприятия по защите государственной тайны, организует контроль за исполнением содержащихся в них требований;

- максимально ограничивает круг должностных лиц, допускаемых к сведениям, составляющим государственную тайну;

- лично возглавляет работу на предприятии по защите государственной тайны;

- организует проведение систематического анализа деятельности структурных подразделений и должностных лиц предприятия, направленной на обеспечение защиты государственной тайны;

- организует и поддерживает строгий порядок в разработке, учете, хранении и уничтожении носителей сведений, составляющих государственную тайну, и в обращении с ними;

- организует защиту информации при использовании средств автоматизации;

- организует подбор, расстановку и обучение сотрудников структурных подразделений по защите государственной тайны;

- обеспечивает необходимые условия для правильной организации режима секретности, учета, хранения, уничтожения носителей сведений, составляющих государственную тайну, и обращения с ними;

- принимает меры по защите государственной тайны при взаимодействии предприятия с иностранными партнерами;

- лично инструктирует членов комиссий предприятия по проверке наличия носителей сведений, составляющих государственную тайну, отбору и уничтожению носителей, утративших актуальность и практическое значение, а также не требующихся в работе.

Для организации внутриобъектового режима используется совокупность имеющихся на предприятии структурных подразделений, выполняющих функции защиты государственной тайны, а также других подразделений, решающих задачи в данной сфере, и применяемых этими подразделениями средств защиты информации. В организации внутриобъектового режима участвуют следующие основные структурные подразделения предприятия: режимно-секретное подразделение, служба безопасности предприятия, подразделение противодействия иностранным техническим разведкам, подразделение ох-

раны (в части вопросов контроля внутренних объектов и служебных помещений предприятия).

Задачи, решаемые подразделением противодействия иностранным техническим разведкам, изучаются в рамках других дисциплин и в настоящем учебнике не рассматриваются.

Ведущую роль в организации внутриобъектового режима на предприятии, а также осуществлении контроля эффективности проводимых в этих целях мероприятий играет режимно-секретное подразделение.

Сотрудники режимно-секретного подразделения при решении возложенных на них задач имеют право:

- требовать от всех сотрудников предприятия соблюдения режима секретности;
- проверять состояние режима секретности в структурных подразделениях предприятия и подчиненных организациях (филиалах, представительствах);
- требовать от сотрудников предприятия письменных объяснений в случае разглашения сведений, утраты носителей сведений или других нарушений режима секретности;
- выработать рекомендации руководителям структурных подразделений предприятия по вопросам защиты государственной тайны;
- готовить руководителю предприятия мотивированные предложения о запрещении ведения тех или иных работ в случае отсутствия необходимых условий для обеспечения защиты государственной тайны или о привлечении к ответственности работников, допустивших нарушения режима секретности.

13.2.5. Организационные средства защиты информации.

В решении задач организационного обеспечения информационной безопасности предприятия важную роль играют организационные средства защиты информации.

Под организационными средствами защиты информации понимается комплекс мероприятий, планируемых и осуществляемых в целях организации внутриобъектового режима.

Они являются, по сути, связующим звеном между персоналом предприятия и различными техническими и иными средствами, используемыми в целях организации и обеспечения режима секретности.

Наиболее эффективны следующие меры по защите информации, относящиеся к организационным средствам защиты информации:

- организация разработки, внедрения и использования различных средств и систем защиты информации;
- организация разработки, размножения, учета и уничтожения носителей конфиденциальной информации с использованием технических средств;
- контроль за соблюдением персоналом предприятия установленных требований при использовании объектов информатизации;
- анализ эффективности функционирования технических систем и средств защиты информации;
- разработка и внедрение в практику инструкций и иных документов, регламентирующих порядок и правила обращения с конфиденциальной информацией.

Порядок организации внутриобъектового режима, задачи, решаемые должностными Лицами и структурными подразделениями предприятия, отражаются в разрабатываемых на предприятии внутренних организационно-распорядительных документах, утверждаемых руководителем предприятия. Сотрудники, в установленном порядке допущенные к информации с ограниченным доступом и осуществляющие непосредственную работу с этой информацией, несут ответственность за соблюдение требований нормативных актов по порядку обращения с носителями конфиденциальной информации и за сохранность этих носителей.

Сотрудники, допущенные к конфиденциальной информации, обязаны:

- знать порядок отнесения информации к категории конфиденциальной, порядок засекречивания сведений, составляющих государственную тайну, а также положения действующего на предприятии развернутого перечня сведений, подлежащих засекречиванию;
- соблюдать установленный порядок работы со сведениями конфиденциального характера и их носителями;
- строго хранить ставшие известными им в силу выполнения должностных (функциональных) обязанностей сведения конфиденциального характера;

- принимать меры по недопущению разглашения другими сотрудниками предприятия конфиденциальной информации, об имевших место таких фактах и предпосылках к ним информировать службу безопасности (режимно-секретное подразделение);

- знакомиться (работать) только с той конфиденциальной информацией (ее носителями), к которой они имеют оформленный установленным порядком допуск;

- знать степень секретности (конфиденциальности) проводных работ (мероприятий), разрабатываемых документов (материалов), соблюдать установленные правила работы и обращения с ними документами (материалами);

- соблюдать установленный порядок приема-передачи, хранения носителей конфиденциальной информации, не допускать безличного пользования ими;

- обеспечивать на своем рабочем месте такое расположение кителей конфиденциальной информации, которое позволяет исключить несанкционированное ознакомление с ними (их содержанием) посторонних лиц, а также сотрудников предприятия, не имеющих к ним непосредственного отношения;

- в порядке, определенном нормативными актами, обеспечивать учет носителей конфиденциальной информации, а также нанесение на указанные носители необходимых реквизитов;

- в определенном руководителем предприятия (структурного подразделения) объеме ознакомливать сотрудников своего предприятия и командированных лиц с содержанием носителей конфиденциальной информации, а также с тематикой и содержанием проводимых работ;

- информировать руководителя предприятия и его заместителя предпринимавшихся посторонними лицами, представителями других предприятий, иностранными гражданами попытках получения конфиденциальной информации;

- вопросы выезда за границу в служебные командировки, по частным делам и с другими целями решать в соответствии с нормативными актами и указаниями органа государственной власти руководителя предприятия.

Сотрудникам, допущенным к конфиденциальной информации, запрещается:

- нарушать установленный порядок обращения с носителями конфиденциальной информации;
- выполнять работы с носителями конфиденциальной информации вне служебных помещений и рабочих мест;
- сообщать сведения конфиденциального характера сотрудникам предприятия, не имеющим к ним непосредственного отношения, и посторонним лицам;
- выполнять записи конфиденциального характера на неучтенных в установленном порядке носителях, в том числе магнитных;
- сообщать конфиденциальные сведения кому бы то ни было по открытым средствам связи (телефон, факс, мобильная связь, электронная почта и т.п.);
- допускать обезличенное пользование носителями конфиденциальной информации, принимать и передавать указанные носители без соответствующих расписок;
- хранить носители конфиденциальной информации на столах, открытых стеллажах, в незапертых хранилищах, шкафах, сейфах, оставлять не запертыми служебные кабинеты, в которых хранятся носители конфиденциальной информации (настольные письменные наборы и т.п.);
- накапливать сведения конфиденциального характера на своем рабочем месте, в открытых носителях (в том числе в электронном виде), в открытых материалах.

Перечисленные обязанности доводятся до сведения всех сотрудников предприятия, работающих с конфиденциальной информацией (ее носителями), под расписку в журнале, хранящемся в режимно-секретном подразделении (службе безопасности). Эти обязанности доводятся также до сведения лиц, вновь назначенных на соответствующие должности (прибывших на предприятие).

Требования к помещениям, в которых проводятся работы с конфиденциальной информацией или хранятся носители информации. Организация внутриобъектового и пропускного режимов имеет целью исключение проникновения посторонних лиц в режимные помещения предприятия, а также несанкционированного посещения таких помещений сотрудниками предприятия и командированными лицами, не имеющими прямого отношения к проводимым в них работам. К помещениям, предназначенным для ведения работ с использованием

сведений, составляющих государственную тайну, или для хранения их носителей, предъявляется ряд требований. На практике данные требования, как правило, распространяются на служебные помещения и хранилища предприятия, в которых используются в работе или хранятся не только названные сведения, но и другие виды конфиденциальной информации (или ее носители). Это позволяет обеспечить сохранение конфиденциальности проводимых в указанных помещениях работ, а также надежную сохранность носителей конфиденциальной информации.

Размещение и оборудование указанных режимных помещений должны исключать возможность бесконтрольного проникновения в них посторонних лиц и гарантировать сохранность находящихся в них носителей конфиденциальной информации. Поэтому к данным помещениям предъявляются особые требования режима секретности. Входные двери этих помещений оборудуются замками, гарантирующими надежное закрытие помещений в нерабочее время, в них также могут устанавливаться кодовые и электронные замки и автоматические турникеты.

Режимные помещения, в которых в нерабочее время хранятся носители конфиденциальной информации, оснащаются охранной сигнализацией, связанной с караульным помещением, пультом централизованного наблюдения за сигнализацией службы охраны и с дежурным по предприятию. Режимные помещения, в которых имеются технические средства, разрабатываются, испытываются или эксплуатируются специальные изделия, имеющие охраняемые характеристики, оборудуются в соответствии с требованиями по противодействию иностранным техническим разведкам и технической защите информации.

Перед началом эксплуатации режимные помещения обследуются комиссией, назначаемой руководителем предприятия, и аттестуются на соответствие требованиям, предъявляемым к помещениям для проведения работ с конкретным видом конфиденциальной информации. Результаты работы комиссии оформляются актом пригодности помещения для проведения конкретных видов работ, утверждаемым руководителем предприятия. Обследование и аттестация режимных помещений проводится не реже одного раза в пять лет, а также после их ремонта или реконструкции.

В эти помещения допускается строго ограниченный круг сотрудников предприятия, имеющих прямое отношение к ведущимся в них работам. Кроме того, в них допускаются руководитель предприятия, его заместитель, руководитель службы безопасности, руководитель режимно-секретного подразделения и их заместители. Доступ других сотрудников предприятия в эти помещения в случае крайней служебной необходимости может быть разрешен заместителем руководителя предприятия, руководителем режимно-секретного подразделения или его заместителем.

Для осуществления приема и выдачи носителей конфиденциальной информации режимные помещения соответствующих структурных подразделений (режимно-секретного подразделения или службы безопасности) оборудуются специальными окнами, не выходящими в общий коридор, или выделяется часть рабочей комнаты, изолированная барьером. Размер режимных помещений определяется исходя из функций этих помещений. Для ознакомления и работы с носителями конфиденциальной информации в помещениях службы безопасности (режимно-секретного подразделения) выделяются специальные комнаты (кабины).

В режимных помещениях службы безопасности (режимно-секретного подразделения) запрещается работать с документами, не имеющими непосредственного отношения к основной деятельности данной службы (подразделения), а также хранить посторонние предметы. Для хранения носителей конфиденциальной информации помещения обеспечиваются необходимым количеством хранилищ, замки которых оборудуются приспособлениями для опечатывания. Хранилища и ключи от хранилищ учитываются в службе безопасности (режимно-секретном подразделении). Хранилища, а также входные двери помещений, в которых они находятся, оборудуются надежными замками с двумя экземплярами ключей от них, один из которых в опечатанном пенале (пакете) хранится у руководителя службы безопасности (режимно-секретного подразделения). Второй экземпляр ключей в опечатанном виде хранится у руководителя предприятия или у его заместителя.

В нерабочее время ключи от хранилищ и от входных дверей режимных помещений, в отдельных пеналах, опечатанных дежурным по службе безопасности (режимно-секретному подразделению), пере-

даются на хранение службе охраны или дежурному по предприятию. По окончании рабочего дня все хранилища и режимные помещения закрываются и опечатываются. Хранилища и входные двери помещений, в которых они находятся, опечатываются разными печатями. При опечатывании мастика (пластилин) или сургуч накладываются таким образом, чтобы исключить их снятие без повреждения оттиска печати.

Режимные помещения, в которых хранятся носители конфиденциальной информации, с опечатанными входными дверями и пеналы с ключами от них сдаются под охрану службе охраны или дежурному по предприятию с указанием времени приема-сдачи и проставлением соответствующих отметок о включении и выключении охранной сигнализации.

Порядок приема-сдачи под охрану режимных помещений определяется инструкцией, специально разрабатываемой службой безопасности (режимно-секретным подразделением) и утверждаемой руководителем предприятия.

Сдачу под охрану и вскрытие помещений производят ответственные за эти помещения сотрудники предприятия на основании утвержденных руководителем предприятия списков этих сотрудников с образцами их подписей. Списки находятся в службе охраны или у дежурного по предприятию. Сотрудники предприятия, которым предоставлено право вскрытия, сдачи под охрану и опечатывания помещений, отвечают за соблюдение в этих помещениях установленных требований режима секретности.

При отсутствии сотрудников предприятия, ответственных за помещения, в которых хранятся носители конфиденциальной информации, данные помещения могут быть вскрыты комиссией, создаваемой по указанию руководителя предприятия (его заместителя) с составлением акта. Перед вскрытием помещений сотрудники, ответственные за их, проверяют целостность печатей и исправность замков. При обнаружении нарушения целостности оттисков печатей, повреждения замков, а также других признаков, указывающих на возможное проникновение в эти помещения или хранилища посторонних лиц, вскрытие не производят, о случившемся составляют акт и немедленно ставят в известность руководителя предприятия, руководителя службы безопасности (режимно-секретного подразделения) и орган безо-

пасности. Одновременно принимаются меры по охране места происшествия, до прибытия сотрудников органа безопасности в эти режимные помещения никто не опускается.

В случае утраты ключа от хранилища или от входной двери помещения режимно-секретного подразделения (службы безопасности) немедленно ставят в известность руководителя этого подразделения. В установленном порядке осуществляют замену замка или его секрета. Хранение носителей конфиденциальной информации в хранилищах, от которых утрачены ключи, до замены замка или изменения его секрета запрещается.

13.3. Компоненты защиты режима секретности

Режим секретности является постоянным, общегосударственным. Его требования обязательны для исполнения на территории Российской Федерации и за ее пределами органами власти, местного самоуправления, предприятиями и организациями независимо от их организационно-правовой формы и формы собственности, должностными лицами и гражданами России, взявшими на себя обязательства либо обязанными по своему статусу исполнять требования законодательства о государственной тайне.

Как и вся иная деятельность исполнительной власти, деятельность по обеспечению секретности должна быть эффективной: основанной на принципах целесообразности, законности, оперативности.

Главные элементы режима секретности: правила засекречивания, защиты государственной тайны, рассекречивания. Их можно рассматривать и как стадии производства по обеспечению секретности.

Не подлежат засекречиванию сведения о:

- чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях;
- состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, преступности;
- привилегиях, компенсациях и льготах, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям;

- фактах нарушения прав и свобод человека и гражданина, нарушения законности органами государственной власти и их должностными лицами;
- размерах золотого запаса и государственных валютных резервах Российской Федерации;
- состоянии здоровья высших должностных лиц России.

Отнесены к государственной тайне и засекречены могут быть названные в законе сведения в военной области, о внешней политике, экономике, научно-исследовательских и проектных работах, технологиях, имеющих важное оборонное или экономическое значение, о разведывательной, контрразведывательной, оперативно-розыскной деятельности.

Должностные лица, засекретившие такие сведения, могут быть привлечены к ответственности, а граждане вправе обжаловать такие акты в суд.

Засекречивание сведений и их носителей состоит в установлении ограничений на их распространение и на доступ к их носителям.

Установлены три степени секретности и соответствующие им грифы (реквизиты), проставляемые на самом носителе и (или) в сопроводительном документе на него: «особой важности», «совершенно секретно» и «секретно». Степень секретности сведений, составляющих государственную тайну, должна соответствовать размеру ущерба, который может быть причинен безопасности страны в случае их распространения. Правила отнесения информации к той или иной степени секретности устанавливаются Правительством РФ.

Президент утверждает Перечень должностных лиц, наделенных полномочиями по отнесению сведений к государственной тайне.

Такой перечень был утвержден распоряжением Президента от 30 мая 1997 г. В нем названы руководители ряда федеральных ведомств, а также руководитель Администрации Президента РФ, начальник Главного управления специальных программ Президента.

Государственные органы, руководители которых наделены правом засекречивать информацию, разрабатывают развернутые перечни сведений, подлежащих засекречиванию. Основанием для засекречивания является соответствие информации перечням сведений, подлежащих засекречиванию. Уполномоченному должностному лицу направляются предложения о засекречивании, оно принимает решение

о необходимости делать это и степени секретности. При засекречивании, помимо прочих обстоятельств, необходимо учитывать реальную возможность сохранить тайну и экономическую целесообразность (соответствие расходов на обеспечение тайны и пользы от этого, влияние засекречивания на экономические связи и т.д.).

Защита государственной тайны прежде всего предполагает *организационное обеспечение*: создание ведомств, органов, структурных единиц, которые постоянно и профессионально занимаются этим делом. Иными словами, необходимо организационное обеспечение. Оно представлено Межведомственной комиссией по защите государственной тайны, Федеральной службой безопасности. Федеральным агентством правительственной связи и информации, службой фельдъегерской связи, Службой внешней разведки, государственной технической комиссией и другими административными ведомствами и исполнительными органами государственной власти.

А в организациях, предприятиях, учреждениях созданы специальные подразделения, обеспечивающие режим секретности (в прошлом они чаще всего назывались первыми отделами). Ответственность за организацию защиты государственной тайны органом, предприятием, учреждением возлагается на его руководителя.

Второй компонент защиты — система допуска должностных лиц, граждан, организаций к государственной тайне. Допуск предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по ее защите осуществляется путем получения ими в установленном порядке лицензий на проведение работ со сведениями соответствующей степени секретности.

Допуск должностных лиц и граждан России к государственной тайне производится в порядке разрешительного производства. Заинтересованные лица подают заявления в компетентные органы, прилагая к ним необходимые документы. Властные субъекты проверяют, нет ли оснований для отказа (наличие судимости за тяжкое преступление, медицинских противопоказаний, постоянное проживание заявителя или его близких родственников за границей и др.). Допуск лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов к го-

сударственной тайне осуществляется в исключительно разрешительном порядке, устанавливаемом Правительством РФ.

Допуск не разрешается, если лицо уклоняется от проверочных мероприятий, сообщает заведомо ложные анкетные данные. С учетом результатов проверочных мероприятия руководитель организации принимает решение о допуске или об отказе в нем. При положительном решении определяется одна из трех форм допуска, соответствующая трем степеням секретности.

Лица, допущенные к государственной тайне, становятся носителями специального административно-правового статуса, который включает ряд специальных обязанностей и прав. Допуск предполагает, в частности, принятие гражданами на себя обязательств по нераспространению доверенных им сведений, составляющих государственную тайну; письменные согласия на проведение в отношении их полномочными органами проверочных мероприятий; определение видов, размеров и порядка предоставления льгот, ознакомление с нормами законодательства Российской Федерации о государственной тайне, предусматривающими ответственность за его нарушение.

Допуск связан с согласием лица на частичное, временное ограничение права выезда за границу.

За работу со сведениями, составляющими государственную тайну, лица, допущенные к ней на постоянной основе, получают ежемесячно процентную надбавку к должностному окладу (тарифной ставке) в зависимости от степени секретности сведений (соответственно 25, 20 и 10%). А сотрудникам структурных подразделений по защите государственной тайны производится ежемесячная надбавка за стаж работы в этих подразделениях в размере:

- 5% — при стаже работы от 1 до 5 лет;
- 10% — при стаже работы от 5 до 10 лет;
- 15% — при стаже работы свыше 10 лет.

Допуск должностного лица, гражданина к государственной тайне может быть прекращен по решению руководителя органа государственной власти, предприятия, учреждения или организации в связи с проведением организационно-штатных мероприятий (сокращения штатов, ликвидации, организации и т.д.), а также даже за однократное нарушение лицом взятых на себя обязательств по соблюдению режима секретности.

Прекращение допуска является дополнительным основанием для расторжения с гражданином трудового договора (контракта), но не освобождает его от взятых обязательств по неразглашению сведений.

В соответствии с Гражданским процессуальным кодексом РФ иски, связанные с государственной тайной, рассматриваются судами субъектов РФ.

В особом, упрощенном порядке, без прохождения разрешительной процедуры допускаются к секретным сведениям члены Совета Федерации, депутаты Государственной Думы, судьи на период исполнения ими своих полномочий, а также адвокаты, участвующие в качестве защитников в уголовном судопроизводстве по делам, связанным со сведениями, составляющими государственную тайну. Указанные лица предупреждаются о неразглашении государственной тайны, ставшей им известной в связи с исполнением ими своих полномочий, и о привлечении их к ответственности в случае ее разглашения, о чем у них отбирается соответствующая расписка.

Передача секретной информации от одной организации другой, другим государствам (т.е. распоряжение сведениями, составляющими государственную тайну) производится только с разрешения компетентного органа государственной власти. Для обеспечения режима секретности установлены правила проведения совещаний, на которых используются сведения, составляющие государственную тайну.

В этом деле широко применяются разнообразные технические средства шифрования, передачи, хранения данных. Транспортировка ее носителей обеспечивается Федеральной службой фельдъегерской связи. На органы ФСБ России возложена обязанность осуществлять контроль за обеспечением сохранности сведений, составляющих государственную тайну, в государственных органах, воинских формированиях, на предприятиях и в учреждениях независимо от форм собственности.

Рассекречивание сведений и их носителей — снятие ранее введенных ограничений на распространение информации и на доступ к ее носителям. Как правило, оно, как и засекречивание, производится в административном порядке, по решению тех должностных лиц, которые признали, что сведения относятся к государственной тайне.

По общему правилу срок засекречивания не должен превышать тридцати лет, и носители государственной тайны рассекречиваются

не позднее сроков, установленных при их засекречивании. В исключительных случаях срок рассекречивания может быть продлен путем принятия специального решения.

Необходимо отметить, что некоторые сведения: об оперативно-розыскной, разведывательной деятельности и др. никогда не должны рассекречиваться.

Рассекречивание может производиться досрочно. Во-первых, в связи с международными обязательствами России. Во-вторых, из-за изменения объективных обстоятельств, вследствие которого дальнейшая защита сведений, составляющих государственную тайну, является нецелесообразной. Закон обязал органы государственной власти, руководители которых наделены полномочиями по отнесению сведений к государственной тайне, периодически, но не реже чем через каждые 5 лет, пересматривать содержание действующих перечней сведений, подлежащих засекречиванию, в части обоснованности засекречивания сведений и их соответствия установленной ранее степени секретности.

Досрочное рассекречивание может быть осуществлено руководителями органов государственной власти, предприятия, организаций, если они установят, что их подчиненные необоснованно засекретили носители информации. Граждане вправе обращаться с запросами о рассекречивании в архивы и другие организации. Кроме того, обоснованность отнесения сведений к государственной тайне может быть обжалована в суд. Сведения могут быть рассекречены по просьбе гражданина или на основании решения суда.

Рекомендуемая литература

Основная литература

Егоров, В. П. Документовед и его профессия / В. П. Егоров, А. В. Слиньков, Е. В. Карпычева. — М. : Юридический институт МИИТ, 2012.

Егоров, В. П. Конфиденциальное делопроизводство / В. П. Егоров, А. В. Слиньков. — М. : Юридический институт МИИТ, 2015.

Нормативные документы

Конституция Российской Федерации: принята всенародным голосованием 12.12.1993 (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ).

Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ.

Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ.

Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ.

Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне».

Федеральный закон от 22.12.2008 № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации».

Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне».

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Указ Президента РФ от 22.05.2015 № 260 «О некоторых вопросах информационной безопасности Российской Федерации»

Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года (утверждены Президентом РФ 24.07.2013 № Пр-1753).

Постановление Правительства РФ от 22.09.2009 № 754 «Об утверждении Положения о системе межведомственного электронного документооборота».

Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

Постановление Правительства РФ от 06.05.2016 № 399 «Об организации повышения квалификации специалистов по защите информации и должностных лиц, ответственных за организацию защиты информации в органах государственной власти, органах местного самоуправления, организациях с государственным участием и организациях оборонно-промышленного комплекса».

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 (утверждены приказом Минкультуры России от 31.03.2015 № 526).

Приказ Минкультуры России от 25.08.2010 № 558 «Перечень типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения».

Приказ Минздравсоцразвития России от 22.04.2009 № 205 «Об утверждении Единого квалификационного справочника должностей руководителей, специалистов и служащих, раздел «Квалификационные характеристики должностей руководителей и специалистов по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, противодействию техническим разведкам и технической защите информации».

ГОСТ Р 52551—2006. Система охраны и безопасности. Термины и определения.

ГОСТ Р 52292—2004. Информационная технология. Электронный обмен информацией. Термины и определения.

ГОСТ Р 6.30—2003. Унифицированные системы документации. Унифицированная система организационно — распорядительной документации. Требования к оформлению документов.

ГОСТ Р 7.0.8—2013 СИБИД. Делопроизводство и архивное дело. Термины и определения.

«ОК 011—93. Общероссийский классификатор управленческой документации» (утвержден постановлением Госстандарта России от 30.12.1993 № 299).

**Виктор Павлович ЕГОРОВ,
Алексей Владимирович СЛИНЬКОВ**

**ДЕЛОПРОИЗВОДСТВО
И РЕЖИМ СЕКРЕТНОСТИ**

Учебное пособие

Редакция Юридического института МИИТа

Изд. заказ 15	Бумага офсетная	Тираж 60 экз.
Подписано в печать 25.05.2016	Печать трафаретная	Цена договорная
Усл. печ. л. 11,6	Уч.-изд. л. 9,0	Формат 60x84/16

127994, Москва, А — 55, ул. Образцова, 9. стр. 9.