Понятие и характеристика конфиденциальной информации

Информация представляет собой сведения, которые регламентированы правовыми нормами. Существует два вида информации: сведения, находящиеся в открытом и в ограниченном доступе. Между открытой и конфиденциальной информацией имеются принципиальные различия.

Распространение конфиденциальной информации создает угрозу экономической безопасности и наказывается в соответствии с действующим законодательством.

Понятие и виды конфиденциальной информации

Согласно Федеральному закону Российской Федерации «Об информации, информационных технологиях и о защите информации» № 149-ФЗ, сведения делятся на два вида:

- информация для общего пользования. Вид данных, находящихся в открытом доступе для всех граждан РФ;
- данные с закрытым доступом. Вид сведений, которые ограничены нормативно-правовыми актами РФ и доступны только определенным категориям лиц, которые получают доступ к информации в связи со своими служебными полномочиями.

Понятие конфиденциальной информации

В широком смысле слова, конфиденциальная информация – это сведения с ограниченным доступом. В узком смысле, конфиденциальная информация имеет особую ценность для лиц, пребывающих на государственной службе или работающих в организации.

Законодатель раскрывает понятие «конфиденциальность информации» в Федеральном законе «Об информации» № 149ФЗ. Согласно ст. 2 закона, к данным ограниченного доступа относятся сведения, которые не могут быть переданы третьим лицам без согласия на это обладателя данных.

Конфиденциальная информация представляет собой определенную тайну, поскольку она доступна только

нескольким категориям лиц, имеющим право и доступ на работу с ней. Охрана и правовая защита конфиденциальных данных гарантирована государством и закреплена в Конституции РФ. В основном законе РФ указано, что гражданин, организация и государство, имеют право на тайну.

Основными источниками правового регулирования конфиденциальной информации в РФ являются:

- международные договоры и соглашения;
- конституция РФ;
- федеральные законы; • законы субъектов;
- локальные акты.

Виды конфиденциальной информации

Конфиденциальная информация делится на несколько видов в зависимости от содержания и от того, в каком кругу используется:

1. Служебная тайна.

Согласно Указу Президента № 188 «Об утверждении Перечня сведений конфиденциального характера», под служебной тайной понимают информацию, имеющую особую ценность, доступ к которой ограничивается государственными органами РФ в соответствии с действующим законодательством.

Информация, являющаяся служебной тайной, также регулируется положениями Постановления Правительства РФ № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».

В указанном Постановлении закреплены правовые положения о работе с информацией, составляющей служебную тайну:

- обязательное проставление отметки «Для служебного пользования»;
- передача сотрудникам информации, содержащей служебную тайну, только под расписку;
- хранение сведений «Для служебного пользования» в сейфах;

- уничтожение документов, содержащих служебную тайну только по акту;
- копирование документов со служебной тайной с письменного согласия руководителя.

2. Коммерческая тайна.

В соответствии со ст. 3 Федерального закона «О коммерческой тайне» № 98-ФЗ, под коммерческой тайной понимается режим ограничения использования, передачи и распространения информации, которая позволяет ее обладателю получить материальную или нематериальную выгоду.

Обладание чужой коммерческой тайной позволяет конкурентам увеличить прибыль, избежать лишних расходов, получить привилегии на рынке товаров и услуг.

Согласно закону № 98-ФЗ, сведениями, составляющими коммерческую тайну, могут быть результаты интеллектуальной деятельности, научно-техническая информация, которая представляет собой особую коммерческую ценность для организации.

Ценность коммерческой тайны заключается в том, что она известна лишь определенному кругу лиц и недоступна третьим лицам. Примером коммерческой тайны может служить производство по уникальной технологии какой-либо продукции.

Законодатель, помимо прочего, указывает, какие сведения не могут признаваться коммерческой тайной:

- сведения из единого государственного реестра юридических и физических лиц, подтверждающие факт внесения записи в реестр;
- лицензии и сертификаты, которые дают право заниматься предпринимательской деятельностью;
- сведения о количестве сотрудников и размере заработной платы на предприятии;
- информация, касающаяся задолженности или невыплаты заработной платы и любых социальных выплат;
- сведения о нарушении законов и привлечении к юридической ответственности;

- информация, касающаяся безопасности граждан, общества в целом и окружающей среды;
- список лиц, имеющих право совершать юридические действия без доверенности;
- информация о проведении конкурсов или аукционов по приватизации государственной или муниципальной недвижимости.

3. Персональные данные.

Федеральный закон «О персональных данных» № 152-ФЗ поясняет, что можно считать персональными данными. Исходя из ст. 3 закона, персональные данные – это любые сведение относящиеся (прямо или косвенно) к субъекту персональных данных, то есть физическому лицу.

Согласно закону, получение, обработка, хранение и иные действия с персональными данными физического лица, производятся только с согласия последнего.

При этом лицо, которое занимается обработкой персональных данных, не имеет права разглашать сведения, которые ему предоставляет гражданин. В исключительных случаях допускается передача таких данных, если физическое лицо лично дает на это согласие, либо это предусмотрено действующим законодательством.

4. Тайна уголовного судопроизводства.

В Уголовно-процессуальном кодексе РФ (УПК РФ), закреплено положение, которое запрещает разглашать сведения, касающиеся уголовного дела на стадии предварительного расследования.

Следователь или дознаватель обязан сообщить участникам уголовного судопроизводства о недопустимости разглашении сведений по уголовному делу, о чем составляется соответствующая расписка.

Однако в ст. 161 УПК РФ говорится о том, что в исключительных случаях данные предварительного расследования могут предать гласности с разрешения лиц, ведущих расследование. Также, законодатель отмечает, что

информация, которая может быть оглашена, не должна противоречить интересам следствия и участников уголовного судопроизводства.

При этом запрещается разглашение сведений, которые содержат информацию о частной жизни участников уголовного дела, а также несовершеннолетних граждан, которые не достигли возраста 14 лет.

5. Судебная тайна.

В судопроизводстве также существует конфиденциальная информация, которая называется судебная тайна. В любой отрасли права (административной, гражданской и уголовной) законодатель закрепляет принцип ее соблюдения.

Сущность данного принципа состоит в следующем:

- судья или коллегия судей выносят решение только в совещательной комнате;
- никто, кроме судей, не имеет право участвовать при вынесении решения, за исключением присяжных заседателей;
- при участии в судебном разбирательстве присяжные заседатели не имеют права разглашать решения суда;
- неразглашение информации по делам особой категории. Несмотря на то, что в РФ одним из принципов судопроизводства является гласность, то есть открытость судебного заседания, имеется ряд дел, по которым заседание в обязательном порядке должно быть закрытым. К таким делам, например, относятся все дела, касающиеся защиты прав и интересов несовершеннолетних.

6. Профессиональная тайна.

Профессиональная тайна есть практически в каждой профессии: врач, адвокат, нотариус, психолог. Для каждого специалиста существует особое понятие профессиональной тайны, которая регламентированное в различных правовых актах.

Например, адвокаты руководствуются Федеральным законом № 63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации». В ст. 8 закона указано, что адвокатской тайной признаются сведения, которые стали известны адвокату при оказании юридической помощи своему доверителю. При этом недопустим допрос адвоката по обстоятельствам, которые стали ему известны в ходе профессиональной деятельности.

Аналогичные правовые положения закреплены для нотариусов, врачей и иных специалистов, получающих сведения, которые не подлежат разглашению. Каждый сотрудник, который получает доступ к данным, подписывает документ о неразглашении сведений.

Защита конфиденциальной информации

Для того чтобы не произошла утечка конфиденциальной информации, необходимо предпринимать соответствующие меры, которые препятствовали бы этому. Законодатель закрепил правовые положения о защите данных в Федеральном законе «Об информации, информационных технологиях и защите информации» № 149.

Также существует несколько правовых способов защиты сведений ограниченного доступа. Законодательное регулирование по вопросам, связанным с защитой сведений ограниченного доступа, заключается также в закреплении юридической ответственности за разглашение такой информации.

Защита информации

Как упоминалось выше, положения, регламентирующие вопросы по защите конфиденциальной информации, закреплены в ФЗ № 149. В соответствии с законодательством, под защитой информации понимается:

- обеспечение защиты сведений ограниченного доступа от неправомерного посягательства;
- соблюдение режима ограниченного доступа к ограниченным данным;

- принятие мер по реализации права на доступ к ограниченной информации.

Законодательное координирование данных ограниченного доступа заключается также в том, чтобы принять меры по защите информации:

- предотвращение утечки информации;
- своевременное обнаружение попытки незаконно получить доступ к информации;
- предупреждение последствий, которые возникают при несанкционированном доступе к сведениям;
- постоянный мониторинг уровня защиты информации;
- возможность восстановить данные, которые были уничтожены;
- размещение информации ограниченного доступа в базах данных на территории РФ.

Для защиты критичных данных существуют следующие виды защиты:

- **Физическая.** Физическая защита заключается в хранении информации в специальных сейфах или хранилищах, доступ к которым разрешен узкому кругу лиц.
- **Аппаратная.** Аппаратный способ защиты предполагает хранение информации на специальных компьютерах или серверах, которые постоянно контролируются с целью предотвращения несанкционированного доступа к данным.
- **Программная.** Защита информации осуществляется с помощью программного обеспечения, которое своевременно блокирует неразрешенные действия пользователей и предотвращает утечку сведений.
- **Математическая (криптографическая).** Математическая защита позволяет шифровать данные, делая их прочтение недоступным для третьих лиц.

Ответственность за правонарушения в сфере информации

Согласно ст. 17 Федерального закона № 149, за нарушение требований, установленных для конфиденциальных сведений, наступает юридическая ответственность.

Правовые нормы закрепляют следующие виды ответственности:

- **Дисциплинарная.** Данный вид ответственности применяется, когда работник совершил дисциплинарный проступок. Например, разгласил персональные данные коллеги третьим лицам.
- **Гражданско-правовая.** Указанный вид ответственности предполагает взыскание морального или материального вреда за разглашение сведений ограниченного доступа.
- **Административная.** К административной ответственности привлекается лицо, совершившее преступление, предусмотренное Кодексом об административной ответственности. Например, разглашение и распространение информации с ограниченным доступом.
- **Уголовная.** Уголовная ответственность за преступление в сфере информации может наступить вследствие незаконного способа получения информации, например, за взлом программного обеспечения.

Правовое регулирование конфиденциальной информации помогает обеспечивать ее сохранность и защиту. При этом гарантом защиты являются сразу несколько нормативных актов, регулирующих правовые вопросы, касающиеся сведений ограниченного доступа.

Отличительные черты служебной и конфиденциальной информации

Процесс выявления и регламентации реального состава информации, представляющей ценность для предпринимателя, в том числе составляющей тайну фирмы,

является основополагающей частью системы защиты информации.

Принимая во внимание, что система зашиты ценной и конфиденциальной информации является дорогостоящей технологией, определение состава сведений, подлежащих защите, должно базироваться на принципе экономической целесообразности их защиты. Поэтому анализ информационных ресурсов фирмы осуществляется с учетом двух основных критериев: степени заинтересованности конкурентов в информации и степени ценности информации (стоимостной, правовой, деловой).

Для анализа необходимо иметь не только полный перечень реальных и потенциальных конкурентов, но и знать слабые и сильные стороны их деятельности, обладать информацией о состоянии дел у каждого конкурента, разрабатываемых новшествах, сотрудничестве со структурами промышленного шпионажа или криминальными структурами. На этой основе можно с полной уверенностью определить, что и какую информацию фирма не хотела бы раскрывать конкурентам. Необходимо также определить экономическую значимость новшества, рассчитать величину ущерба от его утраты и на этой основе сделать вывод о том, является ли оно предметом коммерческой тайны и объектом зашиты.

Следует учитывать, что **вопрос о конфиденциальности информации возникает в** случаях, принятия фирмой новой стратегии развития, заключения выгодных контрактов, появления технического или технологического новшества, установления факта потенциальной или реальной угрозы этому новшеству со стороны конкурента. При определении размера ущерба от возможной утраты информации учитывается стоимость продукции, которая не будет произведена, потери от замораживания капитальных вложений, стоимость произведенных научно-исследовательских работ и другие убытки.

В процессе анализа выделяются главные элементы информации, отражающие фирменный секрет. Это дает возможность удешевить систему защиты и сделать ее максимально целенаправленной, динамичной и эффективной. Защита всего новшества, включая общеизвестные его составляющие, как правило, желаемого результата не дает за счет громоздкости системы защиты и трудности контроля больших объемов конфиденциальной информации. Массовость засекречивания ведет к росту штатной численности служб безопасности и в конечном счете к снижению эффективности защиты и утрате информации. Например, есть смысл защищать новую формулу в известном рецепте производимого продукта, новый алгоритм известных действий, новый прибор в производимом оборудовании и т.п.

Информация может быть отнесена к коммерческой (предпринимательской) тайне и стать конфиденциальной при соблюдении следующих условий:

- информация не должна отражать негативные стороны деятельности фирмы, нарушения законодательства, фальсификацию финансовой деятельности с целью неуплаты налогов и другие подобные факты;
- информация не должна быть общедоступной или общеизвестной;
- возникновение или получение информации предпринимателем должно быть законным и связано с расходованием материального, финансового или интеллектуального потенциала фирмы;

— персонал фирмы должен знать о ценности такой информации и быть обучен правилам работы с ней;

— предприниматель должен быть в состоянии выполнить реальные действия по защите этой

информации, т.е. иметь, например, средства для закупки или разработки системы защиты информации.

В соответствии с постановлением Правительства РФ «О перечне сведений, которые не могут составлять коммерческую тайну» от 05.12.91 № 35 (с изм. от 03.12.2002) к конфиденциальным не могут быть отнесены следующие сведения и документы:

- учредительные документы (решение о создании предприятия или договор учредителей) и устав;
- документы, дающие право заниматься предпринимательской деятельностью (регистрационные удостоверения, лицензии, патенты); р. — сведения по установленным формам отчетности о финансово-хозяйственной деятельности и иные сведения, необходимые для проверки правильности исчисления и уплаты налогов и других обязательных платежей в государственную бюджетную систему РФ;

— документы о платежеспособности;

— сведения о численности, составе работающих, их заработной плате и условиях труда, а также о наличии свободных рабочих мест;

— документы об уплате налогов и обязательных платежей;

— сведения о загрязнении окружающей среды, нарушении антимонопольного законодательства, несоблюдении безопасных условий труда, реализации продукции, причиняющей вред здоровью населения, а также других нарушениях законодательства РФ и размерах причиненного при этом ущерба;

— сведения об участии должностных лиц предприятия в кооперативных, малых предприятиях, товариществах, акционерных обществах, объединениях и других организациях, занимающихся предпринимательской деятельностью.

В отличие от государственной тайны состав сведений, составляющих коммерческую тайну, государством централизованно не регламентируется и определяется индивидуально каждой фирмой. Одновременно фирма устанавливает необходимый уровень конфиденциальности этих сведений, степень требуемой их защиты, длительность защиты, ее стоимость и технологию защиты. Состав ценной и конфиденциальной информации подлежащей защите, определяется собственником или владельцем этих сведений и фиксируется в специальном перечне. В основе перечня лежит типовой состав защищаемых сведений фирм данного профиля.

Перечень конфиденциальных сведений фирмы представляет собой классифицированный список типовой и конкретной ценной информации о выполняемых работах, производимой продукции, научных и деловых идеях, технологических новшествах. В нем закрепляется факт отнесения сведений к защищаемой информации и определяется период (срок) конфиденциальности (то есть недоступности для всех) этих сведений, уровень (гриф) их конфиденциальности, список должностей сотрудников фирмы, которым дано право использовать эти сведения в работе. В перечень включаются действительно ценные сведения («изюминки») о каждой работе фирмы.

Перечень является постоянным рабочим материалом руководства фирмы, служб безопасности и конфиденциальной документации. Поэтому он должен регулярно обновляться и корректироваться. Ограничение доступа к информации, относящейся к новой продукции, но не обладающей ценностью, применяться не должно.

Важной задачей перечня является дробление коммерческой тайны на отдельные информационные элементы, известные разным лицам. Закрепление информации за конкретными должностями позволяет снизить вероятность раскрытия секрета сотрудниками и предотвратить возможность

включения ими в документы избыточной конфиденциальной информации.

Перечень необходим также для выделения конфиденциальных документов из общего документопотока, соответствующего их маркирования (грифования) и автономной обработки, использования и хранения. При рассмотрении в судах дел о краже сотрудниками информации и понесенных фирмой в связи с этим убытках перечень используется в качестве доказательства отнесения этих сведений к разряду конфиденциальных.

Ведение перечня заключается в регулярной его корректировке и обновлении, отражающих новые перспективные разработки фирмы, переход на выпуск нового вида продукции, изменение тематики работы, направлений деятельности, конъюктуры рынка и т.п. В процессе ведения в перечень включается конфиденциальная информация, отражающая реальные новшества, разработки и изобретения. С этой целью руководители структурных подразделений фирмы или направлений ее деятельности должны регулярно составлять реестры новой индивидуальной конфиденциальной информации и информации, потерявшей свою конфиденциальность. Реестры предоставляются в комиссию для внесения изменений в перечень.

Перевод сведений, включенных в перечень, из категории конфиденциальных в категорию открытых, т.е. исключение сведений из перечня, осуществляется указанной выше комиссией по представлению руководства фирмы, структурных подразделений и службы безопасности.

На основании перечня конфиденциальных сведений служба безопасности или служба конфиденциальной документации фирмы составляет и ведет классифицированный **перечень ценных и конфиденциальных документов фирмы,** подлежащих защите с указанием обозначаемого на них грифа ограничения доступа и состава сотрудников, допущенных к этим документам. Перечень составляется в рамках структурных

подразделений или направлений деятельности фирмы и регламентирует два аспекта работы сотрудников фирмы с конфиденциальными документами: а) состав издаваемых подразделением документов и документов, направляемых в подразделение для работы, б) состав конфеденциальных сведений, которые могут быть включены в каждый указанный в перечне документ. Утверждается перечень первым руководителем фирмы.

В перечень включаются также документы, не содержащие защищаемую информацию, но представляющие ценность для фирмы и подлежащие охране от многообразия угроз, Часто обычный открытый правовой акт важно сохранить в целостности и безопасности от похитителя или стихийного бедствия. Перечни формируются индивидуально каждой фирмой в соответствии с рекомендациями специальной комиссии и утверждаются первым руководителем фирмы. Этаже комиссия регулярно вносит текущие изменения в перечни в соответствии с динамикой выполнения фирмой конкретных работ.

В перечне должно быть положение, что сохранение коммерческой тайны партнеров является неотъемлемой частью деятельности фирмы. Открытая публикация сведений, полученных на договорной или доверительной основе или являющихся результатом совместной производственной деятельности, допускается лишь с общего согласия партнеров. При заключении любого договора (контракта) стороны должны брать на себя взаимные письменные обязательства по защите конфиденциальной информации другой стороны и документов, полученных при переговорах, исполнении условий договора.

Следовательно, в целях определения состава защищаемых сведений и документов каждая фирма должна составлять и регулярно обновлять соответствующие перечни, без которых система защиты информации фирмы не может функционировать. Важно, что эти перечни носят индивидуальный характер для каждой фирмы и отражают реальную информационную сферу направлений ее деятельности,

требования собственника информации по ограничению доступа персонала к информации, составляющей интеллектуальную собственность фирмы.

Документирование конфиденциальной информации (составление конфиденциальных документов) является более сложным процессом по сравнению с аналогичной работой по составлению открытого документа. Усложнение процесса определяется объективной необходимостью создать условия для обеспечения сохранения в тайне сведений, включаемых в документ.

В ходе составления конфиденциальные документы подвергаются максимально возможному спектру угроз, которые реализуются за счет:

— документирования конфиденциальной информации на случайном носителе, не входящем в сферу контроля службы конфиденциальной документации (КД);

— подготовки к изданию документа, не обоснованного деловой необходимостью или не разрешенного для издания, т.е. документирования определенной информации;

— включения в документ избыточных конфиденциальных сведений, что равносильно разглашению тайны фирмы;

— случайного или умышленного занижения грифа конфиденциальности сведений, включенных в документ;

— изготовления документа в условиях, которые не гарантируют сохранность носителя, конфиденциальность информации;

— утери оригинала, черновика, варианта или редакции документа, его части, приложения к документу, умолчания этого факта и попытки подмены утраченных материалов;

— сообщения содержания проекта конфиденциального или открытого документа постороннему лицу, несанкционированного копирования документа или его части (в том числе на неучтенной дискете);

- утечки информации по техническим каналам;
- ошибочных действий работника службы КД,

особенно в части нарушения разрешительной системы доступа к документам.

В основе санкционированной работы персонала с конфиденциальными документами, а также правомерности документирования сотрудниками конфиденциальных сведений лежит **разрешительная система доступа к секретам фирмы.** Разрешительная (разграничительная) система доступа в сфере коммерческой тайны представляет собой совокупность правовых норм и требований, устанавливаемых собственником информации с целью обеспечения регламентированного использования сотрудниками доверенных им ценных сведений, необходимых для выполнения служебных обязанностей.

Важно, что в отличие от открытых документов процесс документирования конфиденциальной информации насыщен специфическими технологическими этапами и процедурами. Выделяются следующие основные этапы:

— получение разрешения на издание конфиденциального документа;

— установление уровня грифа конфиденциальности сведений, подлежащих включению в будущий документ;

— оформление и учет носителя для документирования выделенного комплекса конфиденциальной информации;

— составление вариантов и черновика текста документа;

— получение разрешения на изготовление документа;

— учет подготовленного черновика конфиденциального документа;

— изготовление проекта конфиденциального документа;

— издание конфиденциального документа.

Указанные этапы характеризуются не только регламентированной технологией, но и жесткими правилами работы исполнителей с конфиденциальной информацией. Сам

факт фиксирования ценной информации на носителе предполагает наличие защитных мер в отношении информации и носителя от различных рисков.

Передача конфиденциальной информации по деловой необходимости партнерам, посредникам, работникам государственных учреждений допускается только в случаях, установленных законодательством или соответствующим пунктом в контракте, и только по их письменному запросу с указанием конкретного состава и назначения требуемых сведений. Информация передается им также всегда в письменном виде за подписью первого руководителя фирмы и с информированием об этом руководителя службы безопасности. Передача конфиденциальных сведений в устной форме не разрешается.

Общеизвестно, что в наибольшей безопасности находится конфиденциальная информация, не зафиксированная на каком-либо носителе. Угрозы ценной информации появляются немедленно при возникновении мысли о необходимости ее документирования. В связи с этим система защиты конфиденциальной информации должна начинать функционировать не после издания (подписания) конфиденциального документа, а заблаговременно, т.е. до момента нанесения на чистый лист бумаги первых письменных знаков будущего документа. Перед реализацией мысли о создании документа первоначально решаются вопросы: а) является ли данная информация конфиденциальной и, если да. б) какой уровень грифа конфиденциальности ей должен быть присвоен.

До решения вопроса о присвоении будущему документу грифа конфиденциальности должно быть **получено разрешение первого руководителя фирмы на издание этого документа.** Как правило, для типовых категорий документов такое разрешение определяется наличием данного типа документа в утвержденном первым руководителем фирмы перечне ценных и конфиденциальных документов фирмы. При отсутствии

предполагаемого документа в этом перечне вопрос издания решается индивидуально, а решение первого руководителя фиксируется им на носителе, предназначенном для составления черновика данного документа.

Своевременное **установление грифа конфиденциальности сведений**, подлежащих включению в будущий документ, является одним из основных элементов защиты до ванной информации, позволяющим обеспечить относительно надежную безопасность тайны фирмы.

В основе присвоения документу грифа конфиденциальности должны лежать: перечень конфиденциальных сведений фирмы, требования партнеров, условия контрактов, а также перечень ценных и конфиденциальных документов фирмы. Руководители фирмы и структурных подразделений, филиалов фирмы имеют право присваивать гриф конфиденциальности любому разрешенному для издания, но не включенному в перечень документу, если это не противоречит действующему законодательству. Система грифования (маркирования) документов не гарантирует сохранность информации, однако, позволяет четко организовать работу с документами и, в частности, сформировать систему доступа к документам персонала.

Гриф конфиденциальности или гриф ограничения доступа к традиционному, машиночитаемому или электронному документу представляет собой реквизит (элемент, служебную отметку, помету, пометку) формуляра документа, свидетельствующий о конфиденциальности содержащихся в документе сведений и проставляемый на самом документе и (или) сопроводительном письме к нему. Грифы ставятся на всех экземплярах документа, учетных и отчетных формах, черновиках, вариантах и копиях, в которых содержится хотя бы один из конфиденциальных показателей.

Информация и документы, отнесенные к коммерческой (предпринимательской) тайне, имеют несколько уровней грифа

ограничения доступа, соответствующих различным степеням конфиденциальности информации.

Первый, массовый уровень — грифы «Конфиденциально», «Конфиденциальная информация». Не следует ставить гриф «Коммерческая тайна», т.к. грифом обозначается не вид тайны, а характер ограничения доступа к документу.

Второй уровень, достаточно редкий — грифы «Строго конфиденциально», «Строго конфиденциальная информация», «Конфиденциально. Особый контроль». Этот гриф присваивается документу лично первым руководителем фирмы, им изменяется или отменяется. Использование и хранение документов с этим грифом также организуется первым руководителем с возможным привлечением руководителя службы КД.

На документах, содержащих сведения, отнесенные к служебной тайне, ставится гриф «Для служебного пользования», «Служебная информация» или «Не для печати».

Гриф ограничения доступа, указываемый на документе, не сокращается по написанию. Под обозначением грифа указывается номер экземпляра документа, срок действия грифа и иные условия его снятия. Гриф располагается на первом и титульном листах документа, а также на обложке дела (тома) в правом верхнем углу. На электронных документах и документах, записанных на любых машинных носителях, гриф обозначается на всех листах. Ниже грифа или ниже адресата могут обозначаться ограничительные пометы типа: «Лично», «Только в руки», «Только адресату», «Лично в руки» и др. При регистрации конфиденциальных документов к его номеру добавляется сокращенное обозначение грифа конфиденциальности, например: № 37к, 99ск, 97дсп.

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

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

На ценных, но не конфиденциальных документах может проставляться помета (отметка, надпись, штамп), предполагающая особое внимание к сохранности таких документов. Например: «Собственная информация фирмы», «Информация особого внимания», «Копии не снимать», «Хранить в сейфе» и др. Может ставиться штамп, что данная информация без согласия фирмы не может быть использована в каких-либо коммерческих целях и по миновании надобности должна быть возвращена собственнику. Гриф или штамп обязательно проставляются при направлении конфиденциальной для фирмы информации в государственные учреждения, которые обязаны держать ее в тайне.

Гриф конфиденциальности присваивается документу:

— исполнителем при подготовке к составлению проекта документа;

— руководителем структурного подразделения (направления деятельности) или руководителем фирмы при согласовании или подписании документа;

— работником службы КД при первичной обработке поступающих документов, если конфиденциальный для фирмы документ не имеет грифа ограничения доступа.

Изменение или снятие грифа конфиденциальности документа производится при изменении степени конфиденциальности и ценности содержащихся в нем сведений. Основаниями для этих действий являются:

— соответствующая корректировка перечней конфиденциальных сведений или документов фирмы;

— истечение установленного срока действия грифа;

— наличие события, при котором гриф должен быть изменен или снят (например: опубликование ноу-хау в печати, патентование изобретения и др.);

— установление факта неправильности присвоения грифа документу.

Руководители всех рангов и исполнители несут персональную ответственность за своевременное и правильное установление, изменение и снятие грифа конфиденциальности. Фактическое изменение или снятие грифа осуществляет должностное лицо, подписавшее (утвердившее) документ, а также первый руководитель фирмы.

Процедуры изменения и снятия грифа конфиденциальности с документов фирмы должны быть четко регламентированы. В целях своевременного информирования соответствующих должностных лиц о необходимости выполнения этих процедур сотрудник службы КД должен регулярно просматривать учетные карточки или инвентарные описи конфиденциальных документов и выявлять те документы, по которым могут быть изменены характеристики ограничения доступа.

При изменении или снятии грифа должностное лицо делает отметку на самом документе и в сопроводительном письме путем зачеркивания грифа или написания нового, указания основания для выполнения этого действия и проставления подписи и даты. В соответствии с этой отметкой делаются необходимые записи в учетной форме документа. После снятия грифа документ передается в службу открытого делопроизводства фирмы. При необходимости об изменении или снятии грифа конфиденциальности с документа сообщается заинтересованным фирмам и предприятиям.

Следующим принципиально важным вопросом, решаемым заблаговременно руководством фирмы, службой КД и исполнителями, т.е. до начала составления текста документа, является определение необходимости **предварительной регистрации носителя** (листов бумаги, специальных тетрадей и блокнотов с отрывными листами, листов ватмана, фото пленки, магнитных носителей и т.п.), на котором будет формироваться черновик и беловик документа. Назначение учета носителей

конфиденциальной информации состоите том, чтобы обеспечить безопасность информации, контроль за ней не только в подлиннике документа, но в черновых материалах, вариантах и редакциях документа, отдельных записях и подготовительных материалах. На чистом носителе информации ставится избранный гриф конфиденциальности будущего документа.

Носителями документированной конфиденциальной информации могут быть:

-для традиционных текстовых документов: специальный блокнот с отрывными листами и корешком, выполняющим функцию учета листов, нанесения отметок о целевом их использовании; рабочая и стенографическая тетради для больших по объему документов; отдельные пронумерованные листы бумаги, типографские формы и бланки документов;

-для чертежно-графических документов: пронумерованные листы ватмана, кальки, пленки, координатной бумаги и т.п.;

-для машиночитаемых документов: маркированные и пронумерованные магнитные ленты, диски, дискеты, карты и т.п.;

-для аудио- и видеодокументов: маркированные и пронумерованные кассеты с магнитной пленкой, лазерные диски, кассеты с кинопленкой и т.п.;

-для фотодокументов: маркированные и пронумерованные кассеты с фотопленкой фотобумага, микрофиши, слайды, кассеты с микрофотопленкой и т.п.

Основными задачами учета носителей конфиденциальной информации или, как часто их называют в научной литературе — документов предварительного учета, можно назвать следующие:

-закрепление факта присвоения носителю категории конфиденциальности, ограниченного доступа;

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

-документирование фактов перемещения носителя между сотрудниками фирмы, за крепление персональной
ответственности за его сохранность;

- контроль работы исполнителя над документом и своевременного уничтожения носителя или его частей, потерявших практическое значение.

Все типы носителей конфиденциальной документированной информации должны быть учтены до начала составления на них проектов черновика, вариантов и беловика будущего документа. При этом реализуются следующие требования обеспечения зашиты информации:

-формирование основы для последующей персональной ответственности сотрудника за сохранность носителя, повышенного внимания к нему;

- предупреждение возможности нецелевого использования носителя или его неправильного хранения;

- формирование грифа конфиденциальности будущего документа;

- предупреждение возможности тайной подмены носителя, изъятия из него или включения в него отдельных частей (листов, кусков фото-, видео- или магнитно пленки), для
чего фиксируются технические характеристики носителя (количеств листов, длина ленты, наличие склеек и др.);

- предупреждение технической возможности тайной разборки кассет, пеналов, футляров, конвертов и иных оболочек, содержащих технические носители информации;

- включение носителя в сферу регулярного контроля сохранности и местонахождения.

В службах КД коммерческих фирм бумажные носители текстовой и технической информации ставятся на инвентарный (перечневый) учет. В этих структурах учет носителей целесообразен только на уровне руководства фирмы, т.к. именно здесь концентрируется вся действительно ценная информация. На уровне исполнителей документирование элементов конфиденциальной информации ведется на не учитываемых предварительно носителях.

Однако не следует думать, что неучитываемый носитель — это любой кусок бумаги, котором можно фиксировать конфиденциальные сведения и который затем можно смять и выбросить в мусорную корзину. Неучитываемый носитель — это блокнот или тетрадь пронумерованными листами, наличием заверительной надписи и росписью целевого использования каждого листа. Обязательно учитываются типовые формы и бланки доку, ментов. На чистых листах бумаги ставится штамп службы КД, листы нумеруются. У носителя может отсутствовать учетный номер, но в опись документов, находящихся у исполнителя, он обязательно вносится. Исполнитель в любой момент должен быть готов отчитаться об использовании каждого листа.

В производственных и исследовательских фирмах, обладающих оригинальными технологиями и производственными секретами типа «ноу-хау», конфиденциальные документы на всех уровнях управления целесообразно составлять только на предварительно учтенных носителях информации.

Обязательному инвентарному учету и маркировке на всех уровнях управления и в любых структурах подлежат магнитные носители информации, для которых угрозы представляют значительно большую опасность, чем для бумажных, а обнаружение реализации этих угроз возможно только на основе сложных аналитических наблюдений. Маркировка предусматривает нанесение на носитель инвентарного номера, даты регистрации, наименования структурного подразделения и

фамилии исполнителя. Надписи делаются механически стойким красителем. Одновременно этим же веществом окрашиваются винты и иные детали, скрепляющие корпус кассеты, дискеты или футляра с целью сигнализирования об их несанкционированном вскрытии.

Этап оформления и учета носителей конфиденциальной информации, выдачи их исполнителям и приема от исполнителей выполняется в службе КД как в традиционном, так и автоматизированном режимах и включает в себя следующие процедуры:

— первичного оформления носителя, в процессе которого выполняются специализированные операции, позволяющие в дальнейшем контролировать подлинность носителя и сохранность всех его элементов;

— традиционного или автоматизированного учета носителя, при котором документируется факт включения носителя в категорию носителей ограниченного доступа с присвоением ему инвентарного номера;

— окончательного оформления носителя, в процессе которого учетные данные переносятся на носитель и его составные части для их идентификации;

— выдачи учтенного, укомплектованного носителя информации исполнителю, закрепление за исполнителем персональной ответственности за сохранность носителя, его целостность и целевое использование;

— выдачи исполнителю при необходимости дополнительных учтенных листов, форм и бланков;

— приема от исполнителя носителя информации, в процессе которого проверяется комплектность носителя, наличие оправдательных отметок за отсутствующие элементы и документирование факта передачи носителя в службу КД;

— ежедневной проверки правильности учета носителей и их наличия.

При работе с сотрудником фирмы работник службы КД педантично решает следующие задачи обеспечения защиты информации:

- предотвращение выдачи носителя лицу, не связанному с составлением конкретного документа или исключенному из состава лиц, допускаемых к данному носителю (составляемому документу);
- выявление факта утраты носителя или его частей, организация поиска носителя проведения служебного расследования;
- предотвращение нарушения принципа персональной ответственности за сохранность носителя и фиксируемой в нем информации;
- обнаружение факта подмены носителя другим, фальсификации части носителя;

-обнаружение фактов случайной или умышленной порчи носителя, изменения фор мата, нумерации листов, вырывания листов, их загрязнения, склеивания и т.п.:

- предотвращение несанкционированной и не оправданной деловой необходимостью передачи носителя между руководителями и исполнителями;
- предотвращение несанкционированного ознакомления посторонних лиц с содержанием информации, зафиксированной на носителе, в процессе его выдачи исполнителю и прием от исполнителя.

Следовательно, до начала составления черновика конфиденциального документа должен быть выполнен ряд принципиально важных технологических этапов обеспечения сохранности тайны фирмы, которые дают возможность в будущем свести к минимуму риск утраты ценной информации, документирование которой пока только предполагается.

Проекты конфиденциальных документов должны обязательно визироваться руководителем службы КД. При визировании ему предъявляются все экземпляры документа со всеми приложениями, а также их учетные формы.

Если в процессе визирования или подписания проекта документа принимается решение об изменении уровня грифа конфиденциальности, то такое изменение должно быть срочно внесено во все экземпляры документа, черновик, редакции документа, в учетные формы и описи. Изменение грифа во всех указанных материалах заверяется росписью работника службы КД и датируется.

Следовательно, документирование конфиденциальных сведений — изготовление конфиденциального документа сопровождается рядом специфических технологических этапов, необходимых для решения задач обеспечения сохранности всех носителей и конфиденциальность документируемой информации. Иной порядок изготовления конфиденциальных документов неминуемо приведет к утрате секретов фирмы.

Требования к условиям работы с информацией, содержащей личную и служебную тайну

Федеральное законодательство по защите информации устанавливает принципы и методы ее классификации. Определенные законодательные акты также вносят ряд ограничений на получение и использование стратегически значимой информации и регламентируют правила обращения с ней. Базовым разделителем является признание определенного вида сведений общедоступными данными либо конфиденциальной информацией.

Закон определяет, что ограничения на обработку и получение определенных видов информации могут быть установлены исключительно федеральными законами.

Соответственно, любой вид данных, не указанный в специальном законе, считается общедоступным.

Информацию можно условно разделить на четыре категории в зависимости от условий ее получения или правил распространения:

- данные с неограниченным доступом и свободой распространения;
- данные, которые предоставляются исключительно с согласия лиц, принимающих участие в соответствующих отношениях. Например, перед заключением договора купли-продажи граждане добровольно предоставляют свою персональную информацию нотариусу;
- сведения, которые федеральное законодательство предписывает распространять либо публиковать;
- данные, содержащие угрозу государству или безопасности граждан. Распространение такого типа информации ограничивается или блокируется.

Гарантии общедоступности информации

Руководителям организаций стоит помнить, что закон определяет некоторые виды информации, к которым должен быть обеспечен доступ широкой общественности. В эту категорию входят:

- законодательство и нормативы, которые содержат гарантии гражданских прав и свобод. Запрещено ограничивать сокрытие от граждан сведений об их законных правах. В открытом доступе должны храниться и сведения об обязанностях граждан;
- правовая база формирования и функционирования различных органов власти. Сведения о полномочиях силовых и прочих структур власти;
- сведения о решениях органов власти, отдельных руководителей госструктур и коллективных выборных органов самоуправления, за исключением особых случаев, предусмотренных соответствующим законодательством;

- сведения о состоянии бюджетов разных уровней, о трате бюджетных средств и об изменениях, вносимых после их утверждения. Исключение составляют данные, которые подпадают под определение «государственная (служебная) тайна»;
- фонды библиотек и архивных служб с открытой информацией, экспозиции государственных музеев;
- данные в системах информирования, которые создают органы власти для донесения своих решений до общества;
- данные проверок экологического благополучия и мониторинга состояния окружающей среды;
- прочие сведения, закрытие доступа к которым запрещено. Например, благотворительные обязаны публиковать ряд данных о своей структуре и деятельности.

Государственная тайна

Законодательство разделяет информацию с ограниченным доступом на две категории: относящаяся к государственной тайне либо к конфиденциальной информации. По степени закрытости наиболее четко классифицированы сведения, признанные государственной тайной.

Существуют три степени системы защиты информации. Этим степеням соответствуют уровни доступа, которые присваивают данным. К ним могут относиться политикоэкономические, военные, разведывательные или агентурные данные. Под грифами особой важности или секретности сохраняют также научно-технологическую и личную информацию, составляющую государственную тайну.

Прочие виды конфиденциальной информации

Установить значение понятия «конфиденциальность» помогает закон об информации. Последний определяет ее как обязательства, накладываемые на лицо, которое имеет в своем

распоряжении информацию. Обязательства включают в себя обеспечить сохранность данных от несанкционированного доступа третьих лиц без законного согласия их обладателя. В исключительных случаях требуется сокрытие самого факта существования определенного набора данных. Классификацию, которая систематизирует конфиденциальную информацию, можно увидеть в указе №188 «О сведениях конфиденциального характера». Согласно указу, в перечень входят:

1. Данные об обстоятельствах и фактах личной жизни человека, которые способны его идентифицировать. Их называют «персональные данные». Исключение составляют те сведения, которые гражданин либо юридическое лицо обязаны распространить в определенных обстоятельствах, определяемых законом;

2. Данные, разглашение которых может повлиять на осуществление следственных действий или судебного производства;

3. Служебная тайна или данные для служебного использования. Доступ к такой информации предоставляется служащему исключительно для исполнения определенных задач из сферы его служебного ведения. Она не может быть использована с какой-либо иной личной целью;

4. Сведения, которые человек получает как специалист в ходе своей профессиональной деятельности. Доступ к ним регулируется отдельными нормативами и зачастую бывает ограничен частично или полностью;

5. Коммерческая тайна. В эту категорию входят, например, отчеты о финансовом состоянии, планирование и записи о деловой активности. Такую информацию допустимо блокировать согласно внутреннему регламенту коммерческих структур;

6. Сведения об инновациях, их сути, чертежах, прототипах или промышленном образце. Изобретения защищаются от

шпионажа и копирования до публикации официальной открытой информации о них.

Рассмотрим перечисленные категории более подробно.

Обработка персональных данных

Любую информацию, которая непосредственно связана с лицом, определяет его и способна его идентифицировать, можно отнести к категории персональных данных. Закон предусматривает определенные правила обработки персональной информации. Без согласия физического лица запрещена деятельность по получению, владению, использованию и обработке информации о его жизни. Это же касается и действий, которые нарушают личную либо семейную тайну, вторгаются в конфиденциальную переписку и прочие коммуникации, телефонные переговоры, корреспонденцию и иные сообщения. Исключения составляют действия, основанные на законном судебном решении.

Обязанности работодателя при работе с персональной информацией работников регламентируются Трудовым кодексом. Служащие, которые имеют доступ к ее обработке, перед приемом на работу подписывают соглашение о своих правах и обязанностях при работе в этой сфере.

Требование о неразглашении персональной информации применимо и к служащим органов ЗАГС, как и к работникам консульств, на которых возложены идентичные функции по регистрации актов граждан, находящихся на территории иностранных государств. Закон накладывает на работников органов ЗАГС или консульств обязательство о неразглашении информации, полученной ими в ходе служебной деятельности. Данные, которые содержат акты регистрации, приравниваются к закрытой информации и не могут иметь свободный доступ.

За незаконный сбор и распространение информации о частной жизни граждан возможно уголовное преследование.
Кодекс запрещает раскрытие личной либо семейной тайны, распространение таких данных, публичную их демонстрацию

или публикацию в средствах информации. Уголовная ответственность наступает, если подобные действия:

- производились без согласия обладателя данных;
- были совершены в соответствии с корыстными интересами либо иной заинтересованностью третьего лица;
- причинили моральные страдания, нанесли ущерб законным интересам либо нарушили права гражданина.

Тайна судебного и следственного производства

Недопустимость разглашения данных следствия прямо установлена статьей 161 УПК РФ. Эта статья запрещает опубликование информации, полученной следователями на этапе предварительного расследования. В исключительных случаях такие сведения могут быть раскрыты общественности с согласия прокурора либо следователя. Подобное раскрытие возможно только в объеме, который:

- существенно не повлияет на ход расследования;
- не будет негативно влиять на объективность расследования;
- не нарушает интересы лиц, участвующих в следственном производстве.

К предварительному следственному процессу может быть привлечен довольно широкий круг гражданских лиц — свидетели, понятые, эксперты в различных областях знания. Каждого из них предупреждают о запрете разглашения конфиденциальных сведений, которые стали ему известны в ходе исполнения следственных мероприятий. Если раскрытие информации состоялось по вине предупрежденного лица без санкции прокурора либо следователя, это влечет уголовную ответственность.

Правила обращения со служебной информацией

Перечень «сведений конфиденциального характера» утвержден соответствующим указом Президента. В перечне определен комплекс понятий, действие

которых раньше регулировалось исключительно внутренними приказами служб и предприятий. Служебная тайна здесь внесена как комплекс служебных данных, доступ к которым при необходимости могут ограничивать представители государственной власти.

Постановлением Правительства определен порядок оборота служебной информации с лимитированным доступом. К служебной тайне причисляют несекретную информацию, которая касается деятельности государственных учреждений, если вследствие служебной необходимости ее разглашение ограничено. Постановление предписывает, что документы и их копии, которые содержат служебную информацию с ограниченным доступом, должны обрабатываться и храниться отдельно от основного документооборота.

Правила обращения с профессиональной тайной

К профессиональным тайнам можно отнести данные, которые человек получает в ходе исполнения своих трудовых, договорных либо служебных обязанностей. Условия обращения с информацией, которая содержит разные виды профессиональной тайны, определены в ряде законодательных актов. Чаще всего это законы, которые регулируют коммерческие и гражданские взаимоотношения в определенных сферах.

Так, закон «Об адвокатуре» разъясняет понятие «Адвокатская тайна». Любые данные, которые имеет адвокат в результате работы с доверителем после предоставления ему юридических услуг, являются адвокатской тайной. Адвоката нельзя допрашивать в качестве свидетеля в тех же судебных производствах, в которых он оказывал юридическую помощь.

Нотариусам и работникам нотариальных контор нельзя предавать огласке сведения или документы, к которым они получили доступ в ходе совершения нотариальных действий. Более того, нотариус находится под действием такого запрета даже если ушел из профессии и отказался от нотариальной практики. Запрет распространяется и на бывших сотрудников

нотариальных контор. Справочные сведения, оригиналы и копии документов, связанных с информацией о нотариальных актах, могут получить исключительно клиенты, от имени которых были совершены такие действия.

Законодательство РФ предписывает особое обращение с данными, в которых содержится врачебная тайна. К таким данным относятся:

- факт обращения в медицинское учреждение. Это в равной степени относится к клиникам и практикам всех форм собственности;
- общие данные о состоянии здоровья человека, его биологических характеристиках и анамнезе;
- диагноз заболевания, предыдущие диагнозы и сведения о методах лечения;
- любой иной комплекс данных, который был получен в ходе диагностики и лечения.

Закон запрещает разглашение подобных данных врачами, медработниками и персоналом учреждений здравоохранения. Запрет касается также лиц, обладающих такой информацией в результате учебной, профессиональной или любой другой законной деятельности.

Закон «О почтовой связи» предусматривает ряд правил и средств защиты корреспонденции. Соблюдение этих правил способствует сохранности личной информации во время ее обработки. Закон защищает тайну корреспонденции, в том числе почтовых посылок, телеграмм и сообщений. Под действие ограничений, связанных с тайной связи, подпадают данные:

- об имени и месте проживания клиентов почтовых сервисов;
- о времени оформления почтовых посылок и адресах получателей;
- о факте получения или пересылки почтовых переводов. Не подлежат разглашению и получаемые или отправляемые суммы;

- о времени пересылки и содержании телеграмм, обрабатываемых представителем сервиса связи.

Выдачу посылки, переведенных средств, телеграмм и прочих сообщений до востребования работник отделения обязан производить только адресатам или их законным представителям. Нарушение тайны связи согласно ст. 138 УК Российской Федерации карается штрафными санкциями либо лишением свободы на срок до 5 лет.

Коммерческая тайна

Закон «О коммерческой тайне» дает исчерпывающее определение данного понятия. Она определена как набор конфиденциальных данных, который дает ее владельцу ряд преимуществ при текущем положении на рынке или в будущем. К преимуществам относят прежде всего увеличение прибыльности бизнеса. Кроме того, соблюдение режима коммерческой тайны способствует снижению риска непредвиденных трат, сохранению своего положения на рынке и продвижению в конкурентные сферы, а также получению любой иной выгоды.

Данный закон предписывает принятие определенных мер по организации защиты документации, составляющей коммерческую тайну. Указаны некоторые способы предотвращения несанкционированного доступа к таким данным и методы работ с подобной информацией. Одной из них, например, является утверждение специального грифа «Коммерческая тайна» на документах с ограничениями по праву доступа.

Сведения об изобретениях и разработках

Изобретатели и новаторы могут использовать патентирование как способ защиты своих прав. Пока действующая модель или образец, произведенный промышленным способом, не представлены общественности, данные о сущности изобретения, его чертежи и технические расчеты являются конфиденциальными данными. Разрешается регулировать степень доступности информации об изобретениях

до ее официальной публикации и получения патента. Способы организации безопасной среды для таких данных и схемы применения защитных мер для подобной информации устанавливаются внутренними регламентами конструкторских бюро.

Существует много видов информации с ограниченным доступом: государственная, личная, коммерческая, служебная и профессиональная. Правовой режим большинства из этих групп представлен в отечественном законодательстве. К сожалению, между некоторыми законодательными актами существуют противоречия, которые могут приводить к потере ценных данных. Устранять такие несоответствия в процессе работы, создавая внутренние инструкции и правила по работе с информацией ограниченного доступа — одна из главных задач руководителя.

В Положении закреплен порядок формирования, использования и уничтожения документов, содержащих служебную информацию ограниченного распространения. При формировании такого документа решение о необходимости проставления на нем пометки «Для служебного пользования» и о придании конфиденциальности сведениям, содержащим служебную информацию ограниченного распространения, принимается его исполнителем и должностным лицом, подписывающим или утверждающим документ. Указанная пометка и номер экземпляра проставляются в правом верхнем углу первой страницы документа, на обложке и титульном листе издания, а также на первой странице сопроводительного письма к документу.

Прием и учет (регистрация) документов, содержащих служебную информацию ограниченного распространения, ведут, как правило, структурные подразделения, которым поручены прием и учет несекретной документации.

Документы с пометкой «Для служебного пользования» оформляются и печатаются в специальном структурном

подразделении органа исполнительной власти — машинописном бюро. На обороте последнего листа каждого экземпляра документа специалист должен указать количество отпечатанных экземпляров, фамилию исполнителя, свою фамилию и дату печатания документа. Отпечатанные и подписанные документы вместе с черновиками и вариантами передаются для регистрации работнику, осуществляющему их учет. Черновики и варианты уничтожаются этим работником с отражением факта уничтожения в учетных формах. С этого момента документы приобретают конфиденциальное состояние и передаются с разрешения руководителя подразделения работникам под расписку, пересылаются сторонним организациям фельдъегерской связью, заказными или ценными почтовыми отправлениями.

Документы, содержащие конфиденциальные сведения, учитываются, как правило, отдельно от несекретной документации. Однако при незначительном числе таких документов разрешается вести их учет совместно с несекретными документами. В этом случае к регистрационному индексу документа добавляется пометка «ДСП».

Документы с пометкой «Для служебного пользования» хранятся в надежно запираемых и опечатываемых шкафах (ящиках, хранилищах), размножаются (тиражируются) только с письменного разрешения соответствующего руководителя, размноженные документы подлежат учету поэкземплярно.

При необходимости направления документов с пометкой «Для служебного пользования» в несколько адресов составляется указатель рассылки, в котором поадресно проставляются номера экземпляров отправляемых документов. Указатель рассылки подписывают исполнитель и руководитель структурного подразделения, готовившего документ.

Исполненные документы с пометкой «Для служебного пользования» группируются в дела в соответствии с номенклатурой дел несекретного делопроизводства. При этом на

обложке дела также проставляется пометка «Для служебного пользования».

В случаях утраты документов, дел и изданий, содержащих служебную информацию ограниченного распространения, либо разглашения этой информации ставится в известность руководитель организации и назначается комиссия для расследования обстоятельств утраты или разглашения. Результаты расследования докладываются руководителю, назначившему комиссию, после чего на утраченные документы составляется акт, на основании которого делаются соответствующие отметки в учетных формах. Акты на утраченные дела постоянного срока хранения после их утверждения передаются в архив для включения в дело фонда.

При снятии с документов пометки «Для служебного пользования» на документах, делах или изданиях, а также в учетных формах делаются соответствующие отметки и информируются все адресаты, которым эти документы (издания) направлялись.

Уничтожение дел и документов с пометкой «Для служебного пользования», утративших практическое значение и не имеющих исторической ценности, производится по акту. В учетных формах об этом делается отметка со ссылкой на соответствующий акт.

За разглашение служебной информации ограниченного распространения, а также нарушение порядка обращения с документами, содержащими такую информацию, государственный служащий (работник организации) может быть привлечен к дисциплинарной или иной предусмотренной законодательством ответственности.

Например, в соответствии со ст. 37 Федерального закона от 27 июля 2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации» служебный контракт с гражданским служащим может быть расторгнут по инициативе нанимателя в случае разглашения служебной информации, ставшей известной гражданскому служащему в связи с

исполнением им должностных обязанностей[1]. Согласно ст. 13.14 КоАП РФ за разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, может наступить административная ответственность.

Оснащение и оборудование хранилищ документов

Хранение документов — одна из основных функций любого архива. Хранятся документы не в виде мертвого груза, а для того, чтобы ими пользовались в течение тех сроков, пока они представляют ценность (а иногда это могут быть и века).

Весь период хранения документы должны быть ограждены от хищений, потерь по небрежности, или из-за неблагоприятных условий, от порчи физической основы документов (бумаги, пленки, и т.п.) и нанесенного на них изображения.

Важнейшим условием обеспечения сохранности документов является хранение документов в специально оборудованных архивохранилищах с поддержанием определенного режима хранения. Двери в хранилище в рабочее время должны быть плотно закрыты, а после окончания рабочего дня двери опечатываются или пломбируются.

Основные требования к хранению документов едины для государственных и ведомственных архивов.

Расположение архивного здания выбирают вдали от пожароопасных объектов и объектов с опасным пыле- и газовыделением. Приспособленные под архив здания и помещения принимают после целевой экспертизы с участием

архивных, пожарных, санитарных, строительных служб по акту. Экспертиза должна установить состояние здания и его пригодность с учетом потенциальных нагрузок на перекрытия.

Не принимаются в эксплуатацию следующие объекты: деревянные; ветхие; подвальные и чердачные; без отопления и вентиляции; с печным отоплением; с магистральными тепло-, водо-, газо- и электрокоммуникациями; в зданиях с огнеопасными, химическими, пищевыми технологиями.

Однако в основном для государственных архивов строят специальные здания. Разработаны типовые проекты для архивов с различным объемом хранилищ. В них предусмотрены помещения для обеспыливания и реставрации документов.

Помещение для архива должно быть изолировано. Для исключения сырости и опасности затопления трубы отопительной системы, проложенные в помещении архива или в коридоре, заключаются в изоляционные кожухи и подлежат постоянному контролю. Рабочие комнаты также отделяются от хранилища.

Если архивохранилище помещается на первом этаже, окна заделываются металлическими решетками (которые должны открываться наружу); если из архива имеется выход во двор или на улицу, дверь обшивается металлическими листами. Архивохранилища должны быть оборудованы охранной сигнализацией.

Помещение для архива должно отвечать требованиям пожарной безопасности. В нем запрещено пользоваться электронагревательными приборами, а также зажигать спички и курить. Для искусственного освещения используют только электрическое. В помещениях развешиваются огнетушители из расчета один огнетушитель на 40-50 $м^2$, но не менее двух на каждое отдельное помещение. Кроме того, устанавливаются пожарные краны со шлангами, а там, где нет водопровода - ящики с пакетами сухого песка. Все помещения архива оборудуются пожарной сигнализацией.

Архивохранилище оборудуется металлическими стеллажами. При использовании деревянных стеллажей они пропитываются специальным огнестойким и противогрибковым составами.

Стеллажи устанавливаются перпендикулярно стенам с окнами. При использовании стационарных стеллажей, их желательно размещать в простенках между окнами, чтобы лучи скользили вдоль полок, так как прямые солнечные лучи неблагоприятно влияют на документы. Если оконные проемы слишком широки, стеллажи располагают у противоположной стены (также торцами), а вдоль окон оставляется главный проход.

Стеллажи устанавливаются на расстоянии от стен, а нижняя полка поднимается на высоту 10—15 см от пола. Это делается для хорошей циркуляции воздуха, для того чтобы на стенах не появлялась сырость, и чтобы предохранить документы в случае затопления.

Для хранения документов могут использоваться передвижные стеллажи. Они монтируются на фальшпол с рельсовыми направляющими. Вся площадь архива занимается стеллажами, остается лишь один рабочий проход, местоположение которого может меняться благодаря перемещению стеллажей по направляющим пола. По сравнению с обычными шкафами передвижные стеллажи позволяют значительно увеличить вместимость архива при той же занимаемой площади (или уменьшить площадь, сохранив вместимость архива).

Как стационарные, так и передвижные стеллажи устанавливают в архивах с соблюдением норм. Проходы между стеллажами должны быть 75 см, расстояние между рядами (главный проход) — 120 см. Расстояние между наружной стеной здания и стеллажами, параллельными стене, — 75 см, расстояние между стеной и торцом стеллажа - 45 см. Расстояние между полом и нижней полкой стеллажа — не менее 15 см, а в цокольных этажах - не менее 30 см. Между потолком и верхним

краем папок или коробок должен оставаться зазор не менее 5 см для циркуляции воздуха.

Комплекс помещений архива, их состав, расположение, оборудование должны обеспечивать выполнение функциональных задач по приему на хранение, хранению, использованию документов и их специальной обработке.

Сохранность документов в архиве организации обеспечивается комплексом мероприятий по созданию нормативных условий, соблюдению нормативных режимов и надлежащей организации хранения документов, исключающих хищение и утрату и обеспечивающих поддержание в удовлетворительном физическом состоянии (Правила № 24 от 2 марта 2020 г.).

В комплекс работ по обеспечению сохранности документов архива организации в первую очередь включаются предоставление помещения для размещения архивных документов и обеспечение нормативных условий хранения документов.

Архив организации должен быть размещен в специально построенных или приспособленных для хранения документов зданиях или в отдельных помещениях здания. Не допускается размещение архива организации в подвальных и чердачных помещениях (Правила № 24 от 2 марта 2020 г.).

В архиве запрещено находится в верхней одежде, мокрой и грязной обуви, хранить посторонние предметы, оборудование, употреблять пищевые продукты.

Под обеспечением нормативных условий хранения документов понимаются.

1) **Оснащение архивохранилищ специальным оборудованием для хранения документов.**

Все поступающие в архив организации документы размещаются в архивохранилищах на стационарных и/или передвижных металлических стеллажах, в металлических шкафах или контейнерах. Стеллажи должны быть установлены

перпендикулярно стенам с оконными проемами, а в помещении без окон - с учетом особенностей помещения и оборудования. Не допускается размещение стеллажей вплотную к наружным стенам здания и к источникам тепла.

2) **Оборудование помещения архива организации средствами пожаротушения, охранной и пожарной сигнализацией и соблюдение противопожарного режима.**

Противопожарный режим в зданиях, где размещается архив организации, и в архивохранилищах устанавливается в соответствии с нормативными правовыми актами РФ в области пожарной безопасности.

3) **Соблюдение охранного режима.**

Охранный режим обеспечивается путем оборудования архивохранилищ, а также других помещений, где постоянно или временно хранятся архивные документы, средствами охраны, обеспечивающими контроль доступа в архивохранилище и помещения архива, и соблюдением порядка сдачи под охрану и снятия с охраны, установленного руководителем организации.

В случае выдачи архивных документов во временное пользование по запросам государственных органов, органов местного самоуправления и организаций вынос из здания архива или здания организации архивных документов разрешается только по специальным пропускам;

4) **Создание нормативных температурновлажностного, светового режимов, проведение санитарногигиенических мероприятий.**

Архивные документы следует хранить в темноте. Все виды работ с документами должны проводиться при ограниченных или технологически необходимых уровнях освещения.

Температура в помещении для хранения документов на бумажном носителе должна быть 17 - 19 °С, относительная влажность воздуха – 50 - 55%.

Защита документов от действия света обеспечивается хранением документов в коробках, папках и переплетах, в шкафах или на стеллажах закрытого типа.

Архивохранилище должно иметь естественную или искусственную вентиляцию, обеспечивающую рециркуляцию воздуха, стабильность температурно-влажностного режима, очистку воздуха от пыли и агрессивных примесей, а также отвечать современным требованиям компактности и экономичности.

Материалы покрытия стен, полов, потолков, внутренней арматуры архивохранилища, применяемые при изготовлении оборудования и средств хранения архивных документов, не должны выделять агрессивные химические вещества и быть источником пыли.

Помещения архива организации должны содержаться в чистоте, в условиях, исключающих возможность появления плесени, грызунов, насекомых, пыли. В помещениях архивохранилищ должна быть обеспечена свободная циркуляция воздуха, исключающая образование непроветриваемых зон, опасных в санитарно-биологическом отношении.

Список использованных источников и литературы

Нормативные правовые акты:

1. О Государственном гербе Российской Федерации: федеральный конституционный закон от 25 декабря 2000 г. № 2-ФКЗ (в редакции от 20.12.2017) – Доступ из Консультант Плюс, 2022 (дата обращения: 22.05.2022). - Текст : электронный.

2. Российская Федерация. Законы. Гражданский кодекс Российской Федерации (части первая, вторая, третья, четвертая). – Москва: Проспект, КноРус, 2021. –

544 с.–ISBN 978-5-392-25913-4 – Текст : непосредственный.

3. Трудовой кодекс Российской Федерации от 30 декабря 2001 г. № 197-ФЗ (в редакции ФЗ от 14.07.2022 № 349-ФЗ) – Доступ из Консультант Плюс, 2022 (дата обращения: 01.08.2022). - Текст : электронный.

4. Об обязательном экземпляре документов: федеральный закон от 29.12.1994 № 77-ФЗ (в редакции ФЗ от 01.05.2022 № 131-ФЗ) – Доступ из Консультант Плюс, 2022 (дата обращения: 01.08.2022). - Текст : электронный.

5. О коммерческой тайне: федеральный закон от 29.07.2004 № 98-ФЗ (в редакции ФЗ от 14.07.2022 № 311-ФЗ) – Доступ из Консультант Плюс, 2022 (дата обращения: 01.08.2022). - Текст : электронный.

6. О персональных данных: федеральный закон от 27.07.2006 № 152-ФЗ (в редакции ФЗ от 14.07.2022 № 266-ФЗ) – Доступ из Консультант Плюс, 2022 (дата обращения: 01.08.2022). - Текст : электронный.

7. Об информации, информационных технологиях и о защите информации: федеральный закон от 27.07.2006
№ 149-ФЗ (в редакции ФЗ от 14.07.2022 № 325-ФЗ) – Доступ из Консультант Плюс, 2022 (дата обращения: 01.08.2022). - Текст : электронный.

8. О языках народов Российской Федерации: закон Российской Федерации от 25.10.1991 № 1807-1 (в редакции ФЗ от 11.06.2021 № 182-ФЗ) – Доступ из

Консультант Плюс, 2022 (дата обращения: 01.08.2022). - Текст : электронный.

9. О государственном языке Российской Федерации: федеральный закон от 01.06.2005 № 53-ФЗ (в редакции ФЗ от 30.04.2021 № 117-ФЗ) – Доступ из Консультант Плюс, 2022 (дата обращения: 01.08.2021). - Текст : электронный.

10. О порядке рассмотрения обращений граждан Российской Федерации: федеральный закон от 2 мая 2006 г. № 59-ФЗ (в редакции ФЗ от 27.12.2018 № 528-ФЗ) – Доступ из Консультант Плюс, 2022 (дата обращения: 01.08.2022). - Текст : электронный.

11. Об архивном деле в Российской Федерации: федеральный закон от 22.10.2004 № 125-ФЗ (в редакции ФЗ 11.06.2021 № 170-ФЗ) – Доступ из Консультант Плюс, 2022 (дата обращения: 01.08.2022). - Текст : электронный.

12. Об электронной подписи: федеральный закон от 06.04.2011 № 63-ФЗ (в редакции ФЗ от 14.07.2022 № 339-ФЗ) – Доступ из Консультант Плюс, 2022 (дата обращения: 01.08.2022). - Текст : электронный.

13. Об упорядочении изготовления, использования, хранения и уничтожения печатей и бланков с воспроизведением Государственного герба Российской Федерации: Постановление Правительства РФ от 27 декабря 1995 г. № 1268 (в редакции от 17.03.2018) – Доступ из Консультант Плюс, 2022 (дата обращения: 01.08.2022). - Текст : электронный.

14. Об утверждении норм времени на работы по документационному обеспечению управленческих

структур федеральных органов исполнительной власти: Постановление Минтруда РФ от 26.03.2002 № 23 – Доступ из Консультант Плюс, 2022 (дата обращения: 01.08.2022). - Текст : электронный.

15. Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты: Постановление Госкомстата от 05.01.2004 № 1 – Доступ из Консультант Плюс, 2022 (дата обращения: 01.08.2022). - Текст : электронный.

16. Правила организации хранения, комплектования, учета и использования документов Архивного фонда Российской Федерации и других архивных документов в государственных и муниципальных архивах, музеях и библиотеках, научных организациях: Утверждены приказом Федерального архивного агентства от 2 марта 2020 г. № 24 – Доступ из Консультант Плюс, 2022 (дата обращения: 01.08.2022). - Текст : электронный.

17. Об утверждении формы, порядка ведения и хранения трудовых книжек: Приказ Министерства труда и социальной защиты РФ от 19 мая 2021 г. № 320н – Доступ из Консультант Плюс, 2022 (дата обращения: 01.08.2022). - Текст : электронный.

18. Правила оказания услуг почтовой связи: утв. Приказом Министерства связи и массовых коммуникаций Российской Федерации от 31 июля 2014 г. № 234 (в редакции от 19.11.2020) – Доступ из Консультант Плюс, 2022 (дата обращения: 01.08.2022). - Текст : электронный.

19. Инструкция по заполнению трудовых книжек: утв. Постановлением Минтруда России от 10 октября 2003 г. № 69 (в редакции от 31.10.2016) – Доступ из Консультант Плюс, 2022 (дата обращения: 01.08.2022). - Текст : электронный.

20. Перечень сведений конфиденциального характера: утвержден Указом Президента РФ от 6 марта 1997 г. № 188 (в редакции от 13.07.2015) – Доступ из Консультант Плюс, 2022 (дата обращения: 01.08.2022). - Текст : электронный.

21. ГОСТ Р 7.0.97-2016 «Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Организационно-распорядительная документация. Требования к оформлению документов»: Приказ Росстандарта от 08.12.2016 № 2004-ст (в редакции от 14.05.2018) – Доступ из Консультант Плюс, 2022 (дата обращения: 01.08.2022). - Текст : электронный.

22. ГОСТ Р 7.0.8-2013 «Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения»: Приказ Росстандарта от 17.10.2013 № 1185-ст – Доступ из Консультант Плюс, 2022 (дата обращения: 01.08.2022). - Текст : электронный.

23. Об утверждении Примерной инструкции по делопроизводству в государственных организациях: Приказ Росархива от 11.04.2018 № 44 – Доступ из Консультант Плюс, 2022 (дата обращения: 01.08.2022). - Текст : электронный.

Основные источники:

24. Басаков, М.И. Делопроизводство (документационное обеспечение управления): учебник / М.И. Басаков, О.И. Замыцкова. - Феникс, - Ростов-наДону. - 2015. - 376 с. – (Среднее профессиональное образование). – ISBN: 978-5-222-18877-4. – Текст : непосредственный.

25. Документоведение : учебник и практикум для среднего профессионального образования / под редакцией Л. А. Дорониной. — 2-е издание, переработанное и дополненное — Москва : Издательство Юрайт, 2019. — 309 с. — Серия: Профессиональное образование. — ISBN 978-5-53404330-3. — Текст : непосредственный.

26. Мантурова, Н.С. Кадровое делопроизводство и архивы документов по личному составу: учебнометодическое пособие для студентов, обучающихся по направлению подготовки 46.03.02 Документоведение и архивоведение / Н.С. Мантурова. — Электрон. текстовые данные. — Челябинск: Челябинский государственный институт культуры, 2018. — 140 c. — 978-5-94839-600-2. — Режим доступа: http://www.iprbookshop.ru/83609.html

27. Румынина, Л.А. Документационное обеспечение управления: учебник для студентов учреждений среднего профессионального образования \ Л.А. Румынина. – Мосвка: ТК Велби, Издательство

Проспект, 2012. – 208 с. – ISBN 978-5-7695-5205-2. – Текст : непосредственный.

Дополнительные источники:

28. Бялт, В. С. Документационное обеспечение управления. Юридическая техника : учебное пособие для среднего профессионального образования / В. С. Бялт. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2021. — 103 с. — (Профессиональное образование). — ISBN 978-5-53408233-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/474092 (дата обращения: 20.05.2022)

29. Грозова, О. С. Делопроизводство : учебное пособие для среднего профессионального образования / О. С. Грозова. — Москва : Издательство Юрайт, 2021. — 126 с. — (Профессиональное образование). — ISBN 9785-534-08211-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait (дата обращения: 28.05.2022).

30. Корнеев, И. К. Документационное обеспечение управления : учебник и практикум для среднего профессионального образования / И. К. Корнеев, А. В. Пшенко, В. А. Машурцев. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2021. — 384 с. — (Профессиональное образование). — ISBN 978-5-534-05022-6. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/472550 (дата обращения: 12.05.2022).

31. Кузнецов, И. Н. Документационное обеспечение управления персоналом : учебник и практикум для среднего профессионального образования / И. Н. Кузнецов. — Москва : Издательство Юрайт, 2022. — 521 с. — (Профессиональное образование). — ISBN 978-5-534-04451-5. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/444432 (дата обращения: 12.05.2022).

32. Ленкевич, Л.А. Секретарь-референт. Техника машинописи: учебное пособие / Л. А. Ленкевич.— Москва: Издетельский центр «Академия», 2010. — 64 с. – ISBN 978-5-0189-2356-3. – Текст : непосредственный.

33. Ленкевич, Л.А. Делопроизводство. Рабочая тетрадь: учебное пособие для начального профессионального образования / Л.А. Ленкевич. - Москва: Издательский центр «Академия», 2010. -96с. – ISBN 978-6-0148-2348-3. – Текст : непосредственный.

34. Ленкевич, Л.А. Делопроизводство: учебник для студентов учреждений среднего профессионального образования / Л.А. Ленкевич. – 5-е издание, стереотипное — Москва: Издательский центр «Академия», 2014. — 256 с. – ISBN 978-5-0278-0249-2. – Текст : непосредственный.

35. Шувалова, Н. Н. Документационное обеспечение управления : учебник и практикум для среднего профессионального образования / Н. Н. Шувалова. — 2-е изд. — Москва : Издательство Юрайт, 2022. — 265 с. — (Профессиональное образование). — ISBN 978-5-534-00088-7. — Текст :

электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/469832 (дата обращения: 12.05.2022)

36. Методические рекомендации по применению ГОСТ Р 7.0.97-2016 «Система стандартов по информации, библиотечному и издательскому делу. Организационно-распорядительная документация. Требования к оформлению документов»: Федеральное архивное агентство, ВНИИДАД, 2018 г. – Доступ из Консультант Плюс, 2022 (дата обращения: 15.04.2022). - Текст : электронный.

37. Унификация текстов управленческих документов. Методические рекомендации (утв. Главархивом СССР). – Доступ из Консультант Плюс, 2022 (дата обращения: 15.04.2022). - Текст : электронный.