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

КОНФИДЕНЦИАЛЬНОЕ ДЕЛОПРОИЗВОДСТВО

Учебное пособие

**Издательство
Нижневартовского
государственного
университета
2013**

ББК 60.844
К 65

Печатается по постановлению Редакционно-издательского совета
Нижневартовского государственного университета

Рецензент

к.п.н., доцент кафедры информационных технологий
АНО «Сибирский институт информационных технологий»
Ж.В.Каразеева

К 65 **Конфиденциальное делопроизводство:** Учебное пособие: / Сост. Е.А.Давыденко. — Нижневартовск: Изд-во Нижневарт. гос. ун-та, 2013. — 83 с.

ISBN 978–5–00047–082–4

Учебное пособие «Конфиденциальное делопроизводство» составлено в соответствии с требованиями к обязательному минимуму содержания и уровню подготовки государственного образовательного стандарта высшего профессионального образования третьего поколения по направлению «Документоведение и архивоведение».

Предназначено для студентов высших учебных заведений, обучающихся по направлению подготовки бакалавров «Документоведение и архивоведение».

ББК 60.844

ISBN 978–5–00047–082–4

ПРЕДИСЛОВИЕ

Приступая к изучению дисциплины «Конфиденциальное делопроизводство», следует четко представлять себе, что такое современная государственная и коммерческая организация, каковы ее управленческая структура и документационное обеспечение.

В том числе следует иметь представление о видах современного документооборота, как бумажного, так и электронного.

Общеизвестно, что в соответствии с федеральным законодательством информационные ресурсы разделены на категории доступа. Во-первых, это открытые (общедоступные) ресурсы, во-вторых, это ресурсы с ограниченным доступом. В условиях правового режима информация в свою очередь подразделяется на информацию, отнесенную к государственной тайне, и конфиденциальную.

В мире развивающихся информационных технологий, в условиях ценности информации («предупрежден — значит вооружен», «у каждой информации есть своя цена, но и у каждой цены — своя информации») интерес к дисциплине «Конфиденциальное делопроизводство» продиктован практической необходимостью.

В целом анализ нормативно-правовых актов Российской Федерации, общий порядок накопления и обработки документированной информации с ограниченным доступом, правила ее защиты и порядок доступа к ней определяются органами государственной власти, ответственными за определенные виды и массивы информации, в соответствии с их компетенцией либо непосредственно ее собственником в соответствии с законодательством.

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

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

Для освоения курса конфиденциального делопроизводства студенты используют знания, умения и навыки, сформированные в ходе изучения дисциплин «Гражданское право», «Документоведение», «Уголовное право», «Административное право» и т.д.

Процесс изучения дисциплины направлен на формирование следующих компетенций:

— осознание социальной значимости своей будущей профессии, мотивация к выполнению профессиональной деятельности (ОПК-1);

— владение основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией (ОК-10);

— способность анализировать социально значимые проблемы и процессы (ОК-13);

— способностью самостоятельно работать с различными источниками информации (ПК-13);

— способностью анализировать ценность документов с целью их хранения (ПК-17);

— способностью организовать работу службы документационного обеспечения управления и архивного дела (ПК-25);

— владение навыками работы с документами ограниченного доступа (ПК-32);

— владение методами защиты информации (ПК-40).

В результате изучения студент должен знать:

— правовую основу деятельности государственных и коммерческих организаций;

— нормативно-правовую основу организации конфиденциального делопроизводства;

— виды конфиденциальных документов;

— грифы секретности;

— основные мероприятия, проводимые в рамках безопасного документооборота в организации;

— способы защиты документов;

— способы хранения конфиденциальных документов;

— способы регистрации входящих и исходящих конфиденциальных документов;

уметь:

— проводить внутренний аудит конфиденциальных документов юридического лица;

— оформлять конфиденциальные документы;

— оформлять конфиденциальные документы на хранение;

— осуществлять операции с конфиденциальными документами;

владеть:

— навыками работы с электронными конфиденциальными документами;

— навыками работы с базами данных конфиденциального характера;

— навыками работы по проведению экспертизы ценности и идентификации документов.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

Учебное пособие по дисциплине «Конфиденциальное делопроизводство» подготовлено с целью организации самостоятельной работы студентов очной и заочной форм обучения, обучающихся по направлению «Документоведение и архивоведение».

Учебное пособие включает в себя введение, методические рекомендации, четыре главы, заключение, приложения, литературу.

Изложенный учебный материал рассматривается в соответствии с требованиями действующего законодательства, нормативными документами, поэтому курс связан с дисциплинами гражданского, трудового, информационного, административного права.

Материал в учебном пособии составлен таким образом, чтобы не дублировать лекционный курс и обратить внимание на самостоятельное изучение материала.

Цель — закрепление и углубление знаний, полученных в процессе самостоятельного изучения темы, умений работы с источниками (официальными документами, законами и т.д.).

Подготовку к самостоятельной работе необходимо начать с прочтения соответствующего материала в учебнике, рекомендованной литературы. Конспектирование не должно сводиться к механическому переписыванию. Прочитав текст учебника, дополнительного источника, необходимо обдумать его, выделить основные мысли и изложить своими словами или сокращенными формулировками автора, отмечая возникающие при этом вопросы.

После ознакомительного чтения рекомендованной литературы и учебника следует приступить к работе над дополнительными источниками, подобрать материал, необходимый для подтверждения теоретических и практических положений.

Особое внимание следует уделить подготовке выступлений на основе учебного пособия, составлению плана выступления, тезисов и др.

Глава 1

ДОКУМЕНТЫ ФЕДЕРАЛЬНОГО ЗНАЧЕНИЯ, РЕГЛАМЕНТИРУЮЩИЕ ДЕЯТЕЛЬНОСТЬ ЮРИДИЧЕСКОГО ЛИЦА И ИНДИВИДУАЛЬНОГО ПРЕДПРИНИМАТЕЛЯ

Все законодательные акты, принимаемые органами государственной власти Российской Федерации, оказывают влияние на документационное обеспечение управления организаций, в том числе коммерческих, поэтому целесообразно выделить наиболее важные из них, разделив их по силе действия.

К первой группе относятся нормативные правовые документы федерального значения, которые определяют правовую основу государственной регистрации юридических лиц в Российской Федерации[1], и Конституция Российской Федерации[2], являющаяся основным правовым актом, определяющим современную государственную политику и права граждан России в сфере информационно-документационного обмена.

Конституция РФ регулирует деятельность коммерческих организаций в части признания частной собственности (ст. 8) и обеспечивает право на свободное использование своих способностей и имущества для предпринимательской и иной не запрещенной законом экономической деятельности (ст. 34)[3].

Гражданский кодекс Российской Федерации (далее — ГК РФ), являясь основным документом гражданского законодательства, определяет правовое положение участников гражданского оборота, основания возникновения и порядок осуществления права собственности и других вещных прав, регулирует договорные и иные обязательства, а также другие имущественные и связанные

---

[1] Адаменко М.В. Как открыть свой бизнес. М., 2008. 320 с.

[2] Конституция Российской Федерации. Принята всенародным голосованием 12.12.1993 г. (с учетом поправок законов от 30.12.2008 г. № 6-ФКЗ и от 30.12.2008 г. № 7-ФКЗ) // Электронная правовая система. 2011. URL: http://base.consultant.ru (дата обращения 16.03.2011 г.).

[3] Там же. Ст. 8, 34.

с ними личные неимущественные отношения, основанные на равенстве, автономии воли и имущественной самостоятельности их участников (п. 1 ст. 2 ГК РФ)[4].

Однако отдельные вопросы (создание хозяйствующих субъектов различных форм собственности) в этой сфере могут быть урегулированы и другими нормативными правовыми актами.

Например, определение организации как юридического лица дает в ч. 1 п. 1 ст. 48 Гражданский Кодекс РФ. Юридическое лицо — организация, имеющая свою организационно-правовою форму (ООО, ЗАО, ОАО), а также «имеющая в собственности, хозяйственном ведении или оперативном управлении обособленное имущество. Юридическое лицо отвечает по своим обязательствам имуществом, может от своего имени приобретать и осуществлять имущественные и личные неимущественные права, нести обязанности, быть истцом и ответчиком в суде».

Помимо организации в гражданском обороте существует понятие «индивидуальный предприниматель» (ИП). Индивидуальным предпринимателем является физическое лицо, гражданин или не гражданин РФ, занимающийся самостоятельно определенным видом экономической деятельности и извлекающий от своей деятельности прибыль.

Еще одним значимым документом в деятельности юридического лица и предпринимателя является Федеральный закон от 08.08.2001 г. № 129-ФЗ «О государственной регистрации юридических лиц и индивидуальных предпринимателей»[5].

Настоящий закон регулирует отношения организации и предпринимателя, начиная от момента их создания, реорганизации, принудительной и добровольной ликвидации, в том числе регламентирует ведение единого государственного реестра юридических лиц и индивидуальных предпринимателей, а также внесение изменений в учредительные документы организации.

---

[4] Гражданский кодекс Российской Федерации (часть первая): от 30.11.1994 г. № 51-ФЗ (с послед. измен. на 07.02.2011 г. № 4-ФЗ) // Электронная правовая система. 2011. URL: http://base.consultant.ru (дата обращения 10.03.2011 г.).

[5] О государственной регистрации юридических лиц и индивидуальных предпринимателей: ФЗ РФ от 08.08.2001 г. № 129 // Электронная правовая система. 2011. URL: http://www.referent.ru (дата обращения 21.03.2011 г.).

В ст. 51 Гражданского кодекса РФ говорится, что организация как юридическое лицо считается созданной с момента ее государственной регистрации, то есть со дня внесения соответствующей записи в единый государственный реестр юридических лиц[6].

С момента регистрации у организации и индивидуального предпринимателя появляется правоспособность, возникают гражданские права и обязанности.

Государственным органом по государственной регистрации юридических лиц и индивидуальных предпринимателей является Федеральная налоговая служба. Налоговые органы субъектов Российской Федерации осуществляют свою деятельность на основании Постановления Правительства Российской Федерации от 30.09.2004 г. № 506 «Об утверждении Положения о Федеральной налоговой службе»[7].

Территориальные налоговые органы осуществляют регистрацию процедур реорганизации, ликвидации, а также внесения изменений в учредительные документы организации, внесения изменений, касающихся сведений о юридическом лице, ликвидации предпринимательской деятельности.

Все сведения об организации и предпринимателях отражены в единых реестрах, например, единый реестр юридических лиц регулируется Постановлением Правительства РФ от 19.06.2002 г. № 438[8].

Сведения о государственной регистрации организаций и предпринимателей являются открытыми, в том числе сведения о выданных им лицензиях и государственных сертификатах, учредителях, адресе местонахождения и т.д.

При регистрации изменений о деятельности, для оформления соответствующих документов, заверяемых нотариально, организация

---

[6] Гражданский кодекс Российской Федерации (часть первая): от 30.11.1994 г. № 51-ФЗ (с послед. измен. на 07.02.2011 г. № 4-ФЗ) // Электронная правовая система. 2011. URL: http://base.consultant.ru (дата обращения 10.03.2011 г.).

[7] Об утверждении Положения о Федеральной налоговой службе: Постановление Правительства РФ от 30.09.2004 г. № 506 // Электронная правовая система. 2011. URL: http://base.consultant.ru (дата обращения 04.03.2011 г.).

[8] О Едином государственном реестре юридических лиц: Постановление Правительства РФ от 19.06.2002 г. № 438 // Электронная правовая система. 2011. URL: http://base.consultant.ru (дата обращения 11.03.2012 г.).

и предприниматель заказывает в уполномоченном органе (налоговой службе) выписку из единого реестра юридических лиц или индивидуальных предпринимателей.

Для полного представления о данных процедурах можно руководствоваться Постановлением Правительства РФ от 26.02.2004 г. № 110 «О совершенствовании процедур государственной регистрации и постановки на учет юридических лиц и индивидуальных предпринимателей».

Регистрация организации, изменений в деятельности юридического лица и индивидуального предпринимателя осуществляется в течение 5 рабочих дней.

Основными подтверждающими документами о создании юридического лица являются: заверенный в налоговой службе устав и учредительный договор, свидетельство о государственной регистрации, выписка из единого реестра, идентификационный номер.

Основными подтверждающими документами о внесении изменений являются: свидетельство о регистрации внесенных изменений и обновленная выписка из единого реестра юридических лиц или индивидуальных предпринимателей.

Подаваемые в налоговую службу документы должны быть соответствующе оформлены. Унифицированные формы документов утверждены Постановлением Правительства РФ от 19.06.2002 г. № 439 «Об утверждении форм и требований к оформлению документов, используемых при государственной регистрации юридических лиц, а также физических лиц в качестве индивидуальных предпринимателей»[9].

Деятельность организации и индивидуального предпринимателя — это не только производство и оказание услуг, а еще и управленческая деятельность. В принципе каждый управленческий процесс, в том числе и производственный, должен быть документирован. В Российской Федерации система документационного обеспечения управления организации регламентируется следующими нормативно-методическими документами:

[9] Об утверждении форм и требований к оформлению документов, используемых при государственной регистрации юридических лиц, а также физических лиц в качестве индивидуальных предпринимателей: Постановление Правительства РФ от 19.06.2002 г. № 439 // Электронная правовая система. 2011. URL: http://ruspravo.org/list/31004/1.html (дата обращения 06.03.2011 г.).

— Государственный стандарт документационного обеспечения управления (ГСДОУ) включает в себя основные положения по вопросам документационного обеспечения управления.

Цель ГСДОУ — упорядочение документооборота, сокращение количества и повышение качества документов, создание условий для эффективного применения прогрессивных технических средств и технологий сбора, обработки и анализа информации, совершенствование работы аппарата управления[10].

— Общероссийский классификатор видов экономической деятельности (ОКВЭД)[11].

Наименование вида деятельности организации и индивидуального предпринимателя указывается в соответствии с ОКВЭД.

— Общероссийский классификатор видов экономической деятельности, продукции и услуг (ОКДП) входит в состав Единой системы классификации и кодирования технико-экономической и социальной информации (ЕСКК) Российской Федерации[12].

Классификатор состоит из четырех частей. Основная цель классификатора состоит в классифицировании основных экономических видов деятельности, их кодировании и обобщении. По основному виду экономической деятельности определяется налогообложение юридического лица и индивидуального предпринимателя.

Важными документами являются:

— ГОСТ Р 51141-98 «Делопроизводство и архивное дело. Термины и определения»[13];

— ГОСТ Р 6.30-2003 «Унифицированные системы документации. Унифицированная система организационно-распорядительной документации. Требования к оформлению документов»[14];

---

[10] Государственная система документационного обеспечения управления. Основные положения. Общие требования к документам и службам документационного обеспечения. М., 1991.

[11] Общероссийский классификатор видов экономической деятельности, продукции и услуг // Электронная правовая система. 2011. URL: http://base.consultant.ru (дата обращения 15.03.2011 г.).

[12] Там же.

[13] ГОСТ Р 51141-98. Делопроизводство и архивное дело. Термины и определения. М., 1998.

Общероссийский классификатор управленческой документации (ОКУД)[15].

Все нормативно-правовые и методические документы являются общедоступными. С ними можно ознакомиться как на официальных сайтах Правительства РФ, а так и в юридической литературе.

Таким образом, нормативно-правовое и нормативно-методическое регулирование деятельности организации и предпринимателя позволяет грамотно организовать производство товаров, услуг, а также правильно создать и оформить документы, придав им юридическую силу; организовать документооборот; обеспечить хранение и использование документов.

Вопросы и задания для самостоятельной работы

1. Дайте определение понятию «юридическое лицо».
2. В Гражданском кодексе РФ найдите, какие существуют организационно-правовые формы юридических лиц.
3. Дайте определение понятию «индивидуальный предприниматель».
4. В чем заключается разница между экономической деятельностью юридического лица и индивидуального предпринимателя?
5. Оформите необходимый пакет документов для регистрации предпринимателя и юридического лица.
6. Изучите Общероссийский классификатор экономических видов деятельности.
7. Выясните, какие виды деятельности подлежат обязательному лицензированию и сертификации.
8. Является ли выписка из единого реестра юридических лиц и индивидуальных предпринимателей конфиденциальным документом?

---

[14] ГОСТ Р 6.30-2003. Унифицированные системы документации. Унифицированная система организационно-распорядительной документации. Требования к оформлению документов. М., 2003.

[15] ОК 011-93. Общероссийский классификатор управленческой документации. Общие требования // Электронная правовая система. 2011. URL: http://base.consultant.ru (дата обращения 15.03.2011 г.).

9. В каком уполномоченном органе происходит регистрация создания и ликвидации юридического лица, а также индивидуального предпринимателя?

10. Проанализируйте типовой устав, учредительный договор общества с ограниченной ответственностью.

11. Проанализируйте типовой устав любого федерального и муниципального учреждения.

12. В чем заключается разница между различными организационно-правовыми формами юридических лиц?

Глава 2

ОРГАНИЗАЦИОННО-ПРАВОВЫЕ ДОКУМЕНТЫ ЮРИДИЧЕСКОГО ЛИЦА

Создание коммерческой организации начинается с собрания ее участников (учредителей) и выбора организационно-правовой формы юридического лица.

После того как выбор сделан, начинается этап разработки учредительных документов, являющихся правовой основой деятельности организации наряду с нормами действующего законодательства.

Состав учредительных документов для разных видов юридических лиц различен. Распространенным явлением считается, что общества с ограниченной ответственностью действуют на основе учредительного договора и устава. Если собственник (участник) один, то он может не оформлять учредительный договор, а остановиться лишь на оформлении решения о создании частной организации.

Гражданским кодексом РФ предусмотрено, что основой деятельности хозяйственных товариществ является учредительный договор. Для остальных организаций, в том числе и государственных, в качестве единственного учредительного документа предусмотрен устав. Исключения могут составлять некоммерческие организации, основным документом легитимности их деятельности может быть положение.

Учредительный договор юридического лица заключается и скрепляется подписями учредителей. В нем оговариваются основные моменты регулирования экономических и управленческих вопросов. Учредительный договор и его положения не могут противоречить уставу юридического лица. Устав утверждается его учредителями. Юридическое лицо, созданное одним учредителем, действует на основании утвержденного им устава.

На этапе разработки проектов учредительных документов происходит окончательное **комплектование состава учредителей организации, а также определение размера уставного**

(складочного) капитала (фонда) организации. В необходимых случаях может происходить денежная оценка вкладов учредителей в виде материальных ценностей, передачи имущественных прав и права пользования интеллектуальной собственностью на основании решения о выделении имущества и акта передачи его в пользование коммерческой организации.

Принятие решения о создании организации, утверждение или подписание учредительных документов, избрание руководящего состава и принятие решений по другим необходимым вопросам происходит, как правило, на учредительном собрании. Протокол учредительного собрания является документом, закрепляющим эти действия. В случае, когда учредителем организации является одно лицо, соответствующие вопросы оформляются решением учредителя.

На данном этапе также должно начаться формирование уставного капитала общества с ограниченной ответственностью, паевого фонда производственного кооператива, может быть сформирован складочный капитал товарищества. Так, учредители общества с ограниченной ответственностью обязаны оплатить не менее 50% уставного капитала на момент государственной регистрации общества. Оплата уставного капитала акционерного общества и уставного фонда государственных и муниципальных унитарных предприятий производится после их государственной регистрации.

Рассмотрим образец учредительного договора на наличие в нем сведений конфиденциального характера.

Учредительный договор о создании общества с ограниченной ответственностью «Визард»

г.Нижневартовск 08.08.2012 г.

Мы, Иванов Александр Борисович и Петров Василий Евгеньевич, далее именуемые «участники», на основании Гражданского кодекса РФ, ФЗ «Об обществах с ограниченной ответственностью» заключили настоящий договор о нижеследующем:

Статья 1. Предмет Договора.

1.1. Участники на основании объединения своих вкладов обязуются создать общество с ограниченной ответственнотью «Визард», далее по тексту «Общество».

1.2. Участники обязуются внести вклады в соответствии с условиями настоящего Договора и Устава Общества. Затраты по созданию Общества стороны несут пропорционально долям в уставном капитале.

Статья 2. Наименование и местонахождение Общества.

2.1. Полное наименование общество с ограниченной ответственностью «Визард». Сокращенное наименование ООО «Визард».

2.2. Местонахождение общества: 628617, Россия, Тюменская обл., ХМАО—Югра, г.Нижневартовск, ул. Нефтяников, 78, офис № 1.

2.3. Почтовый адрес общества: 628617, Россия, Тюменская обл., ХМАО—Югра, г.Нижневартовск, ул. Нефтяников, 78, офис № 1.

Статья 3. Цель создания и предмет деятельности.

3.1. Основной целью создания Общества является извлечение прибыли и распределение ее между участниками.

3.2. Предмет деятельности Общества определяется Уставом Общества.

Статья 4. Юридический статус Общества.

4.1. Общество обладает правами юридического лица с момента его государственной регистрации в установленном порядке, имеет расчетный и иные счета в учреждениях банков, печать и штамп со своим наименованием и указанием на место нахождения Общества, бланки установленного образца, товарный знак и знаки обслуживания.

4.2. Общество имеет в собственности обособленное имущество, учитываемое на его самостоятельном балансе, может от своего имени приобретать и осуществлять имущественные и личные неимущественные права, нести обязанности, быть истцом и ответчиком в суде и арбитраже.

4.3. Общество имеет гражданские права и несет гражданские обязанности, необходимые для осуществления любых видов

деятельности, не запрещенных федеральными законами, в соответствии с целью и предметом деятельности, указанными в Уставе Общества.

4.4. Общество несет ответственность по своим обязательствам всем принадлежащим ему имуществом.

4.5. Общество не отвечает по обязательствам своих участников.

4.6. Участники Общества не отвечают по его обязательствам и несут риск убытков, связанных с деятельностью Общества, в пределах стоимости внесенных ими вкладов.

Участники Общества, внесшие вклады в уставный капитал Общества не полностью, несут солидарную ответственность по его обязательствам в пределах стоимости неоплаченной части вклада каждого из участников Общества.

4.7. В случае несостоятельности (банкротства) Общества по вине его участников или по вине других лиц, которые имеют право давать обязательные для Общества указания либо иным образом имеют возможность определять его действия, на указанных участников или других лиц в случае недостаточности имущества Общества может быть возложена субсидиарная ответственность по его обязательствам.

4.8. Российская Федерация, субъекты Российской Федерации и муниципальные образования не несут ответственности по обязательствам Общества, равно как и Общество не несет ответственности по обязательствам Российской Федерации, субъектов Российской Федерации и муниципальных образований.

Статья 5. Уставный капитал Общества. Доли участников в уставном капитале. Вклады участников в уставный капитал.

5.1. Участники определяют уставный капитал Общества в размере 120 000 (ста двадцати тысяч) рублей.

5.2. Уставный капитал Общества разделен на доли.

Размеры долей участников составляют: Иванов Александр Борисович — 50% (60 тысяч рублей);

Петров Василий Евгеньевич — 50% (60 тысяч рублей).

5.3. Действительная стоимость доли участника Общества соответствует части стоимости чистых активов Общества, пропорциональной размеру его доли.

5.4. Участники Общества должны оплатить не менее 50% уставного капитала на момент регистрации Общества; в течение года деятельности Общества должно быть оплачено 100% уставного капитала.

5.5. В случае неполной оплаты уставного капитала Общества в течение года с момента его государственной регистрации Общество должно или объявить об уменьшении своего уставного капитала до фактически оплаченного его размера и зарегистрировать его уменьшение в установленном порядке, или принять решение о ликвидации Общества.

5.6. Вкладом в уставный капитал Общества могут быть деньги, ценные бумаги, другие вещи или имущественные права, либо иные права, имеющие денежную оценку.

Денежная оценка неденежных вкладов в уставный капитал Общества, вносимых участниками Общества и принимаемыми в Общество третьими лицами, утверждается решением общего собрания участников Общества, принимаемым всеми участниками Общества единогласно.

5.7. Не допускается освобождение участника Общества от обязанности внесения вклада в уставный капитал Общества, в том числе путем зачета требований к Обществу.

5.8. Общество выдает каждому участнику после внесения последним своего вклада в уставный капитал в полном объеме акт оценки вклада, подписанный всеми участниками и заверенный Обществом, подтверждающий право участника на долю в уставном капитале Общества. Копии актов, а также возобновление акта в случае его утери выдаются участникам за плату.

5.9. Доля участника Общества, который не внес в срок вклад в уставный капитал Общества в полном размере, переходит к Обществу. При этом Общество обязано выплатить участнику Общества действительную стоимость части его доли, пропорциональную внесенной им части вклада, или с согласия участника Общества выдать ему в натуре имущество такой же стоимости.

Статья 6. Права и обязанности участников Общества.

6.1. Участники Общества вправе:

— участвовать в управлении делами Общества в порядке, установленном действующим законодательством, а также учредительными документами Общества;

— получать информацию по всем вопросам, касающимся деятельности Общества; знакомиться с его бухгалтерскими книгами, иными документами Общества и имуществом, находящимся на балансе Общества;

— принимать участие в распределении прибыли от деятельности Общества;

— продавать или иным образом уступить свою долю в уставном капитале Общества либо ее часть одному или нескольким участникам Общества, самому Обществу либо третьим лицам в порядке, предусмотренном Уставом и настоящим Договором;

— в любое время выйти из Общества независимо от согласия других его участников;

— получить в случае ликвидации Общества часть имущества, оставшегося после расчетов с кредиторами, или его стоимость.

6.2. Дополнительные права:

6.2.1. Участники Общества пользуются преимущественным правом на выполнение заказов, полученных Обществом, а также на получение заказов Общества на выполнение работ и оказание услуг.

6.2.2. По решению общего собрания участников всем участникам или определенному участнику Общества могут быть предоставлены иные дополнительные права.

6.2.3. Дополнительные права, предоставленные определенному участнику Общества, в случае отчуждения его доли (части доли) к приобретателю доли (части доли) не переходят.

6.2.4. По решению общего собрания участников Общества дополнительные права участника (участников) Общества могут быть прекращены или ограничены.

6.3. Участники Общества обязаны:

— соблюдать положения Устава и настоящего Договора, выполнять решения общего собрания участников Общества;

— вносить вклады в порядке, в размерах, в составе и в сроки, которые предусмотрены законодательством и настоящим Договором;

— не разглашать конфиденциальную информацию о деятельности Общества;

— предоставлять Обществу информацию, необходимую для его успешной деятельности, и оказывать любое содействие Обществу в достижении его уставных целей;

— воздерживаться от действий, способных нанести моральный или материальный вред Обществу или его участникам.

6.4. Дополнительные обязанности:

6.4.1. В порядке, предусмотренном Уставом Общества, по решению общего собрания участников на всех участников или на определенного участника Общества могут быть возложены дополнительные обязанности.

6.4.2. Дополнительные обязанности, возложенные на определенного участника Общества, в случае отчуждения его доли (части доли) к приобретателю доли (части доли) не переходят.

6.4.3. Дополнительные обязанности могут быть прекращены по решению общего собрания участников Общества в порядке, предусмотренном Уставом Общества.

Статья 7. Распределение прибыли Общества между участниками Общества.

7.1. Общество вправе ежегодно принимать решение о распределении своей чистой прибыли между участниками Общества. Решение об определении части прибыли Общества, распределяемой между участниками Общества, принимается общим собранием участников Общества.

7.2. Часть прибыли Общества, предназначенная для распределения между его участниками, распределяется пропорционально их долям в уставном капитале Общества.

7.3. Выплаты части прибыли могут по решению общего собрания участников и при согласии участника производиться товарами и услугами, производимыми или приобретенными Обществом. Цены на такие товары и услуги должны быть одинаковыми для всех участников Общества.

7.4. Выплата участникам части прибыли производится не позднее одного месяца с момента принятия общим собранием участников соответствующего решения.

За просрочку указанных платежей Общество уплачивает участнику пеню в размере 0,1% просроченной суммы за каждый день просрочки, но не более 20% от всей предназначенной к выплате данному участнику части прибыли.

7.5. Общее собрание участников не вправе принимать решение о распределении прибыли Общества между участниками Общества:

— до полной оплаты всего уставного капитала Общества;

— до выплаты действительной стоимости доли (части доли) участника Общества в случаях, предусмотренных законодательством;

— если на момент принятия такого решения Общество отвечает признакам несостоятельности (банкротства) или если указанные признаки появятся у Общества в результате принятия такого решения;

— если на момент принятия такого решения стоимость чистых активов Общества меньше его уставного капитала и резервного фонда или станет меньше их размера в результате принятия такого решения;

— в иных случаях, предусмотренных законодательством.

7.6. Общество не вправе выплачивать участникам Общества прибыль, решение о распределении которой между участниками Общества принято:

— если на момент выплаты Общество отвечает признакам несостоятельности (банкротства) или если указанные признаки появятся у Общества в результате выплаты;

— если на момент выплаты стоимость чистых активов Общества меньше его уставного капитала и резервного фонда или станет меньше их размера в результате выплаты;

— в иных случаях, предусмотренных законодательством.

По прекращении указанных обстоятельств Общество обязано выплатить участникам Общества прибыль, решение о распределении которой между участниками Общества принято.

Статья 8. Органы Общества.

8.1. Высшим органом Общества является общее собрание участников, которое руководит деятельностью Общества в соответствии с Уставом Общества.

Компетентность, порядок работы и порядок принятия решений общего собрания определены Уставом Общества.

8.2. Руководство текущей деятельностью Общества осуществляется единоличным исполнительным органом Общества — генеральным директором Общества, который избирается общим собранием участников и действует на основании Устава Общества.

Компетентность генерального директора определена Уставом Общества.

8.3. Контроль за финансово-хозяйственной деятельностью Общества осуществляет ревизионная комиссия (ревизор).

Статья 9. Выход участника Общества из Общества.

9.1. Участник Общества вправе в любое время выйти из Общества независимо от согласия других его участников или Общества.

9.2. В случае выхода участника Общества из Общества его доля переходит к Обществу с момента подачи заявления о выходе из Общества. При этом Общество обязано в течение шести месяцев с момента окончания финансового года, в течение которого подано заявление о выходе из Общества, выплатить участнику Общества, подавшему заявление о выходе из Общества, действительную стоимость его доли, определяемую на основании данных бухгалтерской отчетности Общества за год, в течение которого было подано заявление о выходе из Общества, либо с согласия участника Общества выдать ему в натуре имущество такой же стоимости, а в случае неполной оплаты его вклада в уставный капитал Общества — действительную стоимость части его доли, пропорциональной оплаченной части вклада.

Выплата производится на банковский счет выходящего или, в случае выдачи имущества, по акту приема-передачи.

9.3. Действительная стоимость доли участника Общества выплачивается за счет разницы между стоимостью чистых активов Общества и размером уставного капитала Общества. В случае, если такой разницы недостаточно для выплаты выходящему участнику Общества действительной стоимости его доли, Общество обязано уменьшить свой уставный капитал на недостающую сумму.

Статья 10. Переход доли (части доли) участника к другим участникам, Обществу или третьим лицам.

10.1. Участник Общества вправе продать или иным образом уступить свою долю в уставном капитале Общества либо ее часть одному или нескольким участникам данного Общества. Согласие других участников Общества на совершение такой сделки не требуется.

10.2. Отчуждение доли участника (ее части) третьим лицам возможно только в случае согласия остальных участников Общества. Такое согласие считается полученным, если в течение тридцати дней с момента обращения к участникам Общества получено письменное согласие всех участников Общества или не получено письменного отказа в согласии ни от одного из участников Общества.

10.3. Участники Общества пользуются преимущественным правом покупки доли (части доли) участника Общества по цене предложения третьему лицу.

10.4. Если другие участники Общества не использовали свое преимущественное право покупки доли (части доли), преимущественное право покупки доли (части доли) имеет само Общество.

10.5. Участник Общества, намеренный продать свою долю (часть доли) третьему лицу, обязан письменно известить об этом остальных участников Общества и само Общество с указанием цены и других условий ее продажи.

В случае если участники общества и (или) Общество не воспользуются преимущественным правом покупки всей доли (всей части доли), предлагаемой для продажи, в течение месяца со дня такого извещения, доля (часть доли) может быть продана третьему лицу по цене и на условиях, сообщенных Обществу и его участникам.

10.6. Доля участника Общества может быть отчуждена до полной ее оплаты только в той части, в которой она уже оплачена.

10.7. Доли в уставном капитале Общества переходят к наследникам граждан и к правопреемникам юридических лиц, являвшихся участниками Общества, с согласия остальных участников Общества.

Отказ в согласии на переход доли влечет обязанность Общества выплатить наследникам (правопреемникам) участника ее

действительную стоимость или (с их согласия) выдать им в натуре имущество, соответствующее такой стоимости.

Статья 11. Реорганизация и ликвидация Общества.

Порядок реорганизации и ликвидации Общества определен Уставом Общества.

Статья 12. Уведомления.

12.1. Все уведомления Обществу или участнику, связанные с настоящим Договором, отправляются в письменной форме в адрес получателя.

12.2. Отправленное уведомление считается полученным и доведенным до сведения получателя в день его получения. Для телеграмм, факсимильных сообщений днем получения уведомления считается день отправления телеграммы, факсимильного сообщения.

12.3. В случае изменения адреса у любого из участника, этот участник должен сообщить об этом другим участникам.

Статья 13. Ответственность сторон.

13.1. В случае если какой-либо участник не исполняет или ненадлежащим образом исполняет свои обязанности, определенные в настоящем Договоре, то этот участник обязан возместить другим участникам убытки, нанесенные неисполнением или исполнением ненадлежащим образом своих обязательств.

13.2. Под убытками понимается прямой действительный ущерб. Возмещение недополученных доходов не производится.

Статья 14. Расторжение Договора.

Договор может быть расторгнут по взаимному согласию участников в согласованном ими порядке.

При ликвидации Общества настоящий Договор расторгается одновременно с ликвидацией.

Статья 15. Изменение Договора.

15.1. Изменения и дополнения к настоящему Договору оформляются письменно, подписываются надлежащим образом и регистрируются в установленном порядке.

15.2. Если какое-либо из положений Договора является или станет недействительным, то это не отменяет других положений.

Статья 16. Подписи сторон.

Таким образом, деятельность коммерческой организации в Российской Федерации регламентируется большим количеством нормативно-правовых документов как федерального, так и локального внутреннего значения. Все рассмотренные документы в первой главе являются важной частью при документировании деятельности коммерческой организации, на основании их происходит государственная регистрация, ведется финансовая деятельность, регулируются гражданско-правовые и трудовые отношения, регулируются документопотоки, выстраиваются отношения с органами государственной и муниципальной власти.

Любая проверка (выездная, камеральная, документарная) уполномоченными на то государственными органами, начинается с рассмотрения уставных документов. Поэтому учредительные документы должны четко отражать основные этапы управления, цели, задачи, основной вид экономической деятельности, вопросы финансирования организации.

Вопросы и задания для самостоятельной работы

1. Изучите предлагаемый в учебнике учредительный договор.
2. Найдите в учредительном договоре информацию, содержащую конфиденциальные сведения.
3. Является ли информация о долях в уставной капитал и уставном капитале организации конфиденциальной?
4. Являются ли персональные данные учредителей конфиденциальной информацией? Если да, то почему?
5. Назовите основные права учредителей на основании учредительного договора.
6. Назовите основные обязанности учредителей на основании учредительного договора.
7. Каков срок хранения учредительного договора?

Глава 3

ОРГАНИЗАЦИЯ КОНФИДЕНЦИАЛЬНОГО ДЕЛОПРОИЗВОДСТВА

3.1. Общие основы организации конфиденциального делопроизводства

Организации конфиденциального делопроизводства в деятельности современной организации и индивидуального предпринимателя уделяется большое значение, в первую очередь сохранности документов, информации финансового и производственного значения.

Ошибки в системе конфиденциального делопроизводства и нарушение режима сохранности информации приводят к ненужным экономическим издержкам, а зачастую к потере имиджа.

Составными частями делопроизводства в целом являются:

— делопроизводство на бумагоносителях;

— делопроизводство на электронных носителях;

— совмещение бумажного и электронного документооборота.

Как бы ни велико было стремление руководителей перевести весь документооборот в электронный вид, это не всегда удается сделать. Прежде всего потому, что, например, уполномоченные государственные органы на основании положения об организации проверок требуют предоставления документов в бумажном виде. Электронные реестры документов в части подобных проверок не имеют юридической силы.

Опыт работы делопроизводителей, а также нормативные документы говорят нам о том, что при ведении конфиденциального делопроизводства необходимо соблюдать следующие правила:

— четко определить перечень конфиденциальной информации;

— определить и регламентировать основные этапы присвоения и снятия грифа секретности (конфиденциальности) документов;

— определить круг лиц, ответственных за организацию конфиденциального делопроизводства;

— определить места хранения конфиденциальных документов на бумажных и электронных носителях;

— ввести в организации режим обязательной регистрации и учета всех конфиденциальных документов;

— передавать секретные сведения исполнителю под расписку;

— вести реестры выдачи конфиденциальных документов;

— вести контроль за использованием, печатей, штампов, бланков содержащих уникальные номера;

— не хранить пустые бланки с подписями и печатями;

— выделить конфиденциальное делопроизводство из обычного;

— разработать грифы секретности и их обозначения;

— создавать конфиденциальные документы в специальных помещениях, на отдельной технике. Прием и выдачу конфиденциальных документов производить через специальные окна;

— правильно уничтожать конфиденциальные документы по описи, в присутствии комиссии. Уничтожение конфиденциальных документов возможно посредством специальных машин (шредеров), а также посредством сжигания;

— к работе с конфиденциальными документами допускать лиц, заключивших договор о нераспространении государственной и коммерческой тайны, персональных сведений;

— хранить конфиденциальные документы в специальных железных шкафах;

— хранить конфиденциальные документы в архивах отдельно от обычных;

— включать в документы только минимально необходимую конфиденциальную информацию;

— рассылку конфиденциальных документов возможно осуществлять посредством курьера, она должна быть обоснованной и правильно передаваться из рук в руки;

— конфиденциальные документы должны быть четко систематизированы и классифицированы;

— отправку конфиденциальных документов производить только заказными или ценными письмами, по каналам специальной связи, например, посредством EMS почты России, или осуществлять доставку корреспонденции из числа сотрудников (курьерами), допущенных к работе с такими документами.

3.2. Этапы создания отдела конфиденциального делопроизводства

1 этап — создание специального подразделения, отвечающего за делопроизводство в организации или введение в штат должности, в чьи функциональные обязанности будет входить обеспечение делопроизводства организации;

2 этап — приобретение необходимого оборудования, принадлежностей для работы отдела конфиденциального делопроизводства, установка сейфов, шкафов, технического оборудования;

3 этап — создание и принятие необходимых локальных документов (инструкций, положений, договоров, должностных обязанностей и т.д.);

4 этап — знакомство с нормативными документами сотрудников в рамках их должностных обязанностей;

5 этап — создание особых механизмов административного контроля за соблюдением конфиденциального делопроизводства;

6 этап — создание и регламентация механизма персональной ответственности за нарушение правил конфиденциального делопроизводства.

Порядок создания конфиденциального бумажного делопроизводства:

1 этап — создание делопроизводства на бумагоносителях;

2 этап — определение перечня сведений конфиденциального характера;

3 этап — утверждение перечня сведений;

4 этап — определение правил ведения конфиденциального делопроизводства на основе общего делопроизводства на бумагоносителях;

5 этап — регламентация порядка допуска сотрудников к секретным сведениям;

6 этап — заключение договоров о нераспространении конфиденциальных сведений между сотрудниками, которые будут допущены к работе с конфиденциальной информацией и руководством организации;

7 этап — создание необходимой нормативно-правовой базы, регламентирующей конфиденциальное делопроизводство;

8 этап — доведение нормативных документов до сведения сотрудников;

9 этап — организация механизмов управленческого и технического контроля за сотрудниками, работающими с конфиденциальными документами;

10 этап — разъяснение основных моментов административной, уголовной и гражданско-правовой ответственности сотрудникам — носителям конфиденциальной информации, оформляющих секретные документы.

Делопроизводство в организации можно разделить на составные части.

Официальное делопроизводство, имеющее конфиденциальный характер:

— учредительные документы;

— финансовые документы и бухгалтерские документы;

— судебные и судебно-процессуальные документы;

— договоры и соглашения.

Конфиденциальное делопроизводство, связанное с текущей деятельностью:

внешнее делопроизводство:

— входящая конфиденциальная корреспонденция (на бумагоносителях);

— исходящая конфиденциальная корреспонденция (на бумагоносителях);

внутреннее делопроизводство:

— хранение конфиденциальных документов;

— хранение конфиденциальных документов в кабинетах у сотрудников;

— хранение конфиденциальных документов в отделе делопроизводства;

— создание конфиденциальных документов уполномоченным лицом;

— издание нормативных документов, регламентирующих конфиденциальное делопроизводство, руководством организации (приказы, распоряжения и т.д.);

— регистрация конфиденциального документа в секретариате или отделе конфиденциального делопроизводства;

— движение конфиденциального документа внутри организации; создание электронных реестров системы передачи конфиденциальных документов на бумажных и электронных носителях;

— размножение конфиденциальных документов и их копий;

— контроль за исполнением документов, имеющих конфиденциальный характер;

— создание архивов конфиденциальных документов;

— проведение экспертизы ценности конфиденциальных документов, а также установление сроков их хранения;

— определение порядка дальнейшего использования в работе конфиденциальных документов, определенных в архив;

— уничтожение конфиденциальных документов.

Перечень необходимых нормативных документов для функционирования конфиденциального делопроизводства

Нормативно-правовые документы организации с внесенными изменениями и дополнениями, связанными с сохранностью конфиденциальной информации:

— устав или положение об организации;

— учредительный договор;

— коллективный договор;

— правила внутреннего трудового распорядка;

— трудовой договор, контракт;

— договоры гражданско-правового характера, заключаемые с сотрудниками и подрядчиками;

— договоры и соглашения между руководством и сотрудником организации о работе с конфиденциальной информацией;

— инструкция по организации работы с конфиденциальной информацией.

Примерный план инструкции

— общие положения, цели, поставленные задачи;

— определение перечня информации и документов, содержащих конфиденциальную информацию со сроками их действий;

— основные этапы работы с конфиденциальными документами, обозначение конфиденциальных документов;

— грифы секретности;

— порядок сохранности папок и дел, содержащих конфиденциальную информацию;

— порядок допуска сотрудников к сведениям конфиденциального характера;

— контроль за выполнением требований режима сохранности конфиденциальной информации;

— обязанности сотрудников организации, работающих со сведениями, представляющими конфиденциальную информацию, и их ответственность за ее разглашение.

Инструкция по организации конфиденциального делопроизводства

Инструкция должна состоять из следующих разделов:

— общие положения, цели, задачи;

— правила оформления конфиденциальных документов;

— составление и оформление основных видов конфиденциальных документов;

— организация конфиденциального документооборота;

— учет движения и порядок обработки входящих конфиденциальных документов;

— учет движения и порядок обработки исходящих конфиденциальных документов;

— учет движения и порядок обработки внутренних конфиденциальных документов;

— регистрация конфиденциальных документов;

— контроль исполнения конфиденциальных документов;

— систематизация и классификация конфиденциальных документов;

— разработка номенклатуры конфиденциальных дел;

— формирование конфиденциальных дел в тома;

— подготовка и передача конфиденциальных документов к архивному хранению;

— экспертиза ценности конфиденциальных документов;

— описание конфиденциальных документов постоянного и временного сроков хранения;

— обеспечение сохранности конфиденциальных дел в кабинетах и архиве организации;

— передача конфиденциальных дел в архив;

— примерный перечень входящих конфиденциальных документов, не подлежащих регистрации;

— перечень документов, на которых ставится гриф конфиденциальности;

— перечень конфиденциальных документов, подлежащих утверждению и их унификация;

— перечень конфиденциальных документов, подлежащих согласованию на комиссии;

— форма регистрационно-контрольной карточки конфиденциальных дел;

— перечень конфиденциальных документов, подлежащих контролю, с указанием сроков их хранения;

— форма акта о выделении к уничтожению конфиденциальных документов с истекшими сроками хранения или их рассекречивание;

— форма внутренней описи конфиденциальных документов дела;

— форма описи дел, передаваемых на архивное хранение.

Инструкция по конфиденциальному делопроизводству, определяющая:

— порядок перемещения конфиденциальных документов на охраняемой территории;

— порядок работы с конфиденциальными документами вне служебных помещений;

— порядок изготовления и использования бланков организации, печатей и штампов;

— порядок использования бланков строгой отчетности (бланков организации, подготавливаемых за подписью первых лиц организации);

— порядок передачи конфиденциальных документов в случае ухода в отпуск, командировку или увольнение с работы;

— порядок подготовки конфиденциальных документов, его согласование, в том числе с юристами, финансистами, корректорами, а также порядок подписи конфиденциальных документов;

— порядок пересылки конфиденциальных документов вне контролируемых помещений.

Конфиденциальное электронное делопроизводство должно состоять из следующих взаимосвязанных систем:

— технические системы;

— комплексные системы защиты информации, в том числе системы электронного документооборота;

— автоматизированные системы электронного информационного хранилища, банки данных;

— совмещение конфиденциального электронного и бумажного документооборота;

— оснащение компьютерной техникой и программными средствами для оформления документов;

— создание архива электронных форм конфиденциальных документов;

— создание архива сканированных конфиденциальных документов;

— создание архива электронных документов с помощью:

— электронной почты;

— компьютерной сети;

— дисководов, флеш-памяти и т.д.;

— установление на компьютеры текстовых и графических редакторов;

— создание карточек регистрации электронных документов, а также электронных реестров.

Электронные карточки или реестры должны отображать:

— дату создания документа или его получения;

— дату исполнения документа;

— регистрационный номер;

— инициалы исполнителя и телефон;

— информацию о праве доступа;

— степень секретности или конфиденциальности;

— количество листов.

Программные средства должны:

— разделять папки документов по степени конфиденциальности;

— отображать систему получения и отправления электронных документов по корпоративной компьютерной сети;

— осуществлять систематизацию и классификацию документов;

— осуществлять контроль передвижения электронных документов по сети и систему ознакомления с электронными документами;

— осуществлять удобный поиск электронных документов по:

— реквизитам;

— названиям файлов;

— контексту документа;

— дате создания;

— срокам исполнения;

— по исполнителю;

— проводить анализ электронных конфиденциальных документов по:

— тематике;

— исполнителю;

— резолюциям и грифам конфиденциальности;

— дате создания (число, месяц, год).

Конфиденциальное электронно-информационное хранилище включает:

— электронную систему поступающих в хранилище документов различных видов и системы сортировки;

— систему сохранения документов в массивах хранилищ;

— систему отслеживания движения документов, выдаваемых сотрудникам, контроля и обеспечения их возврата;

— систему обеспечения поиска нужных документов в архивах по идентификационным признакам;

— систему фиксации выдачи документов сотрудникам, а также их возврат;

— систему обеспечения режима безопасного хранения документов.

Таким образом, система защиты конфиденциального электронного делопроизводства состоит из следующих блоков:

— блок технических и специальных программных средств;

— блок технической защиты;

— блок приемов и методов отбора персонала;

— блок организационных методов защиты электронного делопроизводства.

3.3. Особенности организации конфиденциального электронного документооборота (на примере электронного банка)

Электронный документ банка имеет важное отличие от привычного нам по повседневной жизни понятия бухгалтерский или банковский «документ». В традиционном «бумажном» документе форма неотрывна от содержания в том смысле, что будучи однажды напечатанным на бумаге, он в дальнейшем сохраняет свою форму и свое содержание в этом виде неизменными. Что касается электронных документов, то один и тот же документ может иметь представление, например, в виде сообщения системы межбанковских расчетов, первичного документа, внутреннего технического формата. Из этого обстоятельства вытекают важные особенности организации электронного документооборота (ЭДО), непосредственно определяющие решения, принимаемые при реализации. Сформулируем эти особенности в виде нескольких правил.

Первое правило: электронным документом (ЭД) следует считать его содержание независимо от формы.

На основе первого правила ЭДО можно сделать следующее заключение. Документ в файле и документ, импортированный в базу данных, если их содержание одинаково, — это один и тот же документ. Копий и экземпляров у ЭД не существует: сколько бы раз ни скопировали, ни трансформировали документ, он по-прежнему остается тем же самым, а не другим документом и не его копией. Это правило может вызывать неприятие и споры, но оно неплохо работает в конкретных технических решениях. Например, документы в формате XML, популярность которого в банковских и расчетных системах неуклонно растет, широко используют его. XML-документ в течение своего жизненного цикла может иметь разный состав тегов и их атрибутов, любую очередность следования атрибутов в тегах, различное представление

содержимого тегов, но, несмотря на все это, будет оставаться тем же самым документом[16].

Второе правило ЭДО: электронным документом является только значимое в текущем контексте содержание. Иными словами, ЭД в системе «клиент — банк» следует рассматривать как совокупность нескольких (многих) электронных документов, причем на разных этапах обработки следует иметь в виду какие-то определенные из этих «парциальных» ЭД, а не весь ЭД. Это правило критически важно именно в документообороте, когда ЭД последовательно проходит через многие этапы технологической цепочки. Например, в момент запуска операции по исходящему платежу поля документа, отражающие схему расчетов, еще пусты. Если подписать такой документ электронной цифровой подписью (ЭЦП) целиком, то на шаге позиционирования при заполнении этих полей подпись окажется нарушенной. Следовательно, надо ставить ЭЦП только на ту часть ЭД, которая имеет смысл в момент запуска операции, — фактически мы видим иной по содержанию ЭД, чем тот, который впоследствии выйдет из рук позиционера. При этом важна процедура принятия решения о подлинности документа в точках проверки ЭЦП: необходимо проверить ЭЦП всех «парциальных» документов, важных в данный момент. Возможно, что это будут не все ЭЦП, которыми подписан документ. Например, документ в момент его ввода в систему подписал операционист. Затем контролер проверил подпись операциониста и подписал документ свой подписью, а позиционер, определив схему расчетов, — своей. На выгрузке во внешнюю систему можно проверить только подписи контролера и позиционера. Подпись операциониста уже не важна: ее заменила подпись контролера, поскольку ею защищена та же самая часть документа[17].

Третье правило ЭДО банка тесно связано со вторым: в электронном документообороте необходимо закреплять ответственность за его участниками. ЭДО устроен таким образом, что лишь слаженный совместный труд всех его участников может привести

[16] См.: Кириев А., Ветров С. Электронный документооборот и ЭЦП в банковских системах // Финансовая газета. Региональный выпуск. 2006. № 17. Апрель. С. 76.

[17] См.: Там же. С. 80.

к успеху. ЭДО будет замечательно работать (и сейчас уже работает в системах, не поддерживающих внутренней ЭЦП) до тех пор, пока не возникнут какие-либо проблемы. Вот здесь-то как нельзя кстати окажется технология ЭЦП с ее уникальными способностями удостоверять целостность и авторство электронных документов. С ее помощью можно непосредственно в процессе обработки обнаружить искажение подписанного документа и, проведя расследование, выявить виновное лицо[18].

Четвертое правило: во внутреннем ЭДО банк может использовать предпочитаемые им средства ЭЦП, а во внешнем вынужден применять те, которые диктуются расчетными системами и корреспондентскими отношениями.

Пятое правило вытекает из всех предыдущих и является самым важным: каждый электронный документ должен быть защищен ЭЦП.

Если ЭД создается внутри системы, то сотрудник, ответственный за его формирование, обязан поставить собственную ЭЦП, и только при этом условии он поступает в последующую обработку. Если ЭД импортируется из внешней системы, то его заверяет ЭЦП сотрудника, ответственного за импорт. Если операция по созданию документа или его импорту выполняется автоматически, он должен удостоверяться ЭЦП назначенного сотрудника или специальной ЭЦП, формируемой особо защищенным автоматическим средством — сервером ЭЦП.

По документам, для которых действует правило «двух рук» (т.е. ответственность за правильность их ввода и обработки несут не менее двух сотрудников), должен производиться дополнительный контроль со стороны назначенного для этой цели должностного лица. В завершение процедуры документ заверяется ЭЦП контролера.

Все сказанное относится к каждому документу, имеющемуся в системе. Даже если это сейчас не так, и пятое правило пока не является отраслевой нормой банковского бизнеса, пройдет всего несколько лет, и никто не сможет объяснить, как АБС могли существовать без внутренней ЭЦП. Точно так же сейчас нам трудно понять, как это АБС могли работать без развитого ЭДО.

---

[18] См.: Там же. С. 82.

Список электронных документов, обрабатываемых в текущей версии Центр финансовых технологий (ЦФТ) «банк — клиент», включает более двух сотен позиций.

Расчетно-денежные документы (РДД) в данной системе призваны обеспечить проведение платежей, и этот их смысл находит свое отражение даже на системном уровне: большинство из таких документов в системе имеют в своей основе общую техническую сущность.

В системе обрабатываются следующие виды РДД:

— мемориальный ордер (в том числе мультивалютный и сводный);

— платеж и требование банка (в том числе мультивалютные);

— платежное поручение и требование клиента (в том числе мультивалютные);

— платежный ордер;

— входящий платеж;

— приходный и расходный кассовый ордер банка;

— чек, объявление на взнос наличными клиента;

— распоряжение на выполнение проводок;

— аккредитив;

— инкассовое поручение.

Списки и формы, позволяющие вводить, редактировать и обрабатывать РДД, доступны пользователям в подсистемах и в режимах, обусловленных технологией обработки документов определенного вида. Каждый РДД содержит множество разнообразных атрибутов с информацией о содержании документа, особенностях обработки, связях с другими сущностями и пр. Значения одних указываются в момент ввода документа в систему, другие же формируются в процессе его обработки. Из всего разнообразия атрибутов РДД выделяются несколько — их совокупность заключает в себе экономический смысл документа:

— сумма и валюта платежа;

— дата зачисления платежа на счет получателя;

— счет плательщика либо реквизиты, идентифицирующие плательщика и его банк (если платеж поступил по системе межбанковских расчетов);

— счет получателя либо реквизиты, идентифицирующие получателя и его банк (если платеж подлежит передаче по системе межбанковских расчетов);

— основание платежа;

— условия выполнения платежа.

Перечисленные атрибуты в той или иной форме присутствуют во всех видах РДД, благодаря чему в системе удалось организовать обработку документов на единых технологических решениях. Эти атрибуты, поскольку они являются наиболее желанным объектом потенциальной атаки злоумышленника, вошли в блок информации, защищаемой от искажения посредством внутренней ЭЦП.

Помимо перечня видов документов и их атрибутного состава следует также иметь в виду еще один аспект понятия «документ» — жизненный цикл. На его протяжении ЭД появляется в системе, проходит определенные технологией этапы обработки вплоть до окончательного исполнения.

Как известно, **электронный банк** — это интегрированная АБС, в которую входит множество в разной степени самостоятельных подсистем. Подсистемы взаимодействуют между собой. Раньше обычным способом такого взаимодействия было непосредственное выполнение подсистемами проводок в таблицах баз данных главной книги. С внедрением внутреннего ЭДО взаимодействие подсистем стало строиться на основе обмена подписанными документами с последующей их обработкой (после проверки ЭЦП) согласно логике и технологии, присущей подсистеме-получателю.

В контуре взаимодействующих подсистем электронный документ, пройдя жизненный цикл в одной подсистеме, попадает в другую для того, чтобы начать там новый цикл, определенный уже ее технологией.

Например, в практике расчетно-кассового обслуживания юридических лиц при недостатке средств на счете клиента для выполнения разового платежа начальный ЭД помещается в картотеку, и далее платеж реализуется на основании порождаемых системой документов частичной оплаты — по мере появления денег на счете плательщика. Порожденный документ является полноценным ЭД и претендует на свой собственный жизненный цикл.

Следует отметить, что не каждый ЭД обязательно проходит все этапы жизненного цикла, и само содержание этих этапов заметно отличается в разных ЭД. Все определяет вид документа и назначение подсистемы, в которой он обрабатывается.

Значительная часть жизненного цикла электронных документов проходит в рамках операции по их обработке посредством специального механизма. Все действия сведены в соответствующий справочник подсистемы «Главная книга бэк-офисов», который помогает технологу банка настраивать обработку ЭД согласно правилам, принятым в кредитном учреждении. В дистрибутиве поставляется полнофункциональный набор операций, основанный на требованиях Банка России и общепринятой банковской практике.

Этапы обработки документа в механизме операций называются шагами. Шаг обычно имеет три фазы, на которых выполняются действия над документом: до транзакции, собственно транзакция, после транзакции. В целом каждый шаг — это логически законченное элементарное действие по обработке документа.

Шаги объединяются в блоки — более крупные, обобщенные действия. Результатом выполнения каждого блока является присвоение документу статуса, описывающего его состояние. От значения этого статуса зависит дальнейшая судьба документа в операции.

Действия по подписанию и проверке ЭЦП документов — там, где это необходимо — привязываются к шагам операций. Выполняется это с помощью специального механизма прикладного применения криптографии (МППК). Технолог банка имеет возможность очень точно и тонко настраивать ЭДО в соответствии с политикой банка, поскольку настройка происходит на самом нижнем уровне организации операции — на шагах.

Функциональность, не использующая механизм операций, также охвачена применением ЭЦП. Например, транспорты подсистемы межбанковских расчетов позволяют подписывать и проверять ЭЦП отдельных документов, входящих в сообщения, самих сообщений и транспортных файлов, содержащих сообщения.

В системе реализовано такое понятие, как «блок целевой информации» (БЦИ). По сути, это набор данных, в который входят избранные и нужным образом преобразованные фрагменты

исходного документа, поэтому именно БЦИ, а не весь ЭД, подписывается ЭЦП. Проверка ЭЦП происходит соответственно: по содержанию документа снова формируется БЦИ и проверяется подпись не всего документа, а только этого БЦИ. Если в промежутке между этими этапами какой-либо из включенных в БЦИ фрагментов претерпит изменение, ЭЦП будет нарушена со всеми вытекающими последствиями: отвержение документа, разбирательство, принятие мер и пр.

БЦИ — это и есть «парциальный» ЭД на конкретном этапе обработки общего ЭД. Он отражает содержание общего ЭД, значимое для данного этапа, и ответственность за него закрепляется с помощью ЭЦП за сотрудником, осуществляющим данный этап обработки.

Следует отметить, что в Сбербанке РФ имеются средства для того, чтобы технолог легко сформировал любые необходимые в работе БЦИ. В настроенной системе пользователи могут даже не знать, с каким БЦИ они работают. На своем рабочем месте они видят только результаты проверок ЭЦП в виде экранных сообщений и подписывают документы своей ЭЦП, просто вставив дискету или предъявив электронный ключ.

Таким образом, в последнее время ЭДО с применением ЭЦП все глубже внедряется в различные процессы внутри АБС, причем не ограничиваясь только платежными документами. Например, в условиях централизованной АБС многофилиального банка можно реализовать построенную на основе ЭДО операцию по предоставлению новому сотруднику филиала прав доступа в систему, когда все этапы, от оформления заявки и ее утверждения руководителем до ввода прав доступа в действие, выполняются путем обмена и обработки электронных документов. Каждый этап обработки заявки начинается с проверки уже имеющихся в ней ЭЦП и завершается подписанием ее ЭЦП очередного ответственного лица.

В любом банке можно выделить большое количество разнообразных процедур, которые целесообразно выполнять именно в рамках ЭДО по описанному примеру. Совершенствование организации ЭДО и технологии применения ЭЦП в недалеком будущем позволит перевести на ЭДО все потребности банка.

Вопросы и задания для самостоятельной работы

1. Дайте определение конфиденциальному делопроизводству.
2. Дайте определение конфиденциальному электронному документообороту.
3. Назовите основные положения инструкции по организации конфиденциального документооборота.
4. Как выглядит электронный документооборот в системе современного банка.
5. Назовите нормативно-правовые документы, регулирующие конфиденциальное делопроизводство.
6. Что такое электронно-цифровая подпись?
7. Из чего состоит электронный ключ?
8. Каковы основные правила хранения конфиденциальной информации?
9. Из чего состоит электронное хранилище электронных конфиденциальных документов?

Глава 4

ПЕРСОНАЛЬНЫЕ ДАННЫЕ

4.1. Состав персональных данных работника

Персональные данные работника — это необходимая работодателю информация о конкретном сотруднике в связи с оформлением трудовых отношений и заключением трудового договора.

К персональным данным работника закон относит:

— фамилия, имя, отчество;

— год, месяц, дата и место рождения;

— данные о социальном, имущественном и семейном положении;

— данные об образовании работника, наличии званий, наград или специальной подготовки;

— данные о профессиях, специальностях работника;

— сведения о доходах, в некоторых случаях доходах семьи;

— данные медицинского характера, медицинская справка или медицинское заключение при особых условиях труда;

— данные о несовершеннолетних членах семьи;

— данные о месте жительства, почтовый адрес, телефон работника;

— идентификационный номер, свидетельство Пенсионного фонда;

— данные и документы воинского учета;

— иные персональные данные (при необходимости).

4.2. Обработка персональных данных работника

Обработка персональных данных работника — это в первую очередь получение, хранение, передача, использование персональных данных работника.

Обработка персональных данных работника осуществляется для обеспечения соблюдения инструкций и положений Пенсионного фонда РФ, Федерального фонда обязательного медицинского страхования, Фонда социального страхования.

Следует учитывать, что персональные данные используются для содействия работнику в трудоустройстве, продвижении по службе, обеспечения личной безопасности работника, контроля качества и количества выполняемой работы и обеспечения сохранности имущества, оплаты труда, пользования льготами, предусмотренными законодательством РФ и актами работодателя.

В Трудовом кодексе РФ и ФЗ «О персональных данных» закреплено, что работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни.

Работодатель не имеет права получать и обрабатывать персональные данные работника о его членстве в любых общественных объединениях или общественной и профсоюзной деятельности, информацию об участии работника в коммерческих организациях, за исключением случаев прохождения государственной службы по контракту.

Когда речь идет, например, о государственных служащих и заключении с ними государственного контракта, в соответствии со ст. 24 Конституции Российской Федерации работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

Работник обязан предоставлять работодателю достоверные сведения о себе и своевременно сообщать ему об изменении своих персональных данных.

Работодатель имеет право проверять достоверность сведений, предоставленных работником, сверяя данные, предоставленные работником, с имеющимися у работника документами.

Обработка персональных данных осуществляется в организации без письменного согласия работника, за исключением случаев, предусмотренных федеральным законом.

Все персональные данные о работнике работодатель может и должен получить от него самого.

Работодатель, в случае необходимости, может получить необходимые персональные данные работника у третьего лица, но для этого он должен уведомить работника и получить от него письменное согласие по установленной форме.

При принятии решений в какой-либо индивидуальной ситуации в организации работодатель не имеет права основываться

на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения.

Работодатель обязан сообщить работнику о целях, способах и источниках получения персональных данных, а также о характере подлежащих получению персональных данных и возможных последствиях отказа работника дать письменное согласие на их получение.

Персональные данные работника хранятся в отделе кадров в личном деле работника. Личные дела хранятся в бумажном виде в папках и находятся в сейфе или в несгораемом шкафу.

Персональные данные работника в отделе кадров хранятся также в электронном виде на локальной компьютерной сети. Доступ к электронным базам данных, содержащим персональные данные работников, обеспечиваются системой паролей. Пароли устанавливаются начальником отдела кадров и сообщаются индивидуально сотрудникам отдела кадров, имеющим доступ к персональным данным работников.

Хранение персональных данных работников в бухгалтерии и иных структурных подразделениях работодателя, сотрудники которых имеют право доступа к персональным данным, осуществляется в порядке, исключающем к ним доступ третьих лиц.

Сотрудник работодателя, имеющий доступ к персональным данным работников в связи с исполнением трудовых обязанностей, обеспечивает хранение информации, содержащей персональные данные работника, исключающее доступ к ним третьих лиц. В отсутствие сотрудника на его рабочем месте не должно быть документов, содержащих персональные данные работников (соблюдение «политики чистых столов»). При уходе в отпуск, служебной командировке и иных случаях длительного отсутствия работника на своем рабочем месте он обязан передать документы и иные носители, содержащие персональные данные работников, лицу, на которое локальным актом организации (приказом, распоряжением) будет возложено исполнение его трудовых обязанностей.

В случае если такое лицо не назначено, то документы и иные носители, содержащие персональные данные работников, передаются другому сотруднику, имеющему доступ к персональным

данным работников по указанию руководителя структурного подразделения.

При увольнении сотрудника, имеющего доступ к персональным данным работников, документы и иные носители, содержащие персональные данные работников, передаются другому сотруднику, имеющему доступ к персональным данным работников по указанию руководителя структурного подразделения.

Доступ к персональным данным работника имеют сотрудники работодателя, которым персональные данные необходимы в связи с исполнением ими трудовых обязанностей согласно перечню должностей.

В целях выполнения порученного задания и на основании служебной записки с положительной резолюцией руководителя организации доступ к персональным данным работника может быть предоставлен иному работнику, должность которого не включена в перечень должностей сотрудников, имеющих доступ к персональным данным работника организации, и которому они необходимы в связи с исполнением трудовых обязанностей.

В случае если работодателю оказывают услуги юридические и физические лица на основании заключенных договоров (либо иных оснований) и в силу данных договоров они должны иметь доступ к персональным данным работников организации, то соответствующие данные предоставляются работодателем только после подписания с ними соглашения о неразглашении конфиденциальной информации.

В исключительных случаях, исходя из договорных отношений с контрагентом, допускается наличие в договорах пунктов о неразглашении конфиденциальной информации, в том числе предусматривающих защиту персональных данных работника.

Процедура оформления доступа к персональным данным работника включает в себя:

— ознакомление работника под роспись с приказом.

При наличии иных нормативных актов (приказов, распоряжений, инструкций и т.п.), регулирующих обработку и защиту персональных данных работника, с данными актами также производится ознакомление работника под роспись;

— истребование с сотрудника (за исключением руководителя организации) письменного обязательства о соблюдении конфиденциальности персональных данных работника и соблюдении правил их обработки, подготовленного по установленной форме.

Сотрудники работодателя, имеющие доступ к персональным данным работников, имеют право получать только те персональные данные работника, которые необходимы им для выполнения конкретных трудовых функций. Доступ к персональным данным работников без специального разрешения имеют работники, занимающие в организации следующие должности:

— руководитель организации;

— заместитель руководителя организации;

— главный бухгалтер;

— работники отдела кадров;

— инженеры-программисты отдела информационных технологий;

— начальники структурных подразделений — в отношении персональных данных работников, числящихся в соответствующих структурных подразделениях.

Допуск к персональным данным работника других сотрудников работодателя, не имеющих надлежащим образом оформленного доступа, запрещается.

Работник имеет право на свободный доступ к своим персональным данным, включая право на получение копии любой записи (за исключением случаев, предусмотренных федеральным законом), содержащей его персональные данные. Работник имеет право вносить предложения по внесению изменений в свои данные в случае обнаружения в них неточностей.

Отдел кадров вправе передавать персональные данные работника в бухгалтерию и иные структурные подразделения в случае необходимости исполнения сотрудниками соответствующих структурных подразделений своих трудовых обязанностей.

При передаче персональных данных работника сотрудники отдела кадров предупреждают лиц, получающих данную информацию, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и истребуют от этих лиц письменное обязательство.

Передача (обмен и т.д.) персональных данных между подразделениями работодателя осуществляется только между сотрудниками, имеющими доступ к персональным данным работников.

Передача персональных данных работника третьим лицам осуществляется только с письменного согласия работника, которое оформляется по установленной форме и должно включать в себя:

— фамилию, имя, отчество, адрес работника, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

— наименование и адрес работодателя, получающего согласие работника;

— цель передачи персональных данных;

— перечень персональных данных, на передачу которых дает согласие работник;

— срок, в течение которого действует согласие, а также порядок его отзыва.

Согласия работника на передачу его персональных данных третьим лицам не требуется в случаях, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника; когда третьи лица оказывают услуги работодателю на основании заключенных договоров, а также в случаях, установленных федеральным законом.

Не допускается передача персональных данных работника в коммерческих целях без его письменного согласия.

Сотрудники работодателя, передающие персональные данные работников третьим лицам, должны передавать их с обязательным составлением акта приема-передачи документов (иных материальных носителей), содержащих персональные данные работников. Акт составляется по установленной форме:

— уведомление лица, получающего данные документы об обязанности использования полученной конфиденциальной информации лишь в целях, для которых она сообщена;

— предупреждение об ответственности за незаконное использование данной конфиденциальной информации в соответствии с федеральными законами.

Передача документов (иных материальных носителей), содержащих персональные данные работников, осуществляется при наличии у лица, уполномоченного на их получение:

— договора на оказание услуг организации;

— соглашения о неразглашении конфиденциальной информации либо наличие в договоре с третьим лицом пунктов о неразглашении конфиденциальной информации, в том числе предусматривающих защиту персональных данных работника;

— письма-запроса от третьего лица, которое должно включать в себя указание на основания получения доступа к запрашиваемой информации, содержащей персональные данные работника, ее перечень, цель использования, Ф.И.О. и должность лица, которому поручается получить данную информацию.

Ответственность за соблюдение вышеуказанного порядка предоставления персональных данных работника организации несет работник, а также руководитель структурного подразделения, осуществляющего передачу персональных данных работника третьим лицам.

Представителю работника (в том числе адвокату) персональные данные передаются в порядке, установленном действующим законодательством.

Информация передается при наличии одного из документов:

— нотариально заверенной доверенности представителя работника;

— письменного заявления работника, написанного в присутствии сотрудника отдела кадров работодателя (если заявление написано работником не в присутствии сотрудника отдела кадров, то оно должно быть нотариально заверено).

Доверенности и заявления хранятся в отделе кадров в личном деле работника.

Персональные данные работника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого работника, за исключением случаев, когда передача персональных данных работника без его согласия допускается действующим законодательством РФ.

Документы, содержащие персональные данные работника, могут быть отправлены через организацию федеральной почтовой связи. При этом должна быть обеспечена их конфиденциальность.

Документы, содержащие персональные данные, вкладываются в конверт, к нему прилагается сопроводительное письмо. На конверте делается надпись о том, что содержимое конверта является конфиденциальной информацией, и за незаконное ее разглашение законодательством предусмотрена ответственность. Далее, конверт с сопроводительным письмом вкладывается в другой конверт, на который наносятся только реквизиты, предусмотренные почтовыми правилами для заказных почтовых отправлений.

4.3. Организация защиты персональных данных работника

Защита персональных данных работника от неправомерного их использования или утраты обеспечивается работодателем.

Общую организацию защиты персональных данных работников осуществляет начальник отдела кадров.

Начальник отдела кадров обеспечивает ознакомление сотрудника с положением о защите конфиденциальных данных под роспись.

При наличии нормативных актов (приказов, распоряжений, инструкций и т.п.), регулирующих обработку и защиту персональных данных работника, с данными актами также производится ознакомление сотрудника под роспись.

Организацию и контроль за защитой персональных данных работников структурных подразделениях работодателя, сотрудники которых имеют доступ к персональным данным, осуществляют их непосредственные руководители.

Защите подлежит:

— информация о персональных данных работника;

— документы, содержащие персональные данные работника;

— персональные данные, содержащиеся на электронных носителях.

Защита сведений, хранящихся в электронных базах данных работодателя, от несанкционированного доступа, искажения и уничтожения информации, а также от иных неправомерных действий обеспечивается разграничением прав доступа с использованием учетной записи и системой паролей.

Права, обязанности, действия сотрудников, в трудовые обязанности которых входит обработка персональных данных работника, определяются также должностными инструкциями.

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут материальную, дисциплинарную, административную, гражданско-правовую или уголовную ответственность в порядке, установленном федеральными законами.

Разглашение персональных данных работника организации (передача их посторонним лицам, в том числе работникам организации, не имеющим к ним доступа), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные работника, а также иные нарушения обязанностей по их защите и обработке, установленных Положением о защите конфиденциальных данных, локальными нормативными актами (приказами, распоряжениями) организации, влечет наложение на сотрудника, имеющего доступ к персональным данным, дисциплинарного взыскания — замечания, выговора, увольнения.

Сотрудники, имеющие доступ к персональным данным работника и совершившие указанный дисциплинарный проступок, несут полную материальную ответственность в случае причинения его действиями ущерба работодателю (п. 7 ст. 243 Трудового кодекса РФ).

Сотрудники, имеющие доступ к персональным данным работника, виновные в незаконном разглашении или использовании персональных данных работников работодателя без согласия работников из корыстной или иной личной заинтересованности и причинившие крупный ущерб, несут уголовную ответственность в соответствии со ст. 183 Уголовного кодекса РФ.

Вопросы и задания для самостоятельной работы

1. Раскройте понятие «персональные данные».
2. Что законодатель относит к персональным данным?
3. Какими нормативно-правовыми актами регламентируется защита персональных данных?
4. Назовите основные этапы работы с персональными данными в организации.

5. Каковы правила сохранности персональных данных работника в организации?

6. Проведите подробный анализ ФЗ «О персональных данных».

7. Составьте перечень документов о приеме на работу сотрудника организации.

8. Разработайте инструкцию по работе с персональными данными в коммерческой организации.

9. Почему персональные данные сотрудника относятся к конфиденциальной информации?

ЗАКЛЮЧЕНИЕ

Анализ законодательных актов и деятельности организации приводит к выводу о том, что конфиденциальное делопроизводство по многим характеристикам схоже с обычным делопроизводством, но имеет особенности в плане работы с конфиденциальной информацией.

Конфиденциальное делопроизводство — это деятельность по защите, обработке и хранению конфиденциальной информации.

Конфиденциальное делопроизводство призвано охранять от ненужных посягательств производственную, управленческую финансовую, научную информацию.

Конфиденциальная информация оформляется на бланках бумажных и электронных документов, имеет реквизиты, дату создания и сведения об исполнителе.

Особое место в системе конфиденциального делопроизводства имеет конфиденциальный электронный документооборот, электронные ключи, электронно-цифровая подпись.

Неправомерные действия сотрудников организации, небрежное отношение к секретной информации и документам может повлечь полную или частичную их утрату, которая сопряжена с экономическими и моральными издержками организации.

Несанкционированные ознакомления с конфиденциальными документами приводят к утечке информации. В таких случаях велика вероятность получения конфиденциальной информации лицами, не работающими в организации, причастными к промышленному шпионажу, рейдерству.

Любое современное предприятие заинтересовано в хорошо организованной защите конфиденциальной информации и документационного оборота.

Таким образом, деятельность руководителя организации должна быть направлена на предотвращение потери, хищения, несанкционированного уничтожения, искажения, блокирования и разглашения информации.

ПРИЛОЖЕНИЯ

Приложение 1

Вопросы для самоконтроля

1. Принципы и основные этапы создания конфиденциального делопроизводства.
2. Порядок взаимодействия обычного и конфиденциального делопроизводства.
3. Общие признаки конфиденциального документа в бумажном и электронном виде.
4. Возможности, которыми должны обладать электронный конфиденциальный документооборот и электронное конфиденциальное информационное хранилище.
5. Порядок и основные этапы создания конфиденциального делопроизводства.
6. Способы и средства защиты конфиденциального делопроизводства на электронных и бумажных носителях.
7. Порядок применения средств криптографической защиты информации.
8. Понятие электронно-цифровой подписи.
9. Ознакомление сотрудников компании с правилами конфиденциального делопроизводства.
10. Автоматизированные системы конфиденциального информационного хранилища, конфиденциальные базы данных и их создание.
11. Назначение, принцип построения конфиденциальных баз данных.
12. Виды ответственности за нарушение режима защиты коммерческой и государственной тайны и правил ведения конфиденциального делопроизводства.
13. Локальные акты министерств и государственных органов в области защиты информации и работы с конфиденциальной документацией.

14. Разработка локальных актов коммерческих и некоммерческих предприятий в области защиты информации и работы с конфиденциальной документацией.

15. Унификация форм конфиденциальных документов.

16. Виды конфиденциальных документов, используемых в государственных органах.

17. Виды конфиденциальных документов, используемых коммерческими предприятиями.

18. Основные обозначения конфиденциальных документов.

19. Ответственность за разглашение конфиденциальной информации и потерю конфиденциальных данных и документов.

20. Взыскания в соответствии с трудовым законодательством.

21. Административная ответственность.

22. Уголовная ответственность.

23. Гражданско-правовая ответственность.

Методические рекомендации к подготовке практических и семинарских занятий

Практические занятия по дисциплине «Конфиденциальное делопроизводство» проводятся в форме докладов студентов по заранее известным им вопросам каждой темы и организации преподавателем обсуждения сделанного доклада.

На практические занятия выносятся темы, которые, как правило, не освещаются в лекциях и подлежат самостоятельному изучению. Время, отводимое на каждый доклад, — 7—10 минут.

В конце каждого занятия преподаватель подводит его итог: дает оценку сделанному докладу и сообщениям, дополняет и систематизирует высказанные мнения, концентрирует внимание студентов на основных моментах рассмотренной темы.

Разбор ошибок проходит коллективно или индивидуально. Занятие может проводиться в форме собеседования преподавателя со студентами по вопросам темы.

Студенты готовятся к практическим занятиям в период времени, отведенного на самостоятельную работу.

Студенты, пропустившие по какой-либо причине практическое занятие, обязаны его отработать в порядке, указанном преподавателем.

Содержание практических занятий по блокам

1. Законодательство об интеллектуальной собственности:

— понятие и виды интеллектуальной собственности;

— законодательство об авторском праве;

— законодательство о смежных правах;

— патентное законодательство;

— объекты патентного законодательства;

— законодательство о «ноу-хау»;

— международные правовые акты, регламентирующие вопросы конфиденциального делопроизводства;

— товарные знаки и знаки обслуживания;

— информация о происхождении товара;

— зарубежный опыт охраны интеллектуальной собственности.

2. Законодательство об информационной безопасности:

— правовые аспекты информационной безопасности;

— законодательство о безопасности и защите информации;

— правовые методы защиты в нормативных актах других отраслей законодательства;

— законодательство о защите государственной тайны;

— законодательство о защите коммерческой тайны и других негосударственных видов тайны;

— законодательство о защите персональных данных.

3. Аналитическая работа как основа формирования системы защиты информации:

— цель и общие задачи аналитической работы в сфере защиты информации;

— источники, угрозы, каналы распространения и утраты конфиденциальной информации;

— задачи аналитической работы по выявлению угроз и каналов утраты конфиденциальной информации;

— критерии целесообразности защиты информации;

— направления использования результатов аналитической работы для формирования системы защиты информации.

4. Разработка и ведение перечня сведений, составляющих предпринимательскую тайну:

— цель, задачи и направления классификации информационных ресурсов в предпринимательской сфере;

— критерии ценности, полезности и конфиденциальности информации;

— содержание процедуры разработки перечня ценных и конфиденциальных сведений;

— содержание процедуры ведения перечня ценных и конфиденциальных сведений;

— назначение и содержание перечня конфиденциальных документов фирмы.

5. Состав нормативно-методических материалов по регламентации системы защиты информации:

— организационные документы системы защиты информации;

— технологические документы системы защиты информации;

— регламентация системы защиты информации для условий экстремальных ситуаций;

— рекомендательные методические указания, правила, памятки и другие пособия для персонала.

Методические рекомендации по написанию реферата или эссе по дисциплине «Конфиденциальное делопроизводство»

Реферат является важной составной частью самостоятельной учебно-исследовательской работы студента и предназначен для углубленного изучения проблематики дисциплины, развития индивидуальных творческих способностей студента.

Задачами работы студента над рефератом или эссе являются:

— углубленное изучение выбранной темы;

— приобретение умения вести поиск необходимого фактического материала, его анализа и систематизации, формулирования научных выводов;

— приобретение навыков грамотного и логически доказательного изложения текста, правильности оформления работы и приложений.

Работа над эссе, рефератом формирует у студентов умение вести анализ, сравнивать мнения авторов, делать выводы, формулировать свою точку зрения.

Реферат, эссе представляет собой исследование по отдельной теме (вопросу) дисциплины, отражает одну некрупную проблему и пишется, как правило, на основе опубликованных источников и научной литературы.

Одновременно реферат может содержать анализ имеющихся в распоряжении студента нормативных, лекционных и других материалов, их творческое обобщение и систематизацию.

В реферате, эссе могут использоваться материалы, полученные в период учебно-исследовательской практики, экскурсий, посещения научных конференции и семинаров.

Результатом работы студента над темой реферата может быть составление определенной схемы, таблицы, графика, формулы или расчета.

Для написания реферата студентом используется время, отводимое на самостоятельную работу. Самостоятельная работа студента включает: работу в библиотеке, работу в архиве или Интернете, поиск необходимой информации в информационных центрах и информационных сетях учреждений, организаций и предприятий, получение консультаций у преподавателя.

Результаты самостоятельной работы студентом документируются, они должны быть представлены в виде картотек, записей, базы данных.

В течение недели студент должен выбрать или сформулировать интересующую его тему, согласовать ее с преподавателем. Студент имеет право предложить для разработки тему, не вошедшую в примерную тематику.

Научным руководителем студента при написании реферета является преподаватель, ведущий практические занятия по дисциплине «Конфиденциальное делопроизводство»

Рефераты оцениваются научным руководителем с учетом правильности и полноты исследования темы, доли творческого вклада студента в раскрытие темы, стиля изложения и качества оформления работы. Научный руководитель имеет право вернуть реферат студенту для доработки. Реферат защищается студентом в процессе экзамена. Студенты, не предоставившие научному

руководителю готовый реферат, к сдаче экзамена по дисциплине не допускаются.

Оценка за реферат учитывается в числе других показателей текущего контроля при определении итоговой (экзаменационной) оценки по дисциплине.

Примерная тематика рефератов

1. Предпринимательская тайна.
2. Корпоративная культура и информационная безопасность.
3. Адвокатская тайна.
4. Экономическая безопасность предпринимательской деятельности.
5. Профессиональная тайна нотариусов.
6. Врачебная тайна.
7. Государственная тайна.
8. Ноу-хау.
9. Нормативно-правовая база конфиденциального делопроизводства.
10. Информационная безопасность в организации.

Приложение 2

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (информация об изменениях)

С изменениями и дополнениями от:
27 июля 2010 г., 6 апреля, 21 июля 2011 г., 28 июля 2012 г.

Принят Государственной думой 8 июля 2006 г.
Одобрен Советом Федерации 14 июля 2006 г.

Статья 1. Сфера действия настоящего Федерального закона.

1. Настоящий Федеральный закон регулирует отношения, возникающие при:

1) осуществлении права на поиск, получение, передачу, производство и распространение информации;

2) применении информационных технологий;

3) обеспечении защиты информации.

2. Положения настоящего Федерального закона не распространяются на отношения, возникающие при правовой охране результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации.

Статья 2. Основные понятия, используемые в настоящем Федеральном законе.

В настоящем Федеральном законе используются следующие основные понятия:

1) информация — сведения (сообщения, данные) независимо от формы их представления;

2) информационные технологии — процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

3) информационная система — совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

4) информационно-телекоммуникационная сеть — технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

5) обладатель информации — лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

6) доступ к информации — возможность получения информации и ее использования;

7) конфиденциальность информации — обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

8) предоставление информации — действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

9) распространение информации — действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

10) электронное сообщение — информация, переданная или полученная пользователем информационно-телекоммуникационной сети;

11) документированная информация — зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;

Информация об изменениях: Федеральным законом от 27 июля 2010 г. № 227-ФЗ статья 2 настоящего Федерального закона дополнена пунктом 11.1, вступающим в силу с 1 января 2011 г.

11.1) электронный документ — документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах;

12) оператор информационной системы — гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных;

Информация об изменениях: Федеральным законом от 28 июля 2012 г. № 139-ФЗ статья 2 настоящего Федерального закона дополнена пунктом 13, вступающим в силу с 1 ноября 2012 г.

13) сайт в сети «Интернет» — совокупность программ для электронных вычислительных машин и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается через сеть «Интернет» по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в сети «Интернет»;

Информация об изменениях: Федеральным законом от 28 июля 2012 г. № 139-ФЗ статья 2 настоящего Федерального закона дополнена пунктом 14, вступающим в силу с 1 ноября 2012 г.

14) страница сайта в сети «Интернет» (далее также — интернет-страница) — часть сайта в сети «Интернет», доступ к которой осуществляется по указателю, состоящему из доменного имени и символов, определенных владельцем сайта в сети «Интернет»;

Информация об изменениях: Федеральным законом от 28 июля 2012 г. № 139-ФЗ статья 2 настоящего Федерального закона дополнена пунктом 15, вступающим в силу с 1 ноября 2012 г.

15) доменное имя — обозначение символами, предназначенное для адресации сайтов в сети «Интернет» в целях обеспечения доступа к информации, размещенной в сети «Интернет»;

Информация об изменениях: Федеральным законом от 28 июля 2012 г. № 139-ФЗ статья 2 настоящего Федерального закона дополнена пунктом 16, вступающим в силу с 1 ноября 2012 г.

16) сетевой адрес — идентификатор в сети передачи данных, определяющий при оказании телематических услуг связи абонентский терминал или иные средства связи, входящие в информационную систему;

Информация об изменениях: Федеральным законом от 28 июля 2012 г. № 139-ФЗ статья 2 настоящего Федерального закона дополнена пунктом 17, вступающим в силу с 1 ноября 2012 г.

17) владелец сайта в сети «Интернет» — лицо, самостоятельно и по своему усмотрению определяющее порядок использования

сайта в сети «Интернет», в том числе порядок размещения информации на таком сайте;

Информация об изменениях: Федеральным законом от 28 июля 2012 г. № 139-ФЗ статья 2 настоящего Федерального закона дополнена пунктом 18, вступающим в силу с 1 ноября 2012 г.

18) провайдер хостинга — лицо, оказывающее услуги по предоставлению вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к сети «Интернет».

Статья 3. Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации.

Правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации, основывается на следующих принципах:

1) свобода поиска, получения, передачи, производства и распространения информации любым законным способом;

2) установление ограничений доступа к информации только федеральными законами;

3) открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;

4) равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;

5) обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;

6) достоверность информации и своевременность ее предоставления;

7) неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;

8) недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для

создания и эксплуатации государственных информационных систем не установлена федеральными законами.

Статья 4. Законодательство Российской Федерации об информации, информационных технологиях и о защите информации.

1. Законодательство Российской Федерации об информации, информационных технологиях и о защите информации основывается на Конституции Российской Федерации, международных договорах Российской Федерации и состоит из настоящего Федерального закона и других регулирующих отношения по использованию информации федеральных законов.

2. Правовое регулирование отношений, связанных с организацией и деятельностью средств массовой информации, осуществляется в соответствии с законодательством Российской Федерации о средствах массовой информации.

3. Порядок хранения и использования включенной в состав архивных фондов документированной информации устанавливается законодательством об архивном деле в Российской Федерации.

Статья 5. Информация как объект правовых отношений.

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:

1) информацию, свободно распространяемую;

2) информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;

3) информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;

4) информацию, распространение которой в Российской Федерации ограничивается или запрещается.

4. Законодательством Российской Федерации могут быть установлены виды информации в зависимости от ее содержания или обладателя.

Статья 6. Обладатель информации.

1. Обладателем информации может быть гражданин (физическое лицо), юридическое лицо, Российская Федерация, субъект Российской Федерации, муниципальное образование.

2. От имени Российской Федерации, субъекта Российской Федерации, муниципального образования правомочия обладателя информации осуществляются соответственно государственными органами и органами местного самоуправления в пределах их полномочий, установленных соответствующими нормативными правовыми актами.

3. Обладатель информации, если иное не предусмотрено федеральными законами, вправе:

1) разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;

2) использовать информацию, в том числе распространять ее, по своему усмотрению;

3) передавать информацию другим лицам по договору или на ином установленном законом основании;

4) защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;

5) осуществлять иные действия с информацией или разрешать осуществление таких действий.

4. Обладатель информации при осуществлении своих прав обязан:

1) соблюдать права и законные интересы иных лиц;

2) принимать меры по защите информации;

3) ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

Статья 7. Общедоступная информация.

1. К общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен.

2. Общедоступная информация может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации.

3. Обладатель информации, ставшей общедоступной по его решению, вправе требовать от лиц, распространяющих такую информацию, указывать себя в качестве источника такой информации.

Статья 8. Право на доступ к информации.

1. Граждане (физические лица) и организации (юридические лица) (далее — организации) вправе осуществлять поиск и получение любой информации в любых формах и из любых источников при условии соблюдения требований, установленных настоящим Федеральным законом и другими федеральными законами.

2. Гражданин (физическое лицо) имеет право на получение от государственных органов, органов местного самоуправления, их должностных лиц в порядке, установленном законодательством Российской Федерации, информации, непосредственно затрагивающей его права и свободы.

3. Организация имеет право на получение от государственных органов, органов местного самоуправления информации, непосредственно касающейся прав и обязанностей этой организации, а также информации, необходимой в связи с взаимодействием с указанными органами при осуществлении этой организацией своей уставной деятельности.

4. Не может быть ограничен доступ к:

1) нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления;

2) информации о состоянии окружающей среды;

3) информации о деятельности государственных органов и органов местного самоуправления, а также об использовании

бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну);

4) информации, накапливаемой в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией;

5) иной информации, недопустимость ограничения доступа к которой установлена федеральными законами.

Информация об изменениях: Федеральным законом от 27 июля 2010 г. № 227-ФЗ в часть 5 статьи 8 настоящего Федерального закона внесены изменения, вступающие в силу с 1 января 2011 г.

См. текст части в предыдущей редакции.

5. Государственные органы и органы местного самоуправления обязаны обеспечивать доступ, в том числе с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет», к информации о своей деятельности на русском языке и государственном языке соответствующей республики в составе Российской Федерации в соответствии с федеральными законами, законами субъектов Российской Федерации и нормативными правовыми актами органов местного самоуправления. Лицо, желающее получить доступ к такой информации, не обязано обосновывать необходимость ее получения.

6. Решения и действия (бездействие) государственных органов и органов местного самоуправления, общественных объединений, должностных лиц, нарушающие право на доступ к информации, могут быть обжалованы в вышестоящий орган или вышестоящему должностному лицу либо в суд.

7. В случае, если в результате неправомерного отказа в доступе к информации, несвоевременного ее предоставления, предоставления заведомо недостоверной или не соответствующей содержанию запроса информации были причинены убытки, такие убытки подлежат возмещению в соответствии с гражданским законодательством.

8. Предоставляется бесплатно информация:

1) о деятельности государственных органов и органов местного самоуправления, размещенная такими органами в информационно-телекоммуникационных сетях;

2) затрагивающая права и установленные законодательством Российской Федерации обязанности заинтересованного лица;

3) иная установленная законом информация.

9. Установление платы за предоставление государственным органом или органом местного самоуправления информации о своей деятельности возможно только в случаях и на условиях, которые установлены федеральными законами.

Статья 9. Ограничение доступа к информации.

1. Ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

2. Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.

3. Защита информации, составляющей государственную тайну, осуществляется в соответствии с законодательством Российской Федерации о государственной тайне.

4. Федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение.

5. Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации.

6. Информация, составляющая профессиональную тайну, может быть предоставлена третьим лицам в соответствии с федеральными законами и (или) по решению суда.

7. Срок исполнения обязанностей по соблюдению конфиденциальности информации, составляющей профессиональную тайну, может быть ограничен только с согласия гражданина (физического лица), предоставившего такую информацию о себе.

8. Запрещается требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе

информации, составляющей личную или семейную тайну, и получать такую информацию помимо воли гражданина (физического лица), если иное не предусмотрено федеральными законами.

9. Порядок доступа к персональным данным граждан (физических лиц) устанавливается федеральным законом о персональных данных.

Статья 10. Распространение информации или предоставление информации.

1. В Российской Федерации распространение информации осуществляется свободно при соблюдении требований, установленных законодательством Российской Федерации.

2. Информация, распространяемая без использования средств массовой информации, должна включать в себя достоверные сведения о ее обладателе или об ином лице, распространяющем информацию, в форме и в объеме, которые достаточны для идентификации такого лица.

3. При использовании для распространения информации средств, позволяющих определять получателей информации, в том числе почтовых отправлений и электронных сообщений, лицо, распространяющее информацию, обязано обеспечить получателю информации возможность отказа от такой информации.

4. Предоставление информации осуществляется в порядке, который устанавливается соглашением лиц, участвующих в обмене информацией.

5. Случаи и условия обязательного распространения информации или предоставления информации, в том числе предоставление обязательных экземпляров документов, устанавливаются федеральными законами.

6. Запрещается распространение информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность.

Статья 11. Документирование информации.

1. Законодательством Российской Федерации или соглашением сторон могут быть установлены требования к документированию информации.

2. В федеральных органах исполнительной власти документирование информации осуществляется в порядке, устанавливаемом Правительством Российской Федерации. Правила делопроизводства и документооборота, установленные иными государственными органами, органами местного самоуправления в пределах их компетенции, должны соответствовать требованиям, установленным Правительством Российской Федерации в части делопроизводства и документооборота для федеральных органов исполнительной власти.

3. Утратила силу.

Информация об изменениях: См. текст части 3 статьи 11.

Федеральным законом от 6 апреля 2011 г. № 65-ФЗ в часть 4 статьи 11 настоящего Федерального закона внесены изменения.

См. текст части в предыдущей редакции.

4. В целях заключения гражданско-правовых договоров или оформления иных правоотношений, в которых участвуют лица, обменивающиеся электронными сообщениями, обмен электронными сообщениями, каждое из которых подписано электронной подписью или иным аналогом собственноручной подписи отправителя такого сообщения, в порядке, установленном федеральными законами, иными нормативными правовыми актами или соглашением сторон, рассматривается как обмен документами.

5. Право собственности и иные вещные права на материальные носители, содержащие документированную информацию, устанавливаются гражданским законодательством.

Статья 12. Государственное регулирование в сфере применения информационных технологий.

1. Государственное регулирование в сфере применения информационных технологий предусматривает:

1) регулирование отношений, связанных с поиском, получением, передачей, производством и распространением информации с применением информационных технологий (информатизации),

на основании принципов, установленных настоящим Федеральным законом;

2) развитие информационных систем различного назначения для обеспечения граждан (физических лиц), организаций, государственных органов и органов местного самоуправления информацией, а также обеспечение взаимодействия таких систем;

3) создание условий для эффективного использования в Российской Федерации информационно-телекоммуникационных сетей, в том числе сети «Интернет» и иных подобных информационно-телекоммуникационных сетей;

Информация об изменениях: Федеральным законом от 21 июля 2011 г. № 252-ФЗ часть 1 статьи 12 настоящего Федерального закона дополнена пунктом 4, вступающим в силу с 1 сентября 2012 г.

4) обеспечение информационной безопасности детей.

2. Государственные органы, органы местного самоуправления в соответствии со своими полномочиями:

1) участвуют в разработке и реализации целевых программ применения информационных технологий;

2) создают информационные системы и обеспечивают доступ к содержащейся в них информации на русском языке и государственном языке соответствующей республики в составе Российской Федерации.

Статья 13. Информационные системы.

1. Информационные системы включают в себя:

1) государственные информационные системы — федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов;

2) муниципальные информационные системы, созданные на основании решения органа местного самоуправления;

3) иные информационные системы.

2. Если иное не установлено федеральными законами, оператором информационной системы является собственник используемых для обработки содержащейся в базах данных информации технических средств, который правомерно пользуется такими

базами данных, или лицо, с которым этот собственник заключил договор об эксплуатации информационной системы.

3. Права обладателя информации, содержащейся в базах данных информационной системы, подлежат охране независимо от авторских и иных прав на такие базы данных.

4. Установленные настоящим Федеральным законом требования к государственным информационным системам распространяются на муниципальные информационные системы, если иное не предусмотрено законодательством Российской Федерации о местном самоуправлении.

5. Особенности эксплуатации государственных информационных систем и муниципальных информационных систем могут устанавливаться в соответствии с техническими регламентами, нормативными правовыми актами государственных органов, нормативными правовыми актами органов местного самоуправления, принимающих решения о создании таких информационных систем.

6. Порядок создания и эксплуатации информационных систем, не являющихся государственными информационными системами или муниципальными информационными системами, определяется операторами таких информационных систем в соответствии с требованиями, установленными настоящим Федеральным законом или другими федеральными законами.

Статья 14. Государственные информационные системы.

1. Государственные информационные системы создаются в целях реализации полномочий государственных органов и обеспечения обмена информацией между этими органами, а также в иных установленных федеральными законами целях.

2. Государственные информационные системы создаются с учетом требований, предусмотренных Федеральным законом от 21 июля 2005 года № 94-ФЗ «О размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд».

3. Государственные информационные системы создаются и эксплуатируются на основе статистической и иной документированной информации, предоставляемой гражданами (физическими

лицами), организациями, государственными органами, органами местного самоуправления.

4. Перечни видов информации, предоставляемой в обязательном порядке, устанавливаются федеральными законами, условия ее предоставления — Правительством Российской Федерации или соответствующими государственными органами, если иное не предусмотрено федеральными законами.

5. Если иное не установлено решением о создании государственной информационной системы, функции ее оператора осуществляются заказчиком, заключившим государственный контракт на создание такой информационной системы. При этом ввод государственной информационной системы в эксплуатацию осуществляется в порядке, установленном указанным заказчиком.

6. Правительство Российской Федерации вправе устанавливать обязательные требования к порядку ввода в эксплуатацию отдельных государственных информационных систем.

7. Не допускается эксплуатация государственной информационной системы без надлежащего оформления прав на использование ее компонентов, являющихся объектами интеллектуальной собственности.

8. Технические средства, предназначенные для обработки информации, содержащейся в государственных информационных системах, в том числе программно-технические средства и средства защиты информации, должны соответствовать требованиям законодательства Российской Федерации о техническом регулировании.

Информация об изменениях: Федеральным законом от 27 июля 2010 г. № 227-ФЗ в часть 9 статьи 14 настоящего Федерального закона внесены изменения, вступающие в силу с 1 января 2011 г.

9. Информация, содержащаяся в государственных информационных системах, а также иные имеющиеся в распоряжении государственных органов сведения и документы являются государственными информационными ресурсами. Информация, содержащаяся в государственных информационных системах, является официальной. Государственные органы, определенные в соответствии с нормативным правовым актом, регламентирующим функционирование государственной информационной системы, обязаны обеспечить достоверность и актуальность информации,

содержащейся в данной информационной системе, доступ к указанной информации в случаях и в порядке, предусмотренных законодательством, а также защиту указанной информации от неправомерных доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения и иных неправомерных действий.

Статья 15. Использование информационно-телекоммуникационных сетей.

1. На территории Российской Федерации использование информационно-телекоммуникационных сетей осуществляется с соблюдением требований законодательства Российской Федерации в области связи, настоящего Федерального закона и иных нормативных правовых актов Российской Федерации.

2. Регулирование использования информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц, осуществляется в Российской Федерации с учетом общепринятой международной практики деятельности саморегулируемых организаций в этой области. Порядок использования иных информационно-телекоммуникационных сетей определяется владельцами таких сетей с учетом требований, установленных настоящим Федеральным законом.

3. Использование на территории Российской Федерации информационно-телекоммуникационных сетей в хозяйственной или иной деятельности не может служить основанием для установления дополнительных требований или ограничений, касающихся регулирования указанной деятельности, осуществляемой без использования таких сетей, а также для несоблюдения требований, установленных федеральными законами.

4. Федеральными законами может быть предусмотрена обязательная идентификация личности, организаций, использующих информационно-телекоммуникационную сеть при осуществлении предпринимательской деятельности. При этом получатель электронного сообщения, находящийся на территории Российской Федерации, вправе провести проверку, позволяющую установить отправителя электронного сообщения, а в установленных федеральными законами или соглашением сторон случаях обязан провести такую проверку.

5. Передача информации посредством использования информационно-телекоммуникационных сетей осуществляется без ограничений при условии соблюдения установленных федеральными законами требований к распространению информации и охране объектов интеллектуальной собственности. Передача информации может быть ограничена только в порядке и на условиях, которые установлены федеральными законами.

6. Особенности подключения государственных информационных систем к информационно-телекоммуникационным сетям могут быть установлены нормативным правовым актом Президента Российской Федерации или нормативным правовым актом Правительства Российской Федерации.

Статья 15.1. Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено.

1. В целях ограничения доступа к сайтам в сети «Интернет», содержащим информацию, распространение которой в Российской Федерации запрещено, создается единая автоматизированная информационная система «Единый реестр доменных имен, указателей страниц сайтов в сети “Интернет” и сетевых адресов, позволяющих идентифицировать сайты в сети “Интернет”, содержащие информацию, распространение которой в Российской Федерации запрещено» (далее — реестр).

2. В реестр включаются:

1) доменные имена и (или) указатели страниц сайтов в сети «Интернет», содержащих информацию, распространение которой в Российской Федерации запрещено;

2) сетевые адреса, позволяющие идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено.

3. Создание, формирование и ведение реестра осуществляются федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий

и связи, в порядке, установленном Правительством Российской Федерации.

4. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, в порядке и в соответствии с критериями, которые определяются Правительством Российской Федерации, может привлечь к формированию и ведению реестра оператора реестра — организацию, зарегистрированную на территории Российской Федерации.

5. Основаниями для включения в реестр сведений, указанных в части 2 настоящей статьи, являются:

1) решения уполномоченных Правительством Российской Федерации федеральных органов исполнительной власти, принятые в соответствии с их компетенцией в порядке, установленном Правительством Российской Федерации, в отношении распространяемых посредством сети «Интернет»:

а) материалов с порнографическими изображениями несовершеннолетних и (или) объявлений о привлечении несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера;

б) информации о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, местах приобретения таких средств, веществ и их прекурсоров, о способах и местах культивирования наркосодержащих растений;

в) информации о способах совершения самоубийства, а также призывов к совершению самоубийства;

2) вступившее в законную силу решение суда о признании информации, распространяемой посредством сети «Интернет», информацией, распространение которой в Российской Федерации запрещено.

6. Решение о включении в реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено, может быть обжаловано владельцем сайта в сети «Интернет», провайдером хостинга, оператором связи, оказывающим

услуги по предоставлению доступа к информационно-телекоммуникационной сети «Интернет», в суд в течение трех месяцев со дня принятия такого решения.

7. В течение суток с момента получения от оператора реестра уведомления о включении доменного имени и (или) указателя страницы сайта в сети «Интернет» в реестр провайдер хостинга обязан проинформировать об этом обслуживаемого им владельца сайта в сети «Интернет» и уведомить его о необходимости незамедлительного удаления интернет-страницы, содержащей информацию, распространение которой в Российской Федерации запрещено.

8. В течение суток с момента получения от провайдера хостинга уведомления о включении доменного имени и (или) указателя страницы сайта в сети «Интернет» в реестр владелец сайта в сети «Интернет» обязан удалить интернет-страницу, содержащую информацию, распространение которой в Российской Федерации запрещено. В случае отказа или бездействия владельца сайта в сети «Интернет» провайдер хостинга обязан ограничить доступ к такому сайту в сети «Интернет» в течение суток.

9. В случае непринятия провайдером хостинга и (или) владельцем сайта в сети «Интернет» мер, указанных в частях 7 и 8 настоящей статьи, сетевой адрес, позволяющий идентифицировать сайт в сети «Интернет», содержащий информацию, распространение которой в Российской Федерации запрещено, включается в реестр.

10. В течение суток с момента включения в реестр сетевого адреса, позволяющего идентифицировать сайт в сети «Интернет», содержащий информацию, распространение которой в Российской Федерации запрещено, оператор связи, оказывающий услуги по предоставлению доступа к информационно-телекоммуникационной сети «Интернет», обязан ограничить доступ к такому сайту в сети «Интернет».

11. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, или привлеченный им в соответствии с частью 4 настоящей статьи оператор реестра исключает из реестра доменное имя, указатель страницы сайта в сети «Интернет»

или сетевой адрес, позволяющий идентифицировать сайт в сети «Интернет», на основании обращения владельца сайта в сети «Интернет», провайдера хостинга или оператора связи, оказывающего услуги по предоставлению доступа к информационно-телекоммуникационной сети «Интернет», не позднее чем в течение трех дней со дня такого обращения после принятия мер по удалению информации, распространение которой в Российской Федерации запрещено, либо на основании вступившего в законную силу решения суда об отмене решения федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, о включении в реестр доменного имени, указателя страницы сайта в сети «Интернет» или сетевого адреса, позволяющего идентифицировать сайт в сети «Интернет».

12. Порядок взаимодействия оператора реестра с провайдером хостинга и порядок получения доступа к содержащейся в реестре информации оператором связи, оказывающим услуги по предоставлению доступа к информационно-телекоммуникационной сети «Интернет», устанавливаются уполномоченным Правительством Российской Федерации федеральным органом исполнительной власти.

Статья 16. Защита информации.

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

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

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации.

2. Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации.

3. Требования о защите общедоступной информации могут устанавливаться только для достижения целей, указанных в пунктах 1 и 3 части 1 настоящей статьи.

4. Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2) своевременное обнаружение фактов несанкционированного доступа к информации;

3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

6) постоянный контроль за обеспечением уровня защищенности информации.

5. Требования о защите информации, содержащейся в государственных информационных системах, устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий. При создании и эксплуатации государственных информационных систем используемые в целях защиты информации методы и способы ее защиты должны соответствовать указанным требованиям.

6. Федеральными законами могут быть установлены ограничения использования определенных средств защиты информации и осуществления отдельных видов деятельности в области защиты информации.

Статья 17. Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации.

1. Нарушение требований настоящего Федерального закона влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

2. Лица, права и законные интересы которых были нарушены в связи с разглашением информации ограниченного доступа или иным неправомерным использованием такой информации, вправе обратиться в установленном порядке за судебной защитой своих прав, в том числе с исками о возмещении убытков, компенсации морального вреда, защите чести, достоинства и деловой репутации. Требование о возмещении убытков не может быть удовлетворено в случае предъявления его лицом, не принимавшим мер по соблюдению конфиденциальности информации или нарушившим установленные законодательством Российской Федерации требования о защите информации, если принятие этих мер и соблюдение таких требований являлись обязанностями данного лица.

3. В случае, если распространение определенной информации ограничивается или запрещается федеральными законами, гражданско-правовую ответственность за распространение такой информации не несет лицо, оказывающее услуги:

1) либо по передаче информации, предоставленной другим лицом, при условии ее передачи без изменений и исправлений;

2) либо по хранению информации и обеспечению доступа к ней при условии, что это лицо не могло знать о незаконности распространения информации.

Статья 18. О признании утратившими силу отдельных законодательных актов (положений законодательных актов) Российской Федерации.

Со дня вступления в силу настоящего Федерального закона признать утратившими силу:

1) Федеральный закон от 20 февраля 1995 года № 24-ФЗ «Об информации, информатизации и защите информации» (Собрание законодательства Российской Федерации, 1995, № 8, ст. 609);

2) Федеральный закон от 4 июля 1996 года № 85-ФЗ «Об участии в международном информационном обмене» (Собрание законодательства Российской Федерации, 1996, № 28, ст. 3347);

3) статью 16 Федерального закона от 10 января 2003 года № 15-ФЗ «О внесении изменений и дополнений в некоторые законодательные акты Российской Федерации в связи с принятием Федерального закона «О лицензировании отдельных видов деятельности» (Собрание законодательства Российской Федерации, 2003, № 2, ст. 167);

4) статью 21 Федерального закона от 30 июня 2003 года № 86-ФЗ «О внесении изменений и дополнений в некоторые законодательные акты Российской Федерации, признании утратившими силу отдельных законодательных актов Российской Федерации, предоставлении отдельных гарантий сотрудникам органов внутренних дел, органов по контролю за оборотом наркотических средств и психотропных веществ и упраздняемых федеральных органов налоговой полиции в связи с осуществлением мер по совершенствованию государственного управления» (Собрание законодательства Российской Федерации, 2003, № 27, ст. 2700);

5) статью 39 Федерального закона от 29 июня 2004 года № 58-ФЗ «О внесении изменений в некоторые законодательные акты Российской Федерации и признании утратившими силу некоторых законодательных актов Российской Федерации в связи с осуществлением мер по совершенствованию государственного управления» (Собрание законодательства Российской Федерации, 2004, № 27, ст. 2711).

Президент Российской Федерации В.Путин

Москва, Кремль
27 июля 2006 г.
№ 149-ФЗ

ЛИТЕРАТУРА

Нормативно-правовые акты

Конституция Российской Федерации // Российская газета. 1993. 25 декабря.

Закон Российской Федерации «О безопасности» от 05.03.92 г. // Ведомости съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации (далее — СНД РФ и ВС РФ). 1992. № 15. Ст. 769.

Закон Российской Федерации «О правовой охране программ для электронных вычислительных машин и баз данных» от 23.09.92 г. // Ведомости СНД РФ и ВС РФ. 1992. № 42. Ст. 2325.

Закон Российской Федерации «О товарных знаках, знаках обслуживания и наименованиях мест происхождения товаров» // Ведомости СНД РФ и ВС РФ. 1992. № 42. Ст. 2322.

Патентный Закон Российской Федерации от 13.09.92 г. // Ведомости СНД РФ и ВС РФ. 1992. № 42. Ст. 2319.

Закон Российской Федерации «О государственной тайне» от 21.07.93 г. с изменениями и дополнениями от 06.10.97 г. // Собрание законодательства Российской Федерации. 1997. № 41. Ст. 4673.

Закон Российской Федерации «Об информации, информатизации и защите информации» от 25.01.95 // Собрание законодательства Российской Федерации. 1995. № 8. Ст. 609.

Гражданский кодекс Российской Федерации от 24.05.96 г. // Собрание законодательства Российской Федерации. 1996. № 25. Ст. 155.

Указ Президента Российской Федерации «Об утверждении перечня сведений конфиденциального характера» от 06.03.97 г. № 188 // Собрание законодательства Российской Федерации. 1997. № 10. Ст. 4775.

Указ Президента Российской Федерации «Об утверждении перечня сведений, отнесенных к государственной тайне» от 24.01.98 г. № 61 // Собрание законодательства Российской Федерации. 1998. № 5. Ст. 561.

Учебная и научная литература

Алексенцев А.И. Организация конфиденциального делопроизводства // Секретарское дело. 2001. № 4.

Алексенцев А.И., *Щегельский А.В.* Организация и ведение секретного делопроизводства: Учебное пособие. М., 1996.

Андрианов В.И. и др. «Шпионские штучки» и устройства для защиты объектов и информации: Справочное пособие. СПб., 1996.

Анин Б.Ю. Защита компьютерной информации. СПб., 2000.

Барсуков В.В., *Водолазкий В.В.* Современные технологи безопасности. Интегральный подход. М., 2000.

Белов В.В., *Виталиев Г.В.*, *Денисов Г.М.* Интеллектуальная собственность. Законодательство и практика его применения: Учебное пособие. М., 1997.

Вус М.А., *Морозов В.П.* Информационно-коммерческая безопасность: Защита коммерческой тайны. СПб., 1993.

Государственная тайна в России: Учебно-методическое пособие. 2-е изд., перераб. и доп. / Под ред. М.А.Вуса. СПб., 2000.

Ярочкин В.И. Служба безопасности коммерческого предприятия. Организационные вопросы. М., 1995.

Ярочкин В.И., *Шевцова Г.А.* Словарь терминов и определений по безопасности информации. М., 1996.

Периодические издания

БДИ: Безопасность, Достоверность, Информация.

Безопасность информации.

Бизнес и безопасность в России.

Вопросы защиты информации (Всероссийский научно-исследовательский институт межотраслевой информации).

Делопроизводство (ЗАО «Бизнес-школа “Интел-Синтез”»).

Документоведение, документационное обеспечение управления (библиографический указатель и экспресс-информация ВНИИДАД ГАС РФ).

Защита информации. Конфидент.

Мир безопасности.

Системы безопасности (компания «Гротек»).

Секретарское дело (ЗАО «Бизнес-школа “Интел-Синтез”»).

Секьюрити.

Телохранитель.

Частный сыск, охрана, безопасность (Интерпол Москва, Издательский дом «Мир безопасности»).

СОДЕРЖАНИЕ

Изд. лиц. ЛР № 020742. Подписано в печать 27.11.2013
Формат 60×84/16. Бумага для множительных аппаратов
Гарнитура Times. Усл. печ. листов 5,25
Тираж 300 экз. Заказ 1423

Отпечатано в Издательстве
Нижневартовского государственного гуманитарного университета
628615, Тюменская область, г.Нижневартовск, ул.Дзержинского, 11
Тел./факс: (3466) 43-75-73, E-mail: izdatelstvo@nggu.ru